International Journal on Perceptive and Cognitive Computing

Volume 11, Issue 1, Year 2025

IIUM
Press

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
e-ISSN: 2462 - 229X
http://journals.iium.edu.my/ijpcc/index.php/IJPCC

INTERNATIONAL JOURNAL ON PERCEPTIVE AND COGNITIVE COMPUTING (IJPCC)

Vol. 11 No. 1 (2025): January 2025

DOI: https://doi.org/10.31436/ijpcc.v11i1

COPYRIGHT TRANSFER AGREEMENT

1. **Consent to publish**: The Author(s) agree to publish the article named above with IIUM Press.

2. **Declaration**: The Author(s) declare that the article named above has not been published before in any form and that it is not concurrently submitted to another publication, and also that it does not infringe on anyone’s copyright. The Author(s) holds the IIUM Press and Editors of the journal harmless against all copyright claims.

3. **Transfer of copyright**: The Author(s) hereby agree to transfer the copyright of the article to IIUM Press, which shall have the exclusive and unlimited right to publish the article in any form, including in electronic media. However, the Author(s) will reserve the right to reproduce the article for educational and scientific purposes provided that written consent of the Publisher is obtained.

The International Journal on Perceptive and Cognitive Computing (IJPCC) journal follows the open access policy.

All articles published open access will be immediately and permanently free for everyone to read, download, copy and distribute for non-commercial purposes.

TABLE OF CONTENT

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 1 (2025)
https://doi.org/10.31436/ijpcc.v11i1.513

The Use of Blockchain in Internet of Medical Things (IoMT)

Haifa Alotaibi, Rana Alaklab, M M Hafizur Rahman
Department of Computer Networks and Communications, King Faisal University, Al-Hofuf, Al-Ahsa 31982, Saudi Arabia

*Corresponding author mhrahman@kfu.edu.sa

(Received: 6th December, 2024; Accepted: 26th December, 2024; Published on-line: 30th January, 2025)

Abstract— The goal of this current study is to address important concerns about data security, privacy, and integrity by amalgamating blockchain technology with the Internet of Medical Things. The IoMT ecosystem consists of wearables, implanted sensors, and remote monitoring tools that generate sensitive medical data continuously, revealing several security vulnerabilities. Blockchain, with its principles of decentralization, transparency, immutability, and cryptographic security, opens up new avenues for securing health data without the use of third-party authorities. This paper outlines the methodology used in this review, including a systematic analysis of relevant literature, utilizing the PRISMA framework to evaluate sources. The analysis identifies key protocols and components of blockchain relevant to IoMT, highlights challenges, and provides solutions. Key findings emphasize blockchain's ability to reduce attacks using distributed ledgers, permissioned access, and encrypted transactions. Furthermore, blockchain may improve patient care by providing real-time data exchange and enabling interoperability across health systems.

Keywords— Blockchain, IoMT, healthcare security, privacy, encryption, interoperability, data management

I. Introduction

Standardized data exchange reinforces clinical decision-making because health professionals will always ensure access to updated and correct patient information [1]. The purpose of the study is to discuss how blockchain technology can be one of the major components in IoMT systems, secure and efficient ones, by stressing how it might solve some of the security and privacy issues when it comes to managing medical data, or how this technology could protect patients' privacy [2]. It further investigates the practical challenges to integrating blockchain into large-scale healthcare systems, including technological complication, cost, and compliance with regulations. Blockchain can improve the overall security of IoMT systems, thereby opening up creative solutions for both medical research and healthcare data management using encryption techniques and decentralized networks [3].

A successful integration of blockchain and IoMT may bring a sea change in healthcare delivery by offering transparent and impregnable data management. It can also be opening up new avenues of collaboration between researchers, insurance companies, and healthcare institutions by guaranteeing secure flow and protection of patient privacy [4]. This is necessary for meeting the legal and ethical criteria when it concerns blockchain-based solutions. In other words, IoMT and blockchain together can pave the path to a more secure, faster, and faultless environment in healthcare for better possibilities in patient care, research based on more reliable data, and therapy personalized. There is greater effort on enhancing health care systems to reach the demand of the patients due to the rapidly developing wearable technologies, wireless connectivity, and implanted sensors. These developments have targeted the continuous and remote patient monitoring while making it decentralized and digitized. Wearables include smartwatches, continuous glucose monitors, ECG sensors, and remote patient monitoring systems that generate enormous data streams at real-time levels [5-6]. These are biometric signals, input from environmental sensors, medical imagery, and patient health records-good examples that can provide time-critical interventions in case scenarios dealing with the health status of a patient. Data such as these can clear the way for healthcare professionals to manage chronic ailments better, early disease diagnosis, and personalized treatment schemes. In addition, remote monitoring technologies continually push the boundaries on standards of treatment by lessening unnecessary hospitalizations and improving patient outcomes [7].

However, the volume and sensitivity of medical data raise several concerns about privacy, security, data management, and interoperability. Sharing healthcare data among multiple stakeholders, such as patients, insurance companies, healthcare providers, and linked devices, raises a variety of trust and illegal access issues [8]. Therefore, the increasing IoMT adoption brings about many threats; in turn, strong security measures are required for the protection of patient privacy and integrity. Medical data breaches or poor handling can lead to severe consequences, such as a loss of trust among patients, litigation issues, and even adverse health consequences. It is thus very important to create secure, transparent, and trustworthy healthcare data ecosystems. Because of its nature, blockchain technology has become a feasible manner in which to overcome these challenges [9]. At first, blockchain technology was used to secure bitcoin transactions; however, today it has evolved as an effective tool in the management and handling of complicated data scenarios. The decentralized nature of blockchain makes alteration or tampering with the data impossible because no one single party would have the complete set of data. Transparency and traceability are added, as every transaction is encrypted and timestamped, with each being verified by the entire network involved. Once data has been entered into the blockchain, the system is virtually unalterable, therefore being a secure means of storing medical information. Since healthcare data management requires strict integrity and confidentiality standards, blockchain pertains especially to this type of data management.

II. Research Methodology

The PRISMA flow diagram describes the study selection process for this review. Initial database searching identified 1,006 records. After excluding 220 records—150 duplicates, 50 automation tool-eligible records, and 20 excluded for other reasons—786 records remained to be screened. After the relevance screening, in the screening phase, a total of 756 records were excluded, and 30 reports were left to retrieve. Of these, 5 reports could not be retrieved due to accessibility issues, thus leaving 25 reports to assess for eligibility.

The eligibility assessment excluded 23 reports on the following grounds: 10 reports on the ground of not meeting the inclusion criteria

- Reason 1 8 due to incomplete data
- Reason 2 and 5 on account of methodological limitations
- Reason 3 Finally, 30 studies met the eligibility criteria and were therefore included in this review.

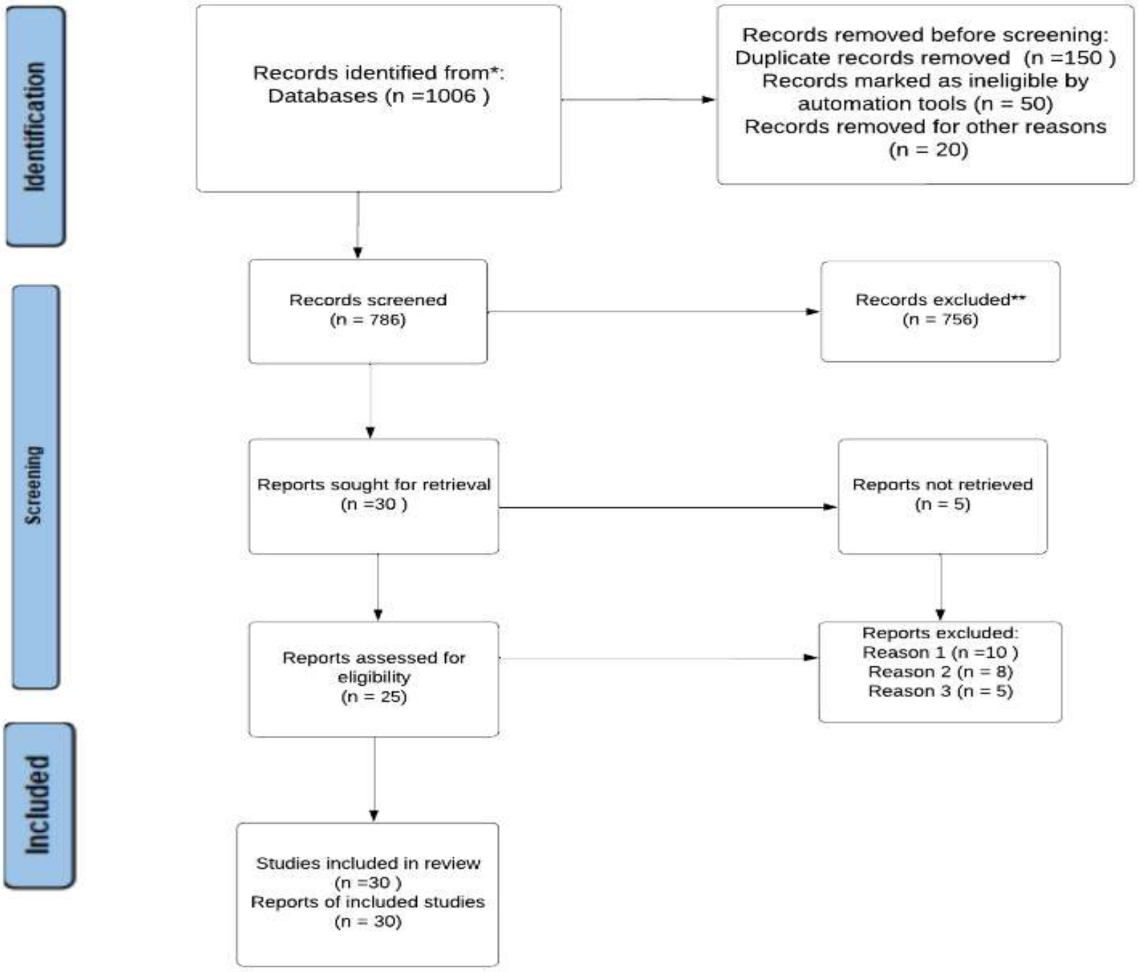


Fig 1: PRISMA Flow Diagram of Study Selection

III. *Related works*

Blockchain is "adecentralized and immutable ledger that securely and transparently records transactions, eliminating the need for a central authority." Blockchain applications in the healthcare industry range from simple data storage to the assurance of patient privacy, data integrity, and trust mechanisms that meet the specific security and accountability requirements of the industry. Therefore, blockchain provides a secure, decentralized foundation for the management of private health information created by IoMT devices, from sophisticated imaging systems to wearable health monitors.

The integration of blockchain into IoMT networks hence improves device security by addressing the inefficiencies of classical systems. For example, a blockchain-based architecture to guarantee secure health data management. As they claimed, such a decentralized blockchain reduces the occurrence of single points of failure while its cryptographic algorithms practically eliminate unwanted accesses, which guarantees the security and integrity of sensitive data. [7]

In this context, security not only includes data protection but also management of digital identities within healthcare networks. IoMT devices are often left vulnerable due to either inappropriate or default authentication mechanisms. The automation of identity verification procedures using smart contracts in blockchain technology is a major constituent of the prevention of identity theft and unauthorized access, ensuring that access to data is allowed only to subjects with permission [11-14]

Given this, researchers in recent times have explored blockchain as a potential solution for IoMT systems' scalability challenges. It also identified how blockchain can further enhance real-time monitoring at minimal costs in healthcare, even though they emphasize that scalability remains one of the most critical issues [12]. They state that though blockchain provides decentralization and integrity, it cannot support the high frequency of flows generated by the devices around IoMT, especially when there are multiple stakeholders present in a system. The balancing of decentralization, security, and scalability without compromising any in effectiveness is really essential via some creative off-chain and on-chain strategies.

While academics are trying to overcome the challenges of protecting sensitive IoT data, much emphasis has been paid to the inclusion of Blockchain technology into IoT security frameworks. According to Banerjee et al. [11] who review IoT security solutions, research and development are hampered by a crucial gap in the availability of publicly available IoT statistics. They argue that blockchain may fill this gap by assuring data integrity and traceability, thus enabling the secure sharing of sensitive datasets. The authors also propose two theoretical Blockchain-based strategies for enhancing the security of IoT systems and call for deeper research into nine specific research problems with a view to guiding future investigations. This position illustrates blockchain as the game-changing technology that would promise safe IoT ecosystems, such as the Internet of Medical Things. [6]

Integrating Blockchain into IoMT to improve data security in the healthcare industry is very important. The underlying data is guaranteed to be accessible while maintaining its integrity without third-party intermediaries due to methods of encryption and Blockchain's inherent decentralized architecture [15]. The approach allows secure communication of IoMT devices with the practitioners of healthcare, privacy laws are ensured, and the weaknesses of a centralized system are reduced. The findings showed that improved clinical practices and real-time, patient-centered care rely on secure data handling. [10]

In addition, the role of blockchain in enabling secure data exchange in healthcare has been investigate [12-18]. It has been noted that smart contracts make possible the secure sharing of data between IoMT devices and healthcare providers, therefore improving data interoperability and adherence to privacy regulations. Secure data exchange is critical within medical contexts, where timely, accurate data sharing is crucial in ensuring proper patient care and related outcomes. [19]

Strong security frameworks need to be designed considering the intrinsic vulnerabilities arising in real-time patient monitoring due to increased IoMT integration in healthcare.IoMT-based security architecture powered with Blockchain, integrated with recent federated learning and state-of-the-art encryption techniques. Availability, confidentiality, and integrity of the data are ensured by this approach through mitigation against different risks related to replay attack, eavesdropping, and manipulation of data. Comparing their results against some benchmark solutions, such as MRMS and BACKM-EHA, they demonstrate very promising enhancements regarding the detection of anomalies and resistance to various types of cyber-attacks. Besides that, an adaptive learning mechanism gives this framework a future-proofed solution for IoMT security because it is also adaptive in changing according to new threats. [20]

Whereas it had been widely regarded that blockchain would help solve some IoMT security challenges that have haunted the world for quite some time, gaps still exist in terms of scalability, interoperability, and regulatory compliance. The advantages of blockchain transparency and traceability but emphasize limitations in handling big volumes of data generated from IoMT systems. This calls for further innovation of blockchain solutions to meet such high demands of frequency without compromising [13].

Consequently, blockchain and IoMT security have turned into an interdisciplinary study that conceptually extracts ideas from information technology, cryptography, and healthcare informatics. These disciplines remain instrumental for the researchers to understand, predict, and improve the applications of blockchain in IoMT, with the ultimate aim of creating a more secure and reliable healthcare system.

Integrating blockchain technology into the Internet of Medical Things (IoMT) has transformative potential for healthcare, notably by enhancing interoperability, data security, and privacy. However, while the promise of blockchain is clear, I believe that several critical challenges must be addressed before widespread, practical implementation in real-world healthcare settings becomes feasible. [18]

TABLE I
KEY STRENGTH OF BLOCKCHAIN TECHNOLOGY IN IOMT

Strength	Description
Decentralization	Reduces single-point failures through distributed networks.
Data Security	Protects sensitive medical data through encryption and ensure unauthorized access is minimized.
Identity Management	Verifies identities using smart contracts, ensuring only authorized users can access data.
Data Integrity	Tracks and audits data all changes to ensure accountability and transparency.
Real-Time Monitoring	Enables continuous monitoring of IoMT devices, providing instant alerts for anomalies.

IV. Strengths of Blockchain in IoMT:

Decentralization: Because blockchain technology does not require a central authority, the probability of single-point failures is greatly decreased.

Data Security: By guaranteeing encryption and anonymity and making illegal access very difficult, blockchain's cryptographic processes protect health data. [1][3][7]

Identity Management: Blockchain improves safe identity verification through the use of smart contracts and decentralized identifiers, which is essential for preventing data fraud and identity theft. [1][3][7]

Data Integrity and Traceability: The immutable nature of blockchain technology facilitates accurate data monitoring and auditing, which promotes accountability and openness in the administration of healthcare data. [1][3][7]

Real-Time Monitoring: Blockchain technology enables ongoing IoMT device monitoring and provides real-time warnings when security abnormalities are detected, facilitating prompt action. [1][3][7]

Weaknesses and Research Gaps in Blockchain for IoMT:

Scalability Issues: IoMT devices generate enormous volumes of data that are too big for existing blockchain platforms to manage. Latency and performance problems result from this incapacity to handle such large numbers, especially in real-time applications.

Performance Issues: IoMT systems' efficiency, which is crucial for applications involving real-time patient monitoring, may be adversely affected by the computational and storage needs necessary for blockchain activities.

Interoperability Limitations: Inadequate interoperability between different blockchain frameworks and IoMT devices makes it difficult to integrate and exchange data seamlessly, which lowers healthcare networks' overall efficiency.

Regulatory and Compliance Issues: The regulatory environment in the healthcare industry poses issues for blockchain compliance, especially in relation to the right to data rectification and data immutability.

Blockchain strengthens IoMT by enhancing data security, decentralizing data management, and improving secure identity verification. Its cryptographic approach reduces vulnerabilities and supports real-time monitoring, giving patients more control over their data. However, challenges like scalability, interoperability, regulatory compliance, and limited user-friendly design remain barriers to widespread adoption in healthcare.

- The Need for New Strategies

The healthcare sector has to embrace novel strategies that go beyond accepted practices in order to reduce the security threats connected to IoMT devices. These tactics have to concentrate on strengthening device authentication, guaranteeing safe data transfer, and preserving the accuracy of medical records.

1. Decentralized Identity Management: Blockchain technology can provide safe identity management systems that guarantee sensitive data is only accessible by authorized people and devices. Blockchain technology can assist with identity verification without the need for a

central authority by utilizing cryptographic keys and decentralized identifiers. [1][3][7]

2. Safe Data Exchange: IoMT devices may exchange data with only those who are allowed thanks to blockchain technology. By automating the authorization procedures, smart contracts can guarantee adherence to privacy laws and foster device interoperability.

3. Real-Time Monitoring and Alerts: Blockchain's real-time features allow for ongoing IoMT device monitoring, identifying irregularities that could point to security lapses. Automatically triggering alerts enables prompt action and correction. [1][3][7]

4. Data Integrity Verification: The immutability of blockchain technology makes it possible to trace and validate any modifications made to patient data, creating an audit trail that improves accountability and transparency in the administration of healthcare data. [1][3][7]

- Identification of Gaps

There are still a number of important gaps in the research, despite the fact that several studies have highlighted the advantages of using blockchain technology into the Internet of Medical Things (IoMT) to improve security. These limitations point to areas that need more research to guarantee the successful and expandable use of blockchain technologies in the medical field.

1. Scalability Challenges The scalability of blockchain solutions in IoMT contexts is one of the main research needs. The majority of studies, such as those by Zhang et al. (2018) and Kuo et al. (2017), concentrate mostly on security and privacy issues without sufficiently discussing how these solutions can scale to handle the enormous amount of data produced by IoMT devices. The underlying blockchain network may find it difficult to handle large transaction volumes in real-time as the number of linked medical devices grows dramatically, which might result in latency problems and poor performance. This is especially important in medical contexts where prompt access to patient data is necessary for efficient care. As transaction volumes increase, the consensus techniques used by many blockchain networks—such as proof-of-work or even proof-of-stake—may create bottlenecks. Alternative consensus algorithms created especially for IoMT contexts should be investigated in future studies in order to improve scalability without sacrificing security.

2. Performance Issues Performance concerns are linked to scalability and have not received enough attention in the literature to yet. Although the studies frequently emphasize the security advantages of blockchain, they frequently fail to consider how the intrinsic features of blockchain affect the overall functionality of IoMT systems. For example, delay may be introduced by the computational and storage cost needed to operate a blockchain, especially in applications that demand real-time patient vital sign monitoring.

3. Interoperability Issues Interoperability between various blockchain systems and IoMT devices is not given enough attention in the current corpus of research, which is another important gap. As there are several blockchain implementations and standards available, it is still difficult to guarantee smooth communication and integration between various IoMT devices and blockchain networks. Without taking into account how they could interact with other healthcare technologies or current systems, the evaluated research frequently isolate their blockchain applications. The broad adoption and integration of blockchain solutions in IoMT may be hampered by the absence of established standards for interoperability. In order to guarantee that data may move freely and securely between platforms, future research should focus on creating frameworks that promote interoperability among different blockchain systems and IoMT devices.

4. Regulatory and Compliance Challenges Although the regulatory environment around data security and privacy is mentioned in a number of publications, thorough examinations of how blockchain applications in IoMT can comply with these frameworks are conspicuously lacking. More study is required to determine how blockchain might facilitate adherence to current standards while encouraging innovation, given the intricate and sometimes disjointed structure of healthcare legislation throughout the world. The regulatory issues of identity verification have been mentioned in studies such as those by Chakchai So-In, but there hasn't been a full analysis of the legal ramifications of blockchain's immutability, particularly with regard to data rectification rights and audit trails. To give practitioners and legislators useful information, researchers should look at how blockchain technology, healthcare laws, and ethical issues interact.

5. User-Centric Design Finally, a gap exists in blockchain applications for IoMT with regard to user-centric design. The majority of current research ignores the end-user experience in favor of technological frameworks and algorithms. The usability of blockchain solutions for patients, healthcare professionals, and other stakeholders is essential to their efficacy in the industry. Studies frequently neglect to discuss how people can be successfully informed about the intricacies of blockchain technology or how user interface design may promote usability while upholding strong security protocols. User experience studies should be given top priority in future research in order to comprehend the requirements, inclinations, and actions of stakeholders dealing with blockchain-enabled IoMT systems.

- Personal Opinion

Blockchain technology's incorporation into the Internet of Medical Things (IoMT) is revolutionizing the healthcare industry, especially in terms of improving interoperability, data security, and privacy. However, even though I see that blockchain solutions have a lot of promise, I also think that there are a lot of issues that need to be resolved before they can be successfully applied in actual healthcare settings.

Stressing the Value of Scalability The scalability of blockchain technology in IoMT apps is one of my main worries. Any blockchain system used in healthcare must be able to manage this expansion without sacrificing speed, given the quickly growing number of linked medical devices and the amount of data they produce. Despite their security, current consensus methods might not be appropriate for IoMT systems' high throughput needs. I think that the creation of scalable, lightweight blockchain systems that can meet the unique requirements of healthcare applications should be the main focus of future research.

Performance as a Crucial Elements Another important topic that, in my opinion, needs further research is performance. It is impossible to ignore the latency problems brought forth by blockchain's intrinsic features in an area where instantaneous data access might mean the difference between life and death. Researchers must concentrate on speeding up blockchain technology without compromising the security aspects that first drew people in since applications like emergency services and remote patient monitoring require quick reaction times.

Performance as a Vital Component Performance is another crucial subject that, in my opinion, requires more investigation. In a field where immediate data access might be life-or-death, it is hard to overlook the latency issues posed by blockchain's inherent properties. Because applications like emergency services and remote patient monitoring demand rapid reaction times, researchers must focus on accelerating blockchain technology without sacrificing the security features that first attracted users.

Handling Regulatory Environments Blockchain technology's regulatory issues are also important to consider. Researchers need to look at how blockchain can fit into these frameworks as healthcare rules continue to change. Blockchain solutions must meet legal requirements for data access, modification, and storage in addition to improving security and privacy. Gaining the trust of patients and healthcare professionals alike will depend on resolving these problems, which is critical for the broad use of blockchain in IoMT.

Using User-Centric Design to Close the Gap Lastly, it is impossible to exaggerate the significance of user-centric design. Any blockchain application in healthcare must prioritize the user experience, even while technological developments are crucial. The advantages of improved security and privacy will be compromised if patients and healthcare providers find blockchain technologies difficult to use or unwieldy. In order to guarantee that the final systems are safe and easy to use, I support a comprehensive strategy that integrates user input into the design process.

In conclusion, even if blockchain technology has unquestionably enormous promise for the Internet of Medical Things, academics and practitioners must fill in the gaps in the literature. Blockchain applications in healthcare may be made safe and successful by emphasizing scalability, performance, interoperability, regulatory compliance, and user-centric design. I'm still hopeful about IoMT's future and how blockchain technology might help build a more patient-centered, safe, and effective healthcare system as we continue to investigate these possibilities.

V. Future Research Directions

Blockchain technology has the potential to significantly improve the security and privacy of Internet of Medical Things (IoMT) systems, particularly when it comes to safeguarding sensitive medical data and maintaining electronic health records. However, because of its high computing needs, blockchain implementation is difficult on IoMT devices, which frequently have limited computational capabilities.

1. **Improving Blockchain Efficiency for Resource-Constrained IoMT Devices**:

   Making blockchain protocols lighter and more effective should be the main focus of future research in order to meet the resource constraints of IoMT devices. This may entail:

   - creating consensus techniques like Delegated Proof-of-Stake (DPoS) and Proof-of-Authority (PoA) that require less computing power.
   - employing off-chain processing strategies to reduce the stress on the device.
   - investigating edge and fog computing as a way to lower latency and energy usage in conjunction with blockchain-based IoMT systems.

2. **New Applications for Data and Permission Management**: Similar to the MedRec concept, blockchain can facilitate safe, permission-based access to health data, giving consumers and healthcare practitioners the ability to manage who has access to the data. Among the possible avenues for investigation are:

   - establishing structures that enable precise management of patient data access.
   - using smart contracts to guarantee data integrity and automate access rights.

- investigating distributed identity management options to improve patient data control while adhering to privacy laws.

3. **Integrating Blockchain with Other Security Technologies**: The synergy between blockchain and technologies such as artificial intelligence (AI) can bolster IoMT systems by:
    - Enhancing threat detection through AI-based anomaly detection integrated with immutable blockchain records.
    - Facilitating predictive analytics by securely sharing anonymized health data.
    - Improving patient outcomes by enabling real-time data sharing among healthcare providers while preserving security.
4. **Developing Security Assessment Standards for Blockchain in IoMT**: To improve system It is crucial to create security assessment guidelines specifically for blockchain applications in IoMT in order to foster confidence and guarantee dependability. This includes:
    - defining measures to assess durability, scalability, and privacy.
    - creating standardized frameworks for penetration testing in IoMT settings.
    - working together with regulatory agencies to guarantee adherence to changing international healthcare standards.
5. **Exploring Hybrid Solutions**: Data security and regulatory compliance may be improved by hybrid models that blend centralized systems with decentralized blockchain components. Solutions that are hybrid could:
    - For data provenance, use decentralized blockchain systems; for storage-intensive operations, use centralized servers.
    - Permit selective decentralization, in which access logs and metadata are maintained on the blockchain while important data is kept in centralized storage.
    - Enable adherence to laws such as GDPR while preserving the advantages of blockchain immutability.
6. **Enhancing Storage Solutions Focused on Users**
   Creating user-owned and controlled decentralized storage systems is a new field of study. Among the possible directions are:

- developing mobile gadgets or systems that run on smartphones for safe local data storage.
- use smart contracts to enforce user-defined access rules in order to ensure accessibility.
- investigating how to integrate distributed storage systems to offer safe and scalable data-sharing options.

7. **Reward-Based Data Contribution Models**
   Current systems often do not recognize or reward patients for contributing valuable health data.
   Future blockchain-based IoMT ecosystems could:

- Implement **token-based rewards** for individuals who contribute data, incentivizing data sharing while respecting privacy.
- Foster **data crowdsourcing** to advance scientific research and improve public health.
- Shift the paradigm from **system-centric to user-centric**, empowering individuals to become active participants rather than passive consumers.

By boosting data security, giving patients more control over their data, and providing transparent, decentralized solutions, integrating blockchain technology into IoMT systems has the potential to completely transform the healthcare industry. But accomplishing these objectives would need overcoming formidable obstacles pertaining to data management, resource limitations, security standards, and regulatory compliance. To fully realize the benefits of blockchain in IoMT and build safe, patient-centered healthcare ecosystems, future research will need to concentrate on creating more effective blockchain protocols, sophisticated data access control, AI-integrated security, standardized security assessment frameworks, and hybrid blockchain models.

VI. Conclusions

The research emphasizes how blockchain technology can alter healthcare systems when combined with the IoMT. Blockchain offers a strong framework for improving patient-centric healthcare by tackling issues like data privacy, decentralized administration, and identity verification. Real-time monitoring and safe exchange among stakeholders are made possible by its cryptographic capabilities, which guarantee the confidentiality and privacy of sensitive medical data and give patients control over their health information. Blockchain supports safe data interchange across institutions, promoting collaborative care and stimulating innovation in healthcare research. It also makes decentralized data administration possible, reducing the hazards associated with centralized repositories, such as breaches and illegal access. However, a number of barriers prevent blockchain from being widely used in IoMT systems for healthcare. The processing needs of blockchain continue to cause scalability problems, which might place a strain on IoMT devices with limited resources. Blockchain solutions must comply with strict healthcare regulations and complicated implementations can lead to unintuitive designs that prevent patient and provider acceptance. Regulatory compliance is still a major barrier. Future research must concentrate on creating standardized security assessment frameworks to guarantee strong privacy and security, investigating hybrid blockchain models to address issues of scalability and compliance, incorporating artificial intelligence to improve security and facilitate predictive analytics, and developing off-chain solutions and lightweight blockchain protocols to support devices with limited resources. Additionally, patients can be empowered to actively manage their health data by giving priority to user-centric platforms with intuitive designs. Large-scale health data collecting is made possible by modern IoMT devices, which presents chances for better patient care and tailored treatment. Blockchain can further this development by developing safe platforms that put privacy, scalability, and interoperability first. These platforms can facilitate cooperative ecosystems in which patient data directly advances science and improves healthcare results. Blockchain-enabled IoMT systems have the potential to build safe, open, and patient-centered healthcare ecosystems, promoting a better-informed and healthier society, even though there are still obstacles to overcome.

ACKNOWLEDGMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1]. J. Indumathi, A. Shankar, M. R. Ghalib, J. Gitanjali, Q. Hua, and Z. Wen, “Block chain based internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (BC IoMT U6 HCS),” *IEEE Access*, vol. 8, no. 12, pp. 123-135, Nov. 2020, doi:10.1109/ACCESS.2020.3040240.

[2]. Y. Sun, F. P.-W. Lo, and B. Lo, “Security and privacy for the internet of medical things enabled healthcare systems: A survey,” *IEEE Access*, vol. 8, no. 1, pp. 123-135, Dec. 2019, doi: 10.1109/ACCESS.2019.2960617.

[3]. M. El Khatib, H. M. Alzoubi, S. Hamidi, M. Alshurideh, A. Baydoun, and A. Al-Nakeeb, “Impact of using the internet of medical things on ehealthcare performance: Blockchain assist in improving smart contract,” *ClinicoEconomics and Outcomes Research*, vol. 15, pp. 397-411, Jun. 2023, doi: 10.2147/CEOR.S407778.

[4]. S. Razdan and S. Sharma, “Internet of medical things (IoMT): Overview, emerging technologies, and case studies,” *IETE Technical Review*, vol. 39, no. 4, pp. 775-788, May 2022, doi: 10.1080/02564602.2021.1927863.

[5]. M. Jmaiel, M. Mokhtari, B. Abdulrazak, H. Aloulou, and S. Kallel, Eds., *The impact of digital technologies on public health in developed and developing countries*, LNCS 12157, Proceedings of the 18th International Conference, ICOST 2020, Hammamet, Tunisia, Jun. 24–26, 2020, doi: 10.1007/978-3-030-51517-1.

[6]. H. Taherdoost, “Blockchain-based internet of medical things,” *Applied Sciences*, vol. 13, no. 1287, 2023, doi: 10.3390/app13031287.

[7]. G. Bigini, V. Freschi, and E. Lattanzi, “A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision,” *Future Internet*, vol. 12, no. 208, Nov. 2020, doi: 10.3390/fi12120208.

[8]. Z. Sun, D. Han, D. Li, X. Wang, C.-C. Chang, and Z. Wu, “A blockchain-based secure storage scheme for medical information,” *Journal of Wireless Communications and Networking*, vol. 2022, no. 40, 2022, doi: 10.1186/s13638-022-02122-6.

[9]. W. A. N. A. Al-Nbhany, A. T. Zahary, and A. A. Al-Shargabi, “Blockchain-IoT healthcare applications and trends: A review,” *IEEE Access*, vol. 12, pp. 1-10, Jan. 2024, doi:10.1109/ACCESS.2023.3349187.

[10]. S. Yongjoh, C. So-in, P. Kompunt, P. Muneesawang, and R. I. Morien, “Development of an internet-of-healthcare system using blockchain,” *IEEE Access*, vol. 9, pp. 136158-136169, Aug. 2021, doi: 10.1109/ACCESS.2021.3103443..

[11]. M. Banerjee, J. Lee, and K.-K. R. Choo, “A blockchain future for internet of things security: A position paper,” Digital Communications and Networks, vol. 3, no. 2, pp. 149–157, 2018, doi: 10.1016/j.dcan.2017.10.006.

[12]. Y. Yasin Ghadi, T. Mazhar, T. Shahzad, M. A. Khan, A. Abd-Alrazaq, A. Ahmed, and H. Hamam, “The role of blockchain to secure internet of medical things,” Scientific Reports, vol. 14, no. 1, pp. 1011-1020, 2024, doi: 10.1038/s41598-024-68529-x.

[13]. M. Pilkington, "Can Blockchain improve healthcare management? Consumer medical electronics and the IoMT," SSRN Electronic Journal, 2016, doi: 10.2139/ssrn.3025393..

[14]. A. Sharma, S. Singh, R. Tomar, N. Chilamkurti, and B.-G. Kim, "Blockchain based smart contracts for Internet of Medical Things in e-healthcare," Electronics, vol. 9, no. 10, pp. 1609, 2020, doi: 10.3390/electronics9101609.

[15]. H. Taherdoost, “Blockchain-based internet of medical things,” *Applied Sciences*, vol. 13, no. 1287, 2023, doi: 10.3390/app13031287. [7] G. Bigini, V. Freschi, and E. Lattanzi, “A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision,” *Future Internet*, vol. 12, no. 208, Nov. 2020, doi: 10.3390/fi12120208.

[16]. C. C. Y. Hang, M. Batumalay, T. D. Subash, R. Thinakaran, and B. Chitra, "Blockchain-based and IoT-based health monitoring app: Lowering risks and improving security and privacy," Journal of Health Informatics, vol. 7, no. 1, pp. 42-48, 2020.

[17]. Y. Wang and L. Sun, "Privacy protection of secure sharing electronic health records based on blockchain," Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 7, pp. 922-928, 2024. doi:10.1109/ACCESS.2023.3349187.

[18]. A. Sharma, S. Singh, R. Tomar, N. Chilamkurti, and B.-G. Kim, "Blockchain based smart contracts for Internet of Medical Things in e-healthcare," Electronics, vol. 9, no. 10, p. 1609, Oct. 2020.DOI: https://doi.org/10.3390/electronics9101609

[19]. F. Ellouze, G. Fersi, and M. Jmaiel, "Blockchain for Internet of Medical Things: A Technical Review," in Proc. ICOST 2020, Sfax, Tunisia, 2020, vol. 12157, pp. 259–267. [Online]. Available: https://doi.org/10.1007/978-3-030-51517-1_22

[20]. H. Mansouri, R. Hireche, C. Benrebbouh, and A.-S. K. Pathan, "A Review of Blockchain in Internet of Medical Things," in Cryptology and Network Security with Machine Learning, A. Chaturvedi et al., Eds., Lecture Notes in Networks and Systems, vol. 918, Singapore: Springer Nature, 2024, pp. 1–10. [Online]. Available: https://doi.org/10.1007/978-981-97-0641-9_28

BiologAR: An Interactive Augmented Reality Application for Learning Biology in Secondary Schools in Malaysia

Hazwani Mohd Mohadis*, Afifi Syahmi Kamal-Ludin, Mohd Norhazmi Nordin
Department of Information Systems, Kulliyyah of Information Communication Technology, International Islamic University Malaysia (IIUM), Malaysia

*Corresponding author hazwanimohadis@iium.edu.my

(Received: 28th August, 2024; Accepted: 29th December, 2024; Published on-line: 30th January, 2025)

Abstract— Biology is one of the subjects taught in secondary school in Malaysia. The subject requires a lot of visualization to enhance students understanding on the scientific theories they learned in Biology class. The advanced of Augmented Reality (AR) technology can be useful for students to help them understand Biology subject better as they able to visualize various scientific theories and concepts using 3D objects. AR also had been proven to be able to create a fun and interactive learning environment for these Generation Z students compared to traditional printed textbook. Accordingly, in this project, we are proposing BiologAR mobile application as an assisting tool to support teachers and students in teaching and learning Biology. This BiologAR application would help students to visualize some content of the Biology syllabus using AR technology. The application also provides a simple quiz for students to assess their understanding of the chapter. The application had been developed using Unity 3D software for Android platform. Based on the user testing conducted with the students and teacher, our BiologAR mobile application had been proven to be easy to use and useful to enhance students understanding of Biology subject.

Keywords— augmented reality, mobile application, biology, assisted learning environment, educational tools.

I. Introduction

In this paper we described the development of BiologAR, an e-learning mobile application that is integrated with augmented reality technology. The application is to be used as an assisting tool for Form 4 and Form 5 secondary school students to learn Biology. It is an interactive application that uses 3D visualizations, animations, sounds and graphics. The objective(s) of the development of BiologAR application are:

I. To help the student understand Biology subject better through visuals and explanations provided in the application.
II. As an assisting tool for teachers to teach and enhance their students understanding about Biology subject.
III. To expose students to use technology in learning, thus preparing them for the Industrial Revolution 4.0 (IR4.0) which emphasizes on the use of technology and internet in everyday life.

II. Problem Statement

A study by Weng et. al [1] found out that learning Biology from the textbook alone can be challenging to students as textbook is lacking in terms of interactivity and visualization –making the learning process less engaging and not effective. Similarly, another study by Sorgo [2] identified that some students have difficulties to visualize the Biology concept from information provided in the textbook due to lack of creativity. Besides, lack of exposure to AR-based e-learning technology also had been an issue as many students did not aware on how these applications would help them to understand the Biology subject better [3].

These problems hence motivated us to develop BiologAR mobile application, with the primary aim to enhance students understanding on Biology concepts through interactive 3D visualization using AR technology. By developing this BiologAR app, we believe students' interest, understanding and engagement in learning Biology subject would be improved.

III. Methodology

For the development approach, we are adopting the Iterative-Visual Cognitive Software Development Life Cycle Methodology (I-VC SDLC) by Chowdhury [4] as presented in the following Fig. 1.

This methodology was used because we as the developers need to understand how augmented reality works as a virtual model that appears and co-existing in the real environment through projection inside the application.

The methodology consists of four majour phases which are 1) analysis on the user needs and requirements, 2) design of the proposed solution, 3) development and evaluation of the mobile e-learning application, and finally 4) implementation and testing with target users. The subsequent sections in this article will be presented based on these sequential phases.

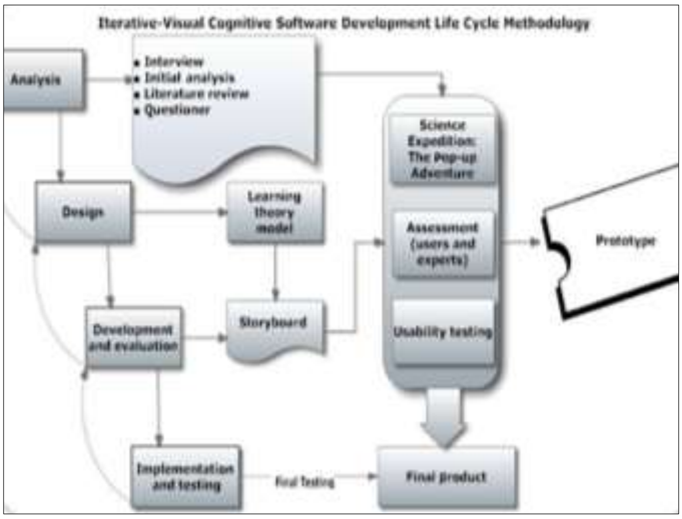

Iterative-Visual Cognitive Software Development Life Cycle Methodology
Analysis
• Interview
• Initial analysis
• Literature review
• Questioner
Design
Learning theory model
Development and evaluation
Storyboard
Science Expedition: The Pop-up Adventure
Assessment (users and experts)
Usability testing
Prototype
Implementation and testing
Final testing
Final product

Fig. 1 Iterative-Visual Cognitive Software Development Life Cycle Methodology (I-VC SDLC) [4]

A. *User Requirements Analysis*

In order to understand the challenges that students experienced in learning Biology, a preliminary user study was conducted using survey method at two (2) secondary schools in southern Malaysia. Before we distribute our survey, we asked for approval to conduct data collection from both schools. Once approval had been granted, we proceed with the distribution of the survey to Form 4 and Form 5 students. A total of 95 students responded to our survey. The following Table I summarized the findings that we got from this user study.

TABLE I
SUMMARY OF FINDINGS FROM STUDENTS' QUESTIONNAIRE RESPONSES

Questionnaire Item	Students' responses (N= 95)
1. Do you find Biology subject difficult?	Not difficult at all (6%) Difficult (89%) Extremely difficult (5%)
2. Which kind of learning materials that you prefer to learn Biology?	Textbook (25%) Slides in class (38%) Notes from teacher (37%)
3. Does learning through textbook helps you to understand topics in Biology?	Yes (78%) No (22%)
4. Did you think that the explanation provided in the textbook sufficient for you to understand the subject?	Yes (44%) No (56%)
5. Do you think adding more visual explanations can improve your understanding in Biology subject?	Yes (100%) No (0%)
6. Which platform you normally used for e-Learning?	PC/Laptop (35%) Smartphone/tablet (42%) Never use (23%)
7. Which feature is the most important to include in the eLearning application?	Visual 3D model (53%) Video explanation (30%) Exercises (17%)

Based on Table 1 above, in terms of level of difficulty, majority of the students feel that Biology is difficult (89%) and extremely difficult (5%) subject. Only very few students (6%) think that the subject is relatively easy. In terms of learning materials preferred to learn Biology, many of the students prefer to use slides in class (38%) and notes from teachers (37%) compared to those prefer to use textbook (25%). However, when we asked them if the textbook helps them to understand, majority of the students said yes (78%), while only (22%) said otherwise.

Besides, when we asked the students if the explanation in the textbook is sufficient, the result shows that more than half of the students (56%) did not agree to the fact that the textbook has been giving good explanations for them to better understand the subject. We believed this is because the information and explanations provided by the textbook are lengthy and complicated. Besides, we also found out that they are having difficulties trying to understand some topics in Biology where they need to visualize those scientific concepts.

Regarding the idea on adding more visual explanations to enhance understanding on Biology subject, it is evidence that all students (100%) agreed that the approach could potentially improve their understanding. This indicate that it is apparent that students need some visualization assistance to understand some topics in the Biology subject better.

Apart of asking questions on their thought on learning Biology, we also asked them on their technological experience to know about the platform that they are familiar with for e-learning. The result shows that 42% of the students use smartphones or tablet compared to 35% using personal computer/laptop. This is potentially due to the fact that smartphones and tablet are more accessible and portable which makes them easier to use for e-learning anytime and anywhere [5]. Besides, we also asked students on the most important feature to include in the e-learning application, to which more than half of the students (53%) suggested visual 3D as the most important feature, followed by video explanation (30%) and exercises (17%).

Further, we also asked the students on topic(s) in Biology subject that they found difficult to understand (*they may choose more than one topic for this question*). The result is presented in the Figure 2.

Based on the table. it is apparent that the 'Cell Division' became the most difficult topic with a total of 65 out of 95 students (68.4%) think they need more guidance for it. This outcome helps us to decide that 'Cell Division' as the most important chapter that need to supported with 3D AR visualization in our BiologAR app.

https://doi.org/10.31436/ijpcc.v11i1.500

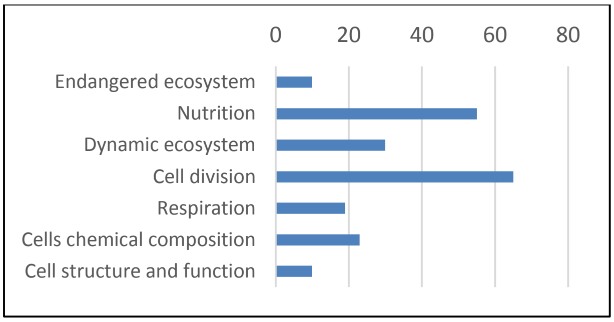


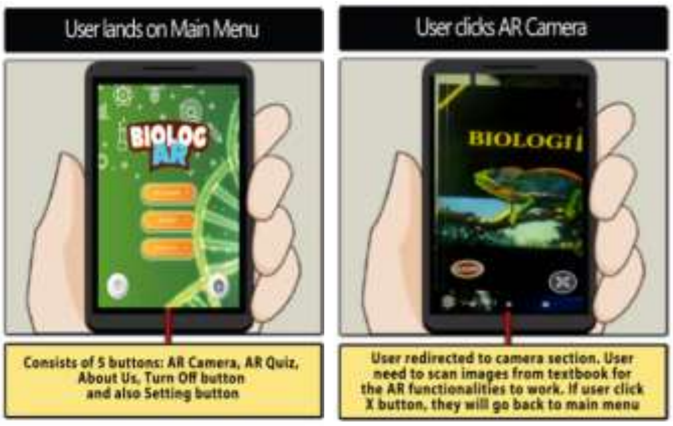
Fig 2: Chapters in Biology That Students Found Challenging to Understand (N=95)

B. *Content Development and Storyboard*

When developing and designing the application, we as the developers need to consider several aspects; which include the syllabus of the subject and topics for the content. Thus, in the early stages of the project, we have conducted multiple discussions with Biology teachers at school to make sure that the theoretical concepts presented in the application along with the accompanied 3D visualization are valid, accurate and able to strengthen students' understanding.

Apart of discussions and advices from the teacher, we also use Biology textbook adopted at the school as our main reference. One of the modules in BiologAR is the cell divisions topic which made up of six (6) phases –interphase, prophase, metaphase, anaphase, telophase and cytokinesis. All these 6 phases have different processes. Therefore, six (6) different 3D models with six (6) different animations are required to be developed to help students easily visualized the cell division processes and profoundly understand this topic.

Further, we also developed storyboard. Storyboarding is a very crucial phase in AR development to give a clear view on the flow of the application, the contexts of use and the system interfaces [6]. The following Fig. 3 shows some storyboard developed for BiologyAR mobile application.



Consists of 5 buttons: AR Camera, AR Quiz, About Us, Turn Off button and also Setting button

User redirected to camera section. User need to scan images from textbook for the AR functionalities to work. If user click X button, they will go back to main menu

Fig. 3 *Storyboard of BiologAR*

C. *Mobile Application Development*

Project development is a very crucial process in developing any kind of application because this phase would determine the success of the end product. In order to develop BiologAR mobile application, we as the developers need to have a thorough and organized plans, which includes considering several issues such as availability, accessibility, integration, and compatibility of the features and content. This is because some features are compatible with different software and can be integrated into one another, while some are not.

In this project, the development process involves both front-end and back-end processes where the front-end consists of the user interface and illustration, digitizing 2D/3D art and scenes. While the back-end process consists of configuration, authoring and coding.

For front-end, we used a few tools to develop some of the components and media for the application which includes Adobe Illustrator and Adobe Photoshop for some illustration and user interface. For back-end coding, we use Unity3D for 3D Model development and Vuforia for AR technology and development.

1) *Digitizing 2D/3D Art*

The background, illustrations, 2D sprite or models for the user interface were done using software such as *Adobe Photoshop* and *Adobe Illustrator (see Fig. 4)*.

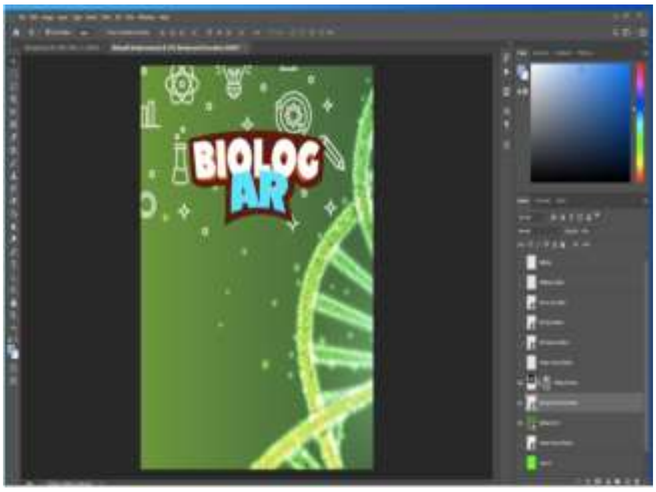


Fig. 4 Designing 2D user interface in Photoshop 2020

As for 3D models and animation, they were done by using *Blender* software. Fig. 5 below shows example of 3D modelling in *Blender 2.8*. As digitizing 2D and 3D art was done in different software, the format for the end product is different from one another. Thus, we exported the raw files into the same format for ease of use.

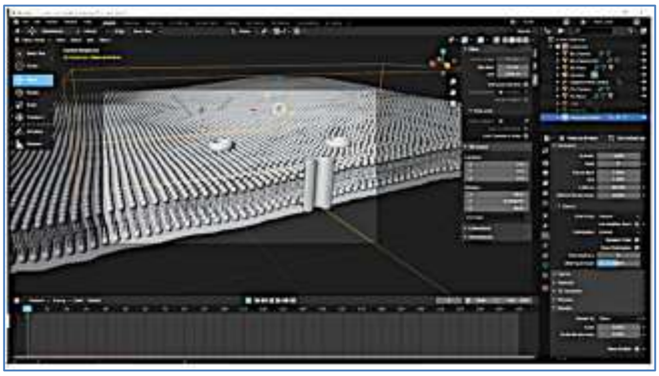


Fig. 5 *3D Modelling in Blender 2.8*

2) *Digitizing Scenes*

Apart of 2D and 3D digitization, the front-end process also includes digitizing scenes. The scenes include the main screen, selection screen, controller, and camera user interface. The process to create every scene according to the storyboard was done using *Unity 2020* software (*see Fig.* 6).

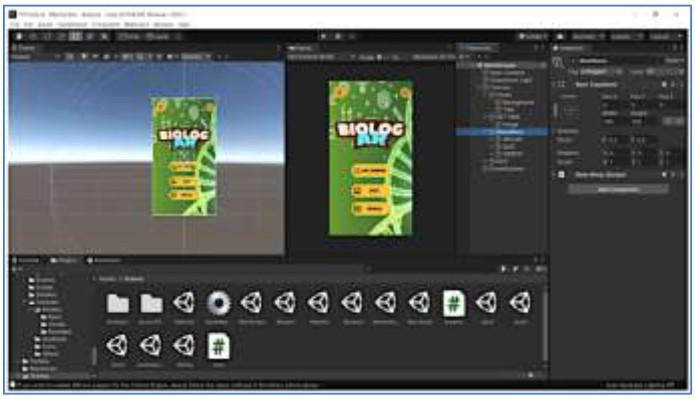


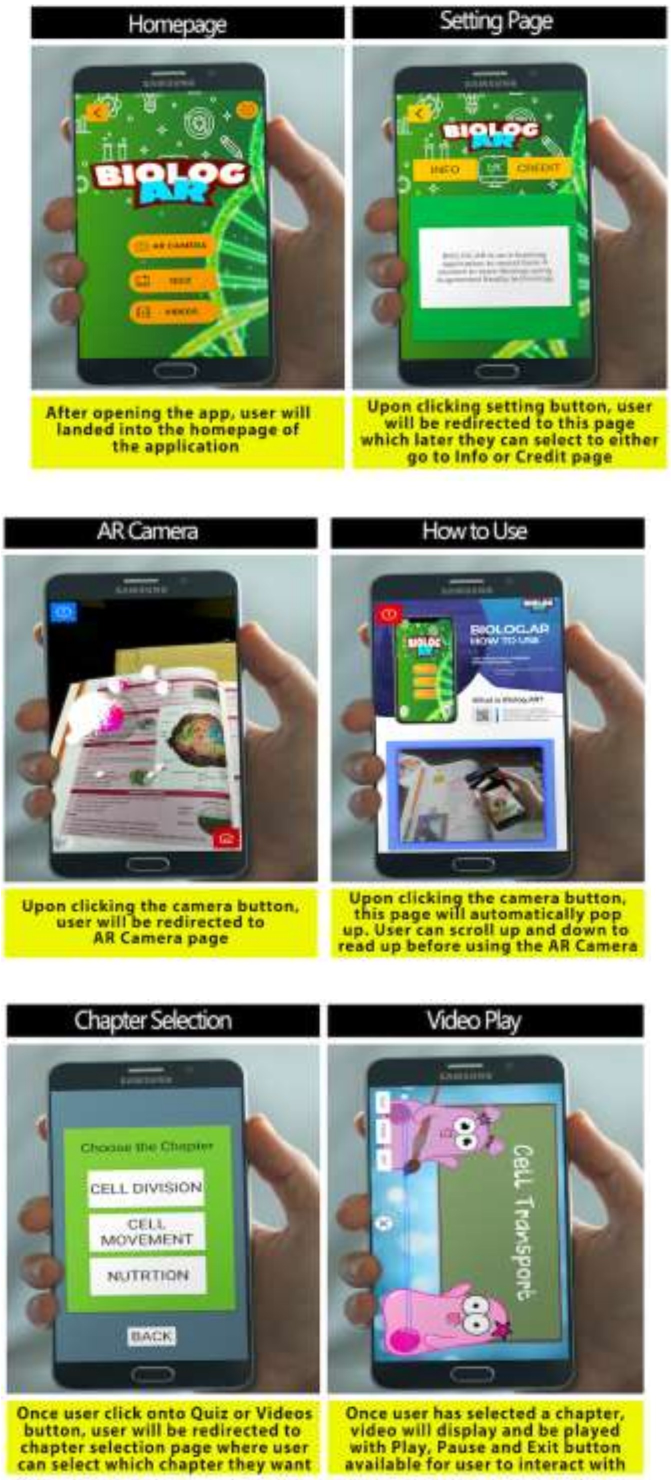
Fig. 6 *Software development in Unity 2020*

3) *Authoring*

In the later stages, the back-end development was done where some implementations and coding were programmed and tested. Rapid testing was done during the development to handle some errors and bugs. At this stage, the user interfaces already have their own programmable functions. Each function was tested before we moved into further development. We tested the functionalities of the product to detect any issues or problems before we deploy the real end product.

D. Implementation

Once the application has been completed, we have decided to deploy the end product on Android platform and upload it on the Google Playstore for commercial use. However, since the BiologAR have not reach commercialization level yet at the moment, we choose to share the Android Application Package (APK) using Google Drive. This APK can be installed on most Android smartphones that use Android 4.4 or Android 'KitKat' and higher. The following Fig.7 shows the users interfaces (UIs) of the BiologAR mobile application after the development have been completed.



Homepage

After opening the app, user will landed into the homepage of the application

Setting Page

Upon clicking setting button, user will be redirected to this page which later they can select to either go to Info or Credit page

AR Camera

Upon clicking the camera button, user will be redirected to AR Camera page

How to Use

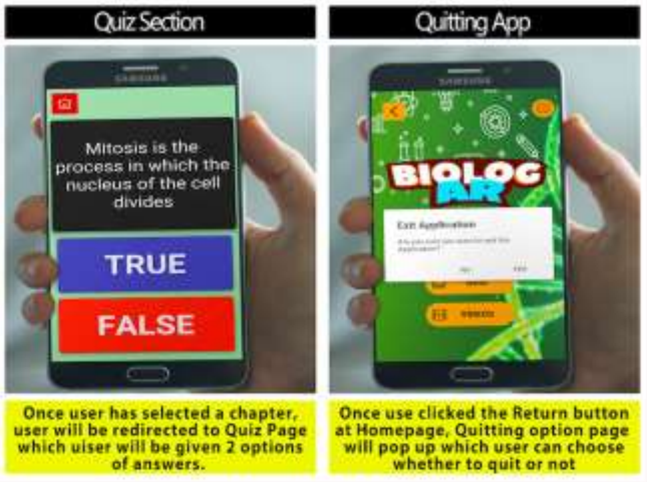
Upon clicking the camera button, this page will automatically pop up. User can scroll up and down to read up before using the AR Camera

Chapter Selection

Once user click onto Quiz or Videos button, user will be redirected to chapter selection page where user can select which chapter they want

Video Play

Once user has selected a chapter, video will display and be played with Play, Pause and Exit button available for user to interact with


Mitosis is the process in which the nucleus of the cell divides
TRUE
FALSE
BIOLOG AR
Exit Application

Quiz Section

Once user has selected a chapter, user will be redirected to Quiz Page which uiser will be given 2 options of answers.

Quitting App

Once use clicked the Return button at Homepage, Quitting option page will pop up which user can choose whether to quit or not

Fig. 7 *The user interfaces (UIs) of BiologAR application*

E. *Usability Testing Session*

It is very important to conduct usability testing of the BiologAR application with end users (students and teachers) to evaluate whether the application is easy and effective to use as assisting tool for learning Biology. Besides, it would also inform the developers on potential improvement that could be made to enhance the functionality and usage of the application.

For this purpose, we have conducted a series of Usability Testing session swith five (5) participants comprising of four Form 4 students who are studying Biology and one teacher teaching Biology subject to evaluate the usability of our BiologAR mobile application. Although the number of participants in this study is few, but according to Nielsen [14], a minimum of five participants is already sufficient to identify 85% of usability problems.

In the beginning of the usability testing session, participants were asked to fill up a set of questions asking about their demographic details. Then, a list of tasks was given to participants in order to ensure they interact with each feature of BiologAR. A total of nine tasks were given to participants to complete which are; 1) navigate through the application, 2) run the augmented reality camera, 3) answer the quiz, 4) play and watch the video, 5) display the 3D model in AR environment, 6) control the video (play, pause, exit), 7) go back to the recent page, 8) exit the application, and 9) control and move the 3D model in AR environment. After the participant completed all the tasks, a post-test usability testing questionnaire were administered to get participants feedback on each feature of BiologAR they interact with.

IV. RESULTS AND DISCUSSIONS

The following Table 2 summarized the participants' feedback as they interact and completed the given tasks on BiologAR mobile application.

TABLE II
PARTICIPANTS FEEB ON BIOLOG.AR FEATURES

Tasks	User Feedback
1. App navigation	*P1:* Everything displayed on the apps are simple, I had no problem going through the apps.
	P2: No problem to navigate
	P3: I can navigate through the application
	P4: Easy to understand the navigation
2. Run the augmented reality camera	*P1:* The camera works fine with the 3D models displayed in it
	P2: Can run the camera
	P3: The camera is working
	P4: Camera is okay
3. Answer the quiz	*P1:* Questions provided are suitable for students, not too easy and not too hard
	P2: The sound produced when answering the quiz makes the quiz more interesting.
	P3: The quiz does not have scores. Maybe having scoring feature will make it more interesting.
	P4: Only true or false quizzes available. Multiple choice quizzes can make it harder.
4. Play and watch the video	*P1:* The video can be played with no problem.
	P2: I can play the video with no problem.
	P3: I can open the video.
	P4: The video is playable.
5. Display 3D model in AR environment	*P1:* All 3D models are designed similar towards the actual model which is pretty impressive.
	P2: Every 3D models inside the apps can be viewed after I scanned the picture.
	P3: The AR can only be displayed if the camera is directed to the image. It is gone if the camera is not directed to the image.
	P4: The 3D model can be displayed. Some audio explanation or marker on the model could help.
6. Control the video (play, pause, exit)	*P1:* I can play, pause and stop the video easily as they are buttons which allow me to do so.
	P2: This feature is really helpful to watch videos
	P3: The control is not that smooth. No time frame displayed.
	P4: The video can be played. Only playtime not displayed.
7. Go back to the recent page	*P1:* The back button is really handy to be used to return to the previous page.
	P2: Back button looking simple, easy for me to recognize what it is for
	P3: I can go back and forth on any page
	P4: Easy, very straightforward.
8. Exit the application	*P1:* No problem exiting the apps.
	P2: I can exit with no problem
	P3: I can exit the application
	P4: Can exit using the app exit button only, cannot exit using phone back button.
9. Control and move the model in AR environment	*P1:* I can interact with the 3D models
	P2: I can zoom in and zoom out the 3D models
	P3: The 3D model can only be scaled up and down. The animation cannot be controlled.
	P4: 3D model can be moved around and scaled but only on the image plane.

Besides that, we also asked the participants to give score from 1 (poor) to 5 (excellent) in terms of ease of use, attractiveness of the user interface, ease of navigation, user friendliness, content of the application, and overall satisfaction. The result is summarized in the following Table III.

TABLE III
AVERAGE SCORE GIVEN BY THE PARTICIPANTS

Criteria	Score (average)
Ease of use	4.5
Attractiveness of the UI	4.0
Ease of navigation	4.75
User friendly	4.25
Content of the application	3.75
Overall satisfaction	4.5

Based on the above Table III, participants rated ‘ease of navigation’ with the highest average score of 4.75 indicating our BiologAR is indeed easy to navigate. In addition, in terms of ‘ease of use’, ‘attractiveness’ and ‘user friendly’, a satisfactory average score of 4.5, 4.0 and 4.25 respectively, also had been received.

However, although the participants gave an average score of 4.5 for ‘overall satisfaction’, in terms of the content of the application, participants gave slightly lower average score with only 3.75. The participants further suggested to improve the app with more attractive and sleek user interface design.

The importance of usability, ease of navigation, attractiveness, and good user interface design in AR applications have been consistently highlighted in several previous studies. Kim et al. [7] for example emphasize that AR applications need to be intuitive and straightforward to ensure that users can quickly learn and operate them without confusion. Research has shown that factors such as learnability and simplicity are critical for user engagement and satisfaction.

A recent study by Nikou [8] similarly found that if students find the AR tools intuitive and user-friendly, they are more likely to engage with the technology and benefit from its educational potential.

In terms of ease of navigation, Santos et al. [9] emphasize that efficient navigation is very crucial for users to move through the AR environment seamlessly, as any issues such as the arrangement of on-screen markers and clarity of visual cues can significantly impact the user experience. Additionally, AR applications that incorporate immersive and interactive design elements not only enhance learning outcomes but also increase student motivation, engagement, and curiosity, which are crucial for effective learning process [10].

Attractiveness of the AR application user interfaces also plays a crucial role in enhancing user engagement – particularly for students. Aesthetic elements such as color schemes, layout design, and graphical components must be carefully designed to enhance the overall user experience [7]. In fact, a study by Sathyapriya [11] found out there is a need for AR applications to be attractive to sustain student interest and improve understanding. Besides, an AR application that can transform traditional learning also must be interactive and engaging, to sustain student motivation and retention.

Further, our usability testing participants also give several suggestions on how BiologAR could be improved. First, the 3D models could use some labeling and animation with audio explanation. According to Billinghurst et al. [12] , the inclusion of labels, animations, and audio explanations in AR applications will enhance the user experience by making complex 3D models more understandable and engaging.

Besides, our participants also suggest the BiologAR interfaces to be more intuitive. A systematic review by Ibanez and Delgado-Kloos [13] highlighted that the intuitiveness is indeed a critical factor for the successful adoption and effectiveness of AR in educational settings, as students should be able to focus on the content rather than struggling with the technology.

V. CONCLUSIONS

Students are having problems in understanding the Biology subject from the textbook alone because the textbook lacks of interactivity and visualization. Our BiologAR mobile application attempt to overcome this problem by visualizing some topics in the Biology syllabus using AR technology and 3D visualizations. The results show that participants found BiologAR mobile application to be easy to use, easy to navigate, user friendly and useful as assisting tool for learning Biology. However, some areas need to improve such as enhancing the 3D model figures, improving the attractiveness of the user interfaces, adding more interactive features in the quiz feature and include more contents in the future.

ACKNOWLEDGEMENT

We would like to thank teachers and students at SMKA Maahad Muar and SMK Tun Sulaiman Ninam Shah, Muar Johor for their advices, guidance, feedback and participation as respondents in this project.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] C. Weng, S. Otanga, S. M. Christianto, and R. J.-C. Chu, "Enhancing students' biology learning by using augmented reality as a learning supplement," *Journal of Educational Computing Research*, vol. 58, no. 4, pp. 747–770, 2020.

[2] A. Sorgo, "Scientific creativity: The missing ingredient in Slovenian science education," *European Journal of Educational Research*, vol. 1, no. 2, pp. 127-141, 2012. [Online].

Available: https://doi.org/10.12973/eu-jer.1.2.127

[3] W. De Silva, P. Naranpanawa, U. Hettihewa, P. Liyanage, U. Samarakoon, and N. Amarasena, "Science zone: An augmented reality based mobile application for science," in *Proc. 2nd Int. Conf. Advancements in Computing (ICAC)*, 2020, pp. 222-227.

[4] S. A. Chowdhury, "A mobile augmented reality and multimedia application for mobile learning," *International Journal of Digital Content Technology and Its Applications*, vol. 7, pp. 25-32, 2013.

[5] A. R. Pratama and L. L. Scarlatos, "The roles of device ownership and infrastructure in promoting e-learning and m-learning in Indonesia," *International Journal of Mobile and Blended Learning (IJMBL)*, vol. 12, no. 4, pp. 1-16, 2020.

[6] R. Romli, F. N. F. Mohd Wazir, and A. R. Singh, "AR Heart: A development of healthcare informative application using augmented reality," *Journal of Physics: Conference Series*, vol. 1962, 2021.

[7] U. Kim, Y. Wang, and W. Yuan, "Study on user-centered usability elements of user interface designs in an augmented reality environment," in *Virtual, Augmented and Mixed Reality. Design and Interaction. HCII 2020*, J. Y. C. Chen and G. Fragomeni, Eds., Lecture Notes in Computer Science, vol. 12190. Cham: Springer, 2020, pp. 95-105. [Online]. Available: https://doi.org/10.1007/978-3-030-49695-1_7

[8] S. A. Nikou, "Factors influencing student teachers' intention to use mobile augmented reality in primary science teaching," *Educational Information Technology*, 2024. [Online].

Available: https://doi.org/10.1007/s10639-024-12481-w

[9] C. Santos et al., "Guidelines for graphical user interface design in mobile augmented reality applications," in *Virtual, Augmented and Mixed Reality. VAMR 2016*, S. Lackey and R. Shumaker, Eds., Lecture Notes in Computer Science, vol. 9740. Cham: Springer, 2016, pp. 139-150. [Online]. Available: https://doi.org/10.1007/978-3-319-39907-2_7

[10] D. Velarde-Camaqui, R. Celaya-Ramírez, Y. Contreras-Fuentes, and Z. Sanabria, "Enhancing STEAM education through augmented reality: The EduAR open platform experience," *Frontiers in Education*, vol. 9, 2024. [Online]. Available: https://doi.org/10.3389/feduc.2024.1391803

[11] J. Sathyapriya, K. Vedavalli, and S. Sree, "Enhancing engagement and understanding in education using augmented reality," *Journal of Information Technology and Digital World*, vol. 6, no. 3, pp. 264-273, 2024.

[12] M. Billinghurst, A. Clark, and G. Lee, "A survey of augmented reality," *Foundations and Trends in Human–Computer Interaction*, vol. 8, no. 2–3, pp. 73–272, 2015. [Online].

Available: https://doi.org/10.1561/1100000049

[13] M. B. Ibáñez and C. Delgado-Kloos, "Augmented reality for STEM learning: A systematic review," *Computers & Education*, vol. 123, pp. 109-123, 2018.

[14] J. Nielsen, "How many test users in a usability study?" NN/g, Jun. 3, 2012. [Online]. Available: https://www.nngroup.com/articles/how-many-test-users/

https://doi.org/10.31436/ijpcc.v11i1.526

Surveys on the Security of Ethereum and Hyperledger Fabric Blockchain Platforms

Nik Nor Muhammad Saifudin Nik Mohd Kamal, Safwah Afiqah, Sara Khadeja, Aliya Nasuha, Wan Muhammad Haziq Nur Iman Wan Mohd Azman, Wan Zul Irfan Wan Zulkifli, Wan Shafiq Aiman Wan Anuar, Muhammad Faizul Isyraf Md Nazri, Ahmad Anwar Zainuddin*

Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Gombak, Malaysia.

*Corresponding author anwarzain@iium.edu.my

(Received: 16th December, 2024; Accepted: 29th December, 2024; Published on-line: 30th January, 2025)

Abstract—Ethereum and Hyperledger are two popular and well-known block chain platforms which represent two kinds of application differentiation. Ethereum is a decentralized platform that also allows DApps to operate on it; many of the conditions for performing functions on Ethereum's blockchain do not require permission to be granted, but smart contracts are available. On the other hand, the Hyperledger Fabric, an enterprise grade blockchain solution, provides the permission to access, update, and apply scalability, privatization, and mandatory access control mechanisms. Due to the decentralized nature and the capacity of performing smart contracts using Ethereum Virtual Machine (EVM), it has been used in a number of areas across the world in financial transactions and DApp. Hyperledger fabric, on the other hand, is pursuant to the permissioned network standards and is centred on providing the set of components that suffice the requirement of an enterprise thereby making it easier for the organization to build a blockchain, which is both highly scalable and security conscious. Several studies have explored Ethereum and Hyperledger Fabric in various contexts. From these studies, it explains how blockchain has the potential in increasing volume in various areas while enhancing its characteristics such as, openness, origin and audibility. Analysing the concrete features of the Ethereum and Hyperledger Fabric platforms, it is almost obligatory for the companies interested into the implementation of the blockchain technology to understand the possibilities offered by one system and the drawbacks some complexity or singularity of the other. That is why, the features of each platform are distinctive and could be utilized for the development of business processes in specific spheres when designing problem-solving approaches.

Keywords— IoT, Blockchain, Ethereum, Hyperledger, Security, Interoperability

I. Introduction

Ethereum and Hyperledger Fabric are two prominent blockchain platforms that have significantly impacted the landscape of decentralized technologies. Ethereum, often considered a second-generation blockchain platform, stands out for its open and decentralized nature, enabling the development of Decentralized Applications (DApps) [1] . It has become a widely used financial application platform, with its native cryptocurrency, Ether, being one of the largest cryptocurrencies in terms of market capitalization [2] . Ethereum's smart contracts are tamper-proof, offering robust protection against attacks that aim to manipulate application execution flows [3].

On the other hand, Hyperledger Fabric is recognized for its focus on enterprise applications, providing a secure and scalable environment for executing smart contracts within secured Docker containers [4] . It emphasizes immutability, transparency, and cryptographic verifiability without the need for a single point of trust, thanks to its decentralized architecture [5]. Hyperledger Fabric has been explored for applications like resilient load balancing, demonstrating its potential for various use cases beyond traditional [6].

Both Ethereum and Hyperledger Fabric have been subjects of security assessments and surveys, highlighting the importance of understanding their vulnerabilities, attacks, and defences [7]. Researchers have delved into the security challenges faced by major blockchain applications, including Ethereum and Hyperledger, emphasizing the need for robust security and privacy techniques to safeguard blockchain-based systems [8]. Additionally, studies have focused on detecting fraudulent schemes like Ponzi schemes implemented as smart contracts on Ethereum, showcasing the importance of ensuring the integrity of blockchain applications [7].

In conclusion, Ethereum and Hyperledger Fabric represent two distinct yet influential blockchain platforms, each catering to different use cases and industries. While Ethereum excels in decentralized applications and cryptocurrency transactions, Hyperledger Fabric shines in enterprise applications and secure smart contract execution.

Understanding the nuances of these platforms is crucial for harnessing the full potential of blockchain technology in various domains.

This paper employs a systematic approach to explore the development and assessment of blockchain platforms for secure and efficient applications. Section I covers the background, fundamental concepts, and objectives of the research. Section II examines previous studies on blockchain technology, with a focus on its evolution, applications, and associated challenges. Section III delves into blockchain technology by highlighting the main features and architectures of Ethereum and Hyperledger Fabric. Section IV analyses the implications, comparisons, and potential applications of these platforms. Lastly, Section V concludes the study by summarizing its key findings and contributions to the blockchain field.

II. Literature Review

Several studies looked at blockchain within the context of IT; they examined security and compatibility of leading blockchains such as Ethereum and Hyperledger Fabric. His previous work [9] provides an assessment of one proposed use of blockchain for PHR, converses more on the usage of specific reference platforms like Ethereum and Hyperledger in related works. Similarly, [10] discussed permissioned DP block chain for private data sharing in Industrial IoT employing encryption strategies using Hyper ledger fabric to manage privateness concerns seasoned at consensus level.

[11] has outlined a reference model of supporting a Hyperledger Fabric to adopt which it asserted the need to deploy an EHR sharing system based on the Hyperledger composer. In addition, [12] utilized Hyperledger Fabric's simulation to determine the detailed aspects of performance and aspects of it.

Interoperability has also been aimed at in the blockchain sphere by employing interoperability solutions. [13] utilized yet another conventional gateway- based architecture for DLT cross boarding and claimed the message specification and created a concrete implementation on Hyperledger Fabric, and Ethereum. Furthermore, [14] also expounded on the actualization of the coupling process between the Ethereum, Hyperledger Fabric and the Tender mint blockchain via inter Blockchain communication.

More specifically in the field of healthcare several authors as discussed in this paper have used the blockchain for privacy-preserving frameworks. The following novels were also recently published: [15] describe a privacy-preserving health care system based on a blockchain implementation, known as Hyperledger Fabric; [16] discuss Health chain as use of blockchain-based solutions anonymous EHRs through which blockchain solutions can be adopted.

These research papers in combination with each other enable to gain precious information about several methods in security, interoperability and privacy of blockchain platforms, along with potential solutions that could enhance efficiency and effectiveness of blockchain systems.

TABLE I
COMPARATIVE ANALYSIS OF BLOCKCHAIN APPLICATIONS IN VARIOUS DOMAINS.

Articles	Key Findings	Supporting Evidence	Strength and Limitations	Significance and Implications
[2]	Proposed a method for tracking Ethereum transactions using a temporal-amount snapshot multigraph approach.	Theoretical framework and validation through simulations.	Strength: Innovative tracking method. Limitation: Requires further real-world validation.	Enhances the ability to trace transactions in the Ethereum network, improving security and transparency.
[3]	Reviewed upgradeable smart contract patterns based on the Open Zeppelin technique.	Literature review of smart contract patterns.	Strength: Focuses on upgradeability. Limitation: Limited to Open Zeppelin patterns.	Provides insights into the design of more flexible and maintainable smart contracts.
[4]	Developed a recommender system leveraging blockchain and deep learning for reusing and recycling.	System design and empirical validation.	Strength: Integrates blockchain and AI. Limitation: Specific to recommender systems.	Demonstrates the application of blockchain and AI in creating efficient and secure recommender systems.
[17]	Explored blockchain applications, challenges, and research opportunities in supply chain operations.	Literature review and analysis of supply chain applications.	Strength: Broad coverage of supply chain issues. Limitation: Lacks empirical validation.	Provides a roadmap for future research and applications of blockchain in supply chain management.

[18]	Investigated blockchain's potential in biomedical and healthcare applications.	Review of biomedical applications.	Strength: Early exploration of blockchain in healthcare. Limitation: Outdated, requires updates with new findings.	Sets the foundation for blockchain applications in biomedical and healthcare sectors.
[19]	Explored the integration of blockchain and AI in e- health applications.	Review and analysis of e-health applications.	Strength: Combines blockchain with AI. Limitation: Specific to e-health applications.	Highlights the synergies between blockchain and AI in enhancing e-health services.
[20]	Proposed a blockchain-based architecture for managing distributed renewable energy resources.	Gap analysis and proposed architecture.	Strength: Practical application in energy management. Limitation: Requires real-world validation.	Enhances renewable energy management through a blockchain-based approach.
[21]	Comprehensive survey on the evolution, architecture, and security of blockchain technology.	Literature review and analysis.	Strength: Broad and comprehensive coverage. Limitation: High-level overview, lacks specific focus.	Offers a detailed overview of blockchain's evolution, architecture, and security aspects.
[22]	Surveyed blockchain applications in business and finance in Vietnam.	Case studies and literature review.	Strength: Specific regional focus. Limitation: May not generalize globally.	Provides insights into how blockchain is being adopted in business and financial sectors in Vietnam.
[23]	Proposed a DNS cache resources trusted sharing model based on consortium blockchain.	System design and validation through simulations.	Strength: Practical DNS sharing model. Limitation: Requires further scalability testing.	Enhances the security and reliability of DNS cache resource sharing through a consortium blockchain model.
[24]	Surveyed various consensus mechanisms used in consortium blockchains.	Literature review and comparative analysis.	Strength: Comprehensive survey of consensus mechanisms. Limitation: General overview, lacks specific focus.	Provides a detailed comparison of different consensus mechanisms for consortium blockchains.
[25]	Proposed a consortium blockchain framework for remote health monitoring.	System design and case study analysis.	Strength: Specific focus on remote health monitoring. Limitation: Needs real-world validation.	Enhances the reliability and security of remote health monitoring systems through consortium blockchain.
[26]	Proposed a service for immutable log storage on both private and public blockchains.	System design and theoretical analysis.	Strength: Versatile log storage solution. Limitation: Needs practical implementation and testing.	Provides a framework for secure and immutable log storage across different blockchain platforms.
[27]	Reviewed various consensus algorithms used in blockchain technology.	Literature review and comparative analysis.	Strength: Broad overview of consensus algorithms. Limitation: High-level review, lacks in-depth analysis.	Provides a comprehensive overview of consensus algorithms, guiding future research and development efforts.
[28]	Reviewed privacy-preserving technologies in blockchain systems.	Literature review and comparative analysis.	Strength: Focus on privacy- preserving techniques.	Provides insights into various privacy-preserving techniques, guiding the development

			Limitation: Primarily theoretical, needs practical applications.	of more secure blockchain systems.
[29]	Developed a web archiving system that preserves content integrity using blockchain.	System design and empirical validation.	Strength: Practical web archiving solution. Limitation: Focused on web content, needs broader application testing.	Enhances the integrity and reliability of web archiving systems through blockchain technology.
[30]	Explored the use of blockchain and smart contracts for managing higher education records in Brazil.	System design and case study analysis.	Strength: Practical application in education. Limitation: Focused on a specific use case.	Demonstrates the potential of blockchain in improving the management and security of higher education records.
[31]	Proposed a high-performance hybrid blockchain system for traceable IoT applications.	System design and empirical validation.	Strength: Practical IoT application. Limitation: Needs further scalability testing.	Enhances the traceability and performance of IoT applications through a hybrid blockchain approach.
[32]	Proposed an enhanced method for detecting P2P botnets through network-flow level community behaviour analysis.	Theoretical framework and empirical validation.	Strength: Effective botnet detection method. Limitation: Needs further real-world validation.	Improves the detection and mitigation of P2P botnets in network systems.
[33]	Analysed threats and security issues in mobile peer-to-peer networks.	Threat analysis and evaluation framework.	Strength: Detailed threat analysis. Limitation: Specific to mobile P2P networks.	Provides a comprehensive threat analysis for securing mobile peer-to-peer networks.
[34]	Developed a decentralized electricity market model with prosumer-centric coordination and grid security.	System design and simulation validation.	Strength: Practical electricity market model. Limitation: Needs real-world implementation.	Enhances the coordination and security of decentralized electricity markets through blockchain technology.
[35]	Proposed a new chaotic encryption model using diffractive techniques.	Theoretical development and validation through simulations.	Strength: Innovative encryption model. Limitation: Needs practical implementation.	Introduces a new encryption model that enhances data security through chaotic techniques.
[36]	Developed a data integrity auditing mechanism for secure cloud storage using Hyperledger Fabric.	Designed and tested auditing mechanisms; empirical validation with performance metrics.	Strength: Improved data integrity mechanisms. Limitation: Focus on cloud storage, may not address other security concerns.	Enhances the security of cloud storage systems using Hyperledger Fabric, ensuring data integrity.
[37]	Investigated the feasibility of Proof of Authority as a consensus protocol model.	Theoretical analysis and simulation validation.	Strength: Focus on Proof of Authority. Limitation: Needs real-world testing.	Provides insights into the feasibility and efficiency of Proof of Authority as a consensus protocol.
[38]	Empirical analysis of Ethereum's gas mechanism and its implications for network performance.	Collected and analysed data on gas usage in Ethereum.	Strength: Empirical data analysis. Limitation: Focus on gas mechanism, may not address other aspects of Ethereum performance.	Offers insights into the efficiency and potential improvements of Ethereum's gas mechanism.

[38]	Proposed a secure and efficient Delegated Proof of Stake consensus algorithm with a downgrade mechanism.	Theoretical development and empirical validation.	Strength: Innovative consensus algorithm. Limitation: Needs further practical validation.	Enhances the security and efficiency of Delegated Proof of Stake consensus algorithms.
[39]	Developed a node selection algorithm for consortium blockchains using a genetic method based on PBFT.	System design and simulation validation.	Strength: Effective node selection method. Limitation: Specific to PBFT consensus.	Improves node selection efficiency and reliability in consortium blockchains using a genetic algorithm.
[40]	Proposed a resource slicing model for blockchain consensus in real-time distributed energy trading.	System design and simulation validation.	Strength: Innovative consensus model. Limitation: Needs further real-world validation.	Enhances the efficiency and reliability of blockchain consensus in energy trading systems.
[41]	Explored blockchain's role in facilitating inter-organizational collaboration, specifically in healthcare during COVID-19.	Case studies of healthcare providers using blockchain for collaboration during the pandemic.	Strength: Timely and relevant case studies. Limitation: Focused on a specific use case, may not generalize.	Demonstrates the potential of blockchain for enhancing collaboration in crisis situations.
[42]	Proposed a formal model for ledger management systems based on contracts and temporal logic.	Developed formal models and provided theoretical proofs.	Strength: Strong theoretical foundation. Limitation: Lack of practical implementation and testing.	Provides a theoretical basis for developing more robust ledger management systems.
[43]	Conducted a systematic review of security vulnerabilities in Ethereum smart contracts.	Analysed various security vulnerabilities through literature review.	Strength: Comprehensive overview of vulnerabilities. Limitation: Lacks new empirical data.	Provides a detailed understanding of common security vulnerabilities in Ethereum, guiding future security improvements.
[44]	Developed visualization techniques for Ethereum's peer-to-peer network topology.	Utilized network analysis tools; visualized Ethereum's P2P network.	Strength: Improved understanding of P2P network structure. Limitation: Visualization focused, may not address other network issues.	Enhances understanding of Ethereum's network structure, aiding in network optimization and security.
[45]	The study introduces a system combining blockchain and machine learning to improve cybersecurity by detecting intrusions more accurately and ensuring data integrity.	The system uses blockchain for secure data sharing and machine learning to identify threats. Simulations validate its performance.	Strengths: Enhanced detection accuracy, robust data integrity, collaborative threat detection. Limitations: Computational complexity, scalability concerns.	This hybrid IDS model offers a promising solution for securing sensitive data and detecting cyber threats in real-time, potentially transforming cybersecurity practices.
[46]	Developed methods for detecting illicit accounts on the Ethereum blockchain.	Utilized machine learning techniques; tested on Ethereum transaction data.	Strength: Advanced detection techniques. Limitation: Requires large datasets and may not detect all types of illicit activities.	Improves the ability to detect and mitigate fraudulent activities on the Ethereum blockchain.
[47]	Evaluated the effect of the uncle block mechanism on selfish and stubborn mining in Ethereum.	Theoretical analysis and simulations of uncle block effects.	Strength: Addresses a specific mining strategy issue. Limitation: Primarily theoretical, requires empirical validation.	Provides insights into improving Ethereum's mining strategies and security.

[48]	Proposed a blockchain-based architecture for secure IoT-based health monitoring systems.	Designed and tested the architecture; empirical evaluation in health monitoring scenarios.	Strength: Practical application in health monitoring. Limitation: Specific to health monitoring, may not generalize.	Enhances the security and reliability of health monitoring systems using blockchain technology.
[49]	The article discusses the development of AppxChain, a platform designed to facilitate application-level interoperability among different blockchain networks. It argues that seamless communication and data exchange are essential for enhancing the scalability and utility of blockchain technology.	The article provides insights into AppxChain's architecture and functionalities, demonstrating its ability to enable communication between various blockchains such as Ethereum, Hyperledger Fabric, and Binance Smart Chain. The methods used likely include descriptive explanations of AppxChain's features and potential use cases.	Strength:AppxChain's innovative approach focuses on application-level interoperability, enhancing collaboration and innovation in blockchain applications. Limitation: Technical challenges may arise in implementing and maintaining interoperability across diverse blockchain networks.	The article's findings have significant implications for the future of blockchain technology, as AppxChain's interoperability features can mitigate fragmentation, improve scalability, and encourage cross-platform collaboration. These outcomes could accelerate innovation and utility in industries relying on blockchain applications.
[50]	The article reviews the concept of Digital Twin (DT), highlighting its definitions, key characteristics, and various applications across industries. It emphasizes the potential of DT in improving system design, monitoring, and maintenance.	The authors conduct a comprehensive literature review to classify and analyse existing DT definitions, applications, and design frameworks.	Strengths: Broad coverage of DT concepts, identification of key characteristics, extensive application examples. Limitations: Evolving field, varying definitions may cause inconsistencies.	This survey provides a foundational understanding of DT, aiding researchers and practitioners in leveraging DT for innovative solutions in system optimization and predictive maintenance.
[51]	Presented Hyperledger Fabric as a distributed operating system for permissioned blockchains.	In-depth architectural analysis of Hyperledger Fabric.	Strength: Comprehensive architectural overview. Limitation: May be too technical for non-specialists.	Offers a detailed understanding of Hyperledger Fabric’s architecture, aiding developers and researchers.
[52]	Reviewed the application of Hyperledger Fabric in IoT contexts.	Surveyed existing literature and case studies on Hyperledger Fabric implementations in IoT.	Strength: Comprehensive literature review. Limitation: Limited new empirical data.	Provides a broad overview of how Hyperledger Fabric can be utilized in IoT, guiding future implementations.
[53]	Proposed a blockchain-based framework for medical image sharing and critical-results notification using Hyperledger Fabric.	Developed and tested a framework; empirical testing in medical imaging scenarios.	Strength: Practical application in healthcare. Limitation: Specific to medical imaging, may not generalize.	Demonstrates the practical utility of Hyperledger Fabric in securely sharing medical data.
[54]	Proposed a private and trustworthy lending model using Hyperledger Besu.	Designed a new lending model; empirical validation in financial scenarios.	Strength: Practical application in finance. Limitation: Specific to lending, may not generalize to other financial services.	Enhances the security and trustworthiness of financial lending services using blockchain.

[55]	Developed an AI-enabled consensus protocol for blockchain-based IoT networks.	Applied AI techniques to consensus protocols; tested in IoT scenarios.	Strength: Innovative use of AI for consensus. Limitation: Computationally intensive, requires significant resources.	Improves the efficiency and security of consensus protocols in blockchain-based IoT networks.
[56]	The article proposes a framework for efficient clinical data sharing using blockchain technology to ensure data security, integrity, and interoperability.	The framework is validated through a combination of theoretical analysis and simulation experiments. It involves the use of blockchain to create a decentralized and immutable ledger for clinical data transactions.	Strengths: Enhanced data security and privacy, improved interoperability, and reliable data sharing. Limitations: High computational costs and potential scalability issues.	This framework can revolutionize clinical data sharing by providing a secure, transparent, and efficient method for managing patient records, potentially improving healthcare outcomes.
[57]	The article explores how integrating multiple blockchain ledgers can improve control and security in IoT systems. It discusses the use of interledger technologies to facilitate secure and efficient interactions between different blockchain networks.	The authors propose a framework for combining various blockchain ledgers, emphasizing interoperability and security. They validate their approach through use case scenarios and performance evaluations.	Strengths: Enhanced security, improved control, and flexibility in IoT applications. Limitations: Potential complexity in implementation, need for robust interoperability standards.	This approach can significantly enhance IoT systems' security and efficiency by allowing better control over multiple interconnected blockchain networks.
[58]	The article discusses the development of a blockchain-assisted patient-owned system for electronic health records (EHRs), emphasizing the potential benefits of blockchain technology in enhancing data security, privacy, and patient control over their health information.	The authors likely conducted a comprehensive review of existing literature on blockchain applications in healthcare and electronic health records. They may have also presented case studies or prototypes demonstrating the feasibility and effectiveness of their proposed system.	Strength: The article's strength lies in its innovative approach to leveraging blockchain technology to empower patients with greater ownership and control over their EHRs, potentially improving data integrity and patient outcomes. Limitations: Potential challenges may include technical complexities in implementing blockchain- based EHR systems on a large scale, as well as regulatory and privacy concerns that need to be addressed for widespread adoption.	The findings of this article have significant implications for the healthcare industry, as a blockchain-assisted patient-owned EHR system could enhance data security, privacy, and patient engagement. This could lead to improved healthcare outcomes, reduced medical errors, and increased trust between patients and healthcare providers.
[59]	The article surveys blockchain interoperability, highlighting past efforts, current methods, and future trends. It identifies three main categories: cryptocurrency-directed	The authors reviewed 332 documents, analysing 80 in detail to classify and discuss various interoperability approaches.	Strengths: Comprehensive overview, systematic classification. Limitations: Fragmented knowledge, evolving standards.	This work provides a foundation for future research, emphasizing the importance of interoperability for blockchain technology's growth.

	approaches, blockchain engines, and blockchain connectors.			
[60]	Improved key management in LoRaWAN networks using permissioned blockchain.	Developed a blockchain-based key management scheme; tested in LoRaWAN scenarios.	Strength: Enhances security in IoT networks. Limitation: Specific to LoRaWAN, may not generalize to other networks.	Strengthens IoT network security through improved key management techniques.

III. Overview of Blockchain Technology

A. Functioning

In Figure 1, explained the foundation of blockchain was laid using Bitcoin in 2009, but a lot of changes have been observed in the modern blockchain platforms that provide secure, transparent and efficient solutions in various domains. They discovered that in the context of the supply chain logistics of blockchain technology has been considered as an opportunity to advance the opportunity and manage the challenges and new research areas [17]. Therefore, it has found application in supply chain management solving areas because it enhances visibility, audibility, and security of products in supply chains [18].

In healthcare, the application of the blockchain technology is where it can used to observe the future that it would bring into management of data and its security and ability to interconnect. Advantages in biomedical or health care domains include better security of information, better documentation and relative higher levels in terms of database handling as against normal databases [18]. Further, and as discussed briefly above, blockchain has been considered for IoT as a solution for the creation of a distributed ledger that could upgrade the communication and information exchange readily [61].

An effort has been made to contextualize blockchain in e-Health cooperated with AI performance, opening possibilities of enabling effective and patient-centric healthcare. The study found out that problems like scalability, interoperability and regulatory issues are some of the concerns that may hinder large scale implementation [19]. However, overcoming these challenges can open numerous opportunities for using blockchain technology as a decentralized and safe platform for various purposes, for instance, supply chain management in the healthcare sector, collaborative and project-based healthcare initiatives, and state-supported patient-oriented projects [62].

In conclusion, the use of blockchain technology is still advancing and penetrating essence to various industries to come up with solution-facilitating solutions. Blockchain must be warmly welcomed for its ability to bring innovative disruptive solutions to institutions, improve managing data systems, and advance collaborative societal causes and missions.

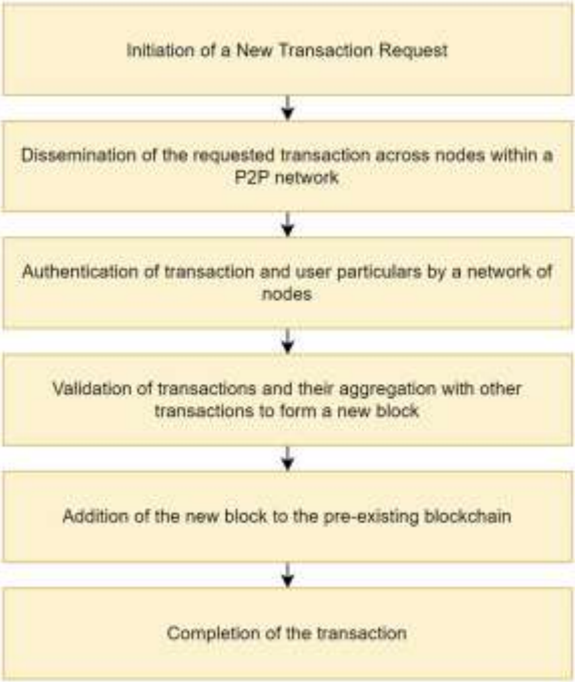

Initiation of a New Transaction Request
Dissemination of the requested transaction across nodes within a P2P network
Authentication of transaction and user particulars by a network of nodes
Validation of transactions and their aggregation with other transactions to form a new block
Addition of the new block to the pre-existing blockchain
Completion of the transaction

Fig. 1 An overview of blockchain flow

B. Classification of Blockchain Technology

1) Public Blockchain

In Figure 2, explained the simplified blockchains or centralized blockchains are some of the original concepts of blockchains that allow the visitors to the same system to have full control over the chain. They are the anonymous messaging type where no one requires authorization to subscribe, provide/forward information or endorse the transactions. Every transaction that will take place within the network has to be well understood by other people within that same network, since as mentioned earlier, within public blockchains everyone and anything is transparent and therefore, has to be answerable.

In the words of [20], the term is used to repeat the fact that it is possible to open it to the public and they congregate around features that are public as well as opened. Similarly, [21] has also discussed the differentiation between public and private blockchains in terms of the fact that in public blockchain everyone has the ability to join the network of the respective blockchain network and even participate in the process of validation of the blocks in order to make consensus along with decentralizing the network.

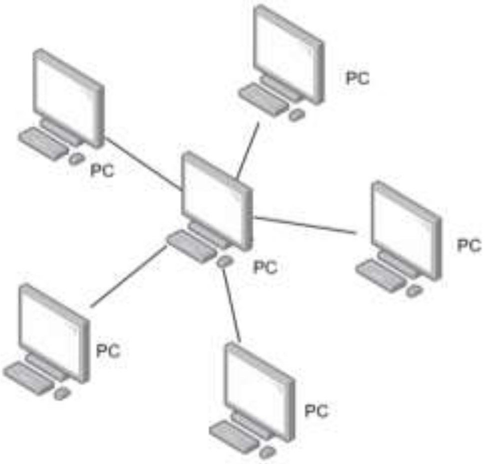


Fig. 2 Example of Public Blockchain

In addition, [22] continue with the elaboration on the features of the permission less or public blockchains they argue that they are clear records meaning that the records are accessible by anyone and one can join the network at any given time. This open-accessing ensures that the blockchain is more secure and less likely to be an entry point for hackers to attack as more people will be adding to the size and complexity of the book.

Hence the adoption of public blockchains in the pursuit of these goals of transparency, decentralization and most importantly, trust within the blockchain participants. The open and permission less nature of two layers demonstrates that it is possible to facilitate a high number of participants to be involved in consensus to validate a number of different transactions and in the process enhancing the security of the entire Blockchain solution.

2) Private Blockchain

In Figure 3, explained the other categories of DLT may incorporate private distributed ledgers also known as enterprise blockchains and compliance with lawful standards including data security regulation GDPR [63]. The interference of third parties on the transactions or records which they have no right to do so is also true with private key blockchains since there are no governing bodies or owners who are always hungry to manipulate or delete entries on the chain. This kind of control is extremely stringent because only particular consensus algorithms can be employed, and the model will function strictly as wished by the governments behind it.

Moreover, except for various or public blockchains, the values of data are only accessible to members/fixed or selected only [64]. Regarding the node access feature in the private blockchain, only specific individuals who are allowed to gain access to the platform are the only ones who can access it, and this can be considered as efficient in terms of limiting the number of nodes that can access a given system. In contrast to all such traditional electronic databases this access prevents or restricts the dissemination of information within the blockchain network that provides a higher level of protection for the data that is being exchanged in the network; this is acceptable for those cases only where such exchange in the information is limited only to only a few parties.

By extension, permission-based or private ledgers involve a limited and confined network with well-established gates or walls for the players. These blockchain networks have fairly well-developed self-organization and anonymity that are necessary and sufficient for applications that allow limited data exchange and compatibility with different legal rules and requirements.

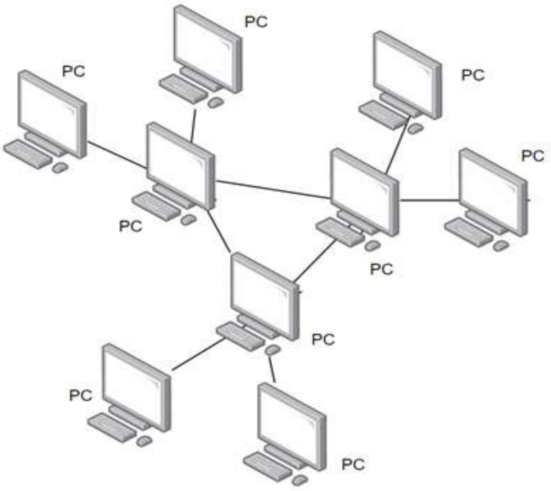


Fig. 3 Example of Private Blockchain

3) Consortium Blockchain

In Figure 4, explained the consortium block chain also known as an enterprise block chain is a type of private block chain whereby the block chains are developed with the collaboration of several organisations in a consortium manner. To some extent, these blockchains are open, enabling crossover between the public and private blockchains although not exactly [65]. Finally, in consortium blockchains people can join the participate only in case they belong to the consortium and the structure that defines the blockchain contains read, write, or participating permissions according to the rules of the consortium [23]. Such blockchains are often founded on decisions by some number of preselected clients from these organizations with consensus being the agreed choice. The overall goal of consortium blockchains is that, while some other set of organizations that are very relevant in the context of the given consortium and at the same time sufficiently decentralized, achieve some value added by cooperation. This notion called as 'partial decentralization' explains consortium blockchains in that only a few stakeholders manage the network [23]. Compared to the public blockchain, the consortium does not have the problem of supplying a resource that would support a demanding global consensus protocol [24].

All nodes are known and selected in a consortium Blockchain which greatly reduces the risk and opens up trusted and viable partnerships [25]. These blockchains are also similar to the public blockchains with a catch in which only the entered set of nodes involves the consensus part [26]. Thus, even though it remains unclear whether consortium blockchains will eventually be recognized and adopted on the global level, it becomes apparent that they seem to be more advantageous when it comes to the range of potential uses compared to private blockchains [27].

Therefore, consortium blockchains provide a consensus of the middle ground between the public and private distribution and the users with limited access to the blockchain database while making decentralization and transparency applicable in the consortium scenario.

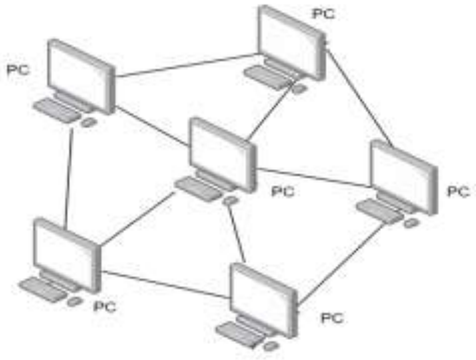


Fig. 4 Example of Consortium Blockchain

C. Classification of Blockchain Technology

Security is the immunization process given in the centre of the blockchain technology to safeguard against threats like unauthorized access, leakage of information, and unwanted revelation of privacy. It is also worth to emphasize that blockchain systems are developed targeting for many security aspects that potentially could help to protect from IT threats and risks.

According to [28], for the blockchain systems to have a reasonable level of security they need to have the following features: Randomness, the system cannot be replaced or modified, there are different users with different pseudonyms, the system is consistent, and the system is immune to DDoS and double spending.

Additionally, [29] proposed that blockchain has been considered to be a high-quality security system owing to its distinct security features, reviewing the security qualities that make it highly useful in averting cyber-risk and ensuring veracity of records.

Furthermore, [30] have supported that transactions within block-chain environment are secure, can always be relied on, unmodifiable thus could always be traced making these security provisions vital for facilitating the solidity and openness of block-chain activities.

Furthermore, [31] have pointed towards the fact private keys are essential to make Blockchain secure as it machines against identify forging attack stressing that those key must need to be secured so that nobody without permission can alter the transaction in the Blockchain ledgers.

Thus, it can also offer a number of protection mechanisms such as, data authenticity meaning that data within block chain cannot be manipulated, parties' immunity to deny having conducted a certain transaction, where necessary, parties' immunity to keep certain transaction information secret, bio availability, where necessary, and secure storage and encryption as well as access to keys which are evidence of existence of a secure platform to store data or perform a transaction.

1) P2P network

Security in P2P networks ensures message confidentiality, integrity, and accessibility. Recent studies address threats from physical addressing and highlight encryption's role in mitigating vulnerabilities, with growing interest in decentralized P2P network management.

[32], discuss on the P2P network structure and emphasize the use of physical addressing threats on the basis of diversification of physical network P2P connections. [33], also described a comprehensive security model of the impact of web threats that may be experienced by mobile P2P networks, limitations and types of network attacks that might be experienced as well as the measures such as encryption.

Further, it contains an overview of the still very much nascent research area of P2P-based Network Management (P2PBNM) with a clear focus on the use of P2P technology to further decentralize and secure basic network management architecture. [34], emphasize the importance of the grid security measures to the peer-to-peer (P2P Electricity Market) where the prosumers will be organized through the security measures deemed as being reflected in the tariff-based security and product discrimination.

Security in P2P networks is essential to mitigate threats arising from their decentralized and anonymous nature. Consequently, with the open-to-all all security for a P2P network in combination with other unification measures, as well as encryption and other threat avoidance measures, the risk of the overall range of threats in the form of cyber threats may be reduced to a negligible level, including through the regulation of the provision of access to the network.

2) Cryptography

Cryptographic security ensures that data is immutable and accessible only to authorized users, while verifying the authenticity of the information. Only a few of them are recent and they attempted to give some information on a variety of aspects related to security features and employments of cryptography.

[35], The authors employed the use of diffractive encryption as a subset of the chaotic encryption model and regarding diffuse sensitive issues pointed out the problems associated with the identification of initial conditions and control parameters and noted the essential feature of key sensitivity within the area of cryptology. [36] indicated that agility, decentralization, honesty, and verifiability were the four core values promoted by blockchain and cryptography.

In [66], the authors provided the assessment of the security aspects concerning quantum cryptography, and concerning the given work, the major focus had been paid to the understanding of the paradigms such as unconditional security and measurability of the Quantum Cryptography technique. [67], presented a new secret sharing encryption method which is based on the polarization sample feature, and proved that the current method was more secure and less complex in decrypting the encrypted information.

3) Smart contract

Certain functions must be coded into the smart contracts to allow specific types of transactions to occur while at the same time maintaining the security and secrecy of the transaction. The studies carried out in the past few years have brought about the following main areas that focus on aspects of security in smart contracts.

[68], defined the necessity of creating high-quality, efficient, and high-security codes while designing smart contracts because it is connected with the feature of the impossibility of alteration of the developed software codes after distribution on the blockchain net. Another thing that scholars [69] said is that there is a need to capture the international dimension in the dance of smart contract security and appears to be urging those who analyse smart contracts to have a broad view of contracts' flaws and lapses.

Some other works that are related to security aspects of quantum cryptography include other works that discuss the same or related issues. [70], discussed the question of unconditional security of quantum cryptography and the problem of making the eavesdropper's presence recognizable to enhance the degree of security protection. This is how a new polarization-based secret sharing encryption also featured in [71], adding extra security as well as a less complicated process of decryption, was created.

In other words, the security characteristics of smart contracts involve the quality of the smart contract code, international security issues, no direct reliance on the external environment, and a very complex algorithm to secure the datatype and transaction data to minimize the risks of the transaction.

4) Blockchain Consensus Algorithms

Consensus algorithms are the core facilitators of blockchains' reliability, security, and operational performance. [37] discusses the applicability of PoA as the consensus making protocol model to solve consensus issue in decentralized computing systems with assurance of correctness and security of the system. [38] also talk about the Delegated Proof of Stake with Downgrade as one of the safe and effective consensus algorithms of the blockchain network, mentioning that it's important to note that consensus algorithms are subjected to changes to fit the new needs.

[39] have developed the node selection algorithm based on genetic method in consortium blockchains that adopted Practical Byzantine Fault Tolerance (PBFT), another evolution in consensus mechanism. Further, [40] gives the real-time DE trading CRSM model to illustrate how consensus resource slicing greatly influences the blockchain system efficiency because of the consensus algorithms.

Therefore, it can be understood that consensus algorithms in Blockchain are critical for determining the nodes' consensus as well as security, reliability, and efficiency of Blockchain networks.

5) Power of Work (PoW)

The basic model used in many blockchains to check transactions and to add new blocks to the chain is Proof of Work consensus method. Pow assigns miners to solve complicated mathematical problems, hashes, related to the transaction addition to the blockchain. PoW algorithms make use of a difficult hash function, taking a lot of processing time to solve and hence successfully add a block to the chain. In the contest to obtain a solution first, the winner is that initial miner, which receives newly generated bitcoin.

6) Power of Stake (PoS)

The general process of operating on the blockchain networks involves use of a consensus mechanism called Proof of Stake (PoS), for approving operations as well as adding more chains blocks. Unlike PoW, which requires miners to solve complex problems, Proof intends to get random individuals to embed their computer's computational power into a hashing algorithm.

Proof of Stake (PoS) work on the basis of a set of tokens of a particular cryptocurrency, for example, Bitcoin, to receive new blocks and confirm transactions.

IV. Overview of Ethereum

A. Security Ethereum

One of the issues that has been explored in the Ethereum ecosystem is security; In fact, various papers have explored the vulnerability, threat, and countermeasure that exists in the Ethereum domain. Of the components that make up Ethereum has smart contracts been investigated because of their security(discuss)mostly because they handle large amounts of cryptocurrencies which else would have notable monetary value and become ideal bait for an attacker [72]. The current study also reveals that new weakness has been found in the smart contracts of Ethereum hence the need to apply proper security measures that would avoid these areas being exploited [72].

Nonetheless, because Ethereum has become more and more complex over time and evolves at a high rate, it is critically important to get constant expert feedback and adhere to strict SSDLC not to encounter such issues at the protocol level, such as replay attacks or some shortcomings of using elliptic curve cryptography that provides only partial forward secrecy [73]. As the described ecosystem does not have central points of control and management, and is constantly developing, then the analysis and monitoring should be continuous to ensure that the transactions are protected from hacking and that the fulfillment of smart contracts is correct [73].

Furthermore, Ethereum an open-source distributed computing engine designated famous for smart contract attracted investors researchers' and attackers since it hosts the decentralized application (Dapps) [74]. This makes it possible to develop Dapps not only in the field of financial transactions but also it creates a basis for creating many applications for the platform environment of [74], [75]. The current threats in the ethereal domain have shaped the research on the anomaly detection systems, which conduct intrusion detection mechanisms to eliminate the threats [76].

Hence, one can presume that the aspect of security in Ethereum has multiple problems and concerns, which include threats to smart contracts, threats to the Ethereum networks, and an important aspect that has to do with the constant emergence of new threats and the subsequent improvement of current security measures. Haven broadly and susceptibly, Ethereum and its partitions continue to be maintained by academics and professionals in respect to the specific security aspects of Ethereum and in respect towards the methods that render it secure for protecting users' and their trade's assets.

B. Main Benefits of Security Ethereum

More recently, certain factors have been made different from one another, that can account for the observed gain of Security in Ethereum. Privileged benefit is the ability to execute smart contracts securely through reliance on Ethereum's blockchain. When executed, smart contracts on Ethereum operate within a context known as the Ethereum Virtual Machine, EVM, which regulates consensus and security in the system [76]. Compared to typical smart contract execution mechanisms, this secure one is a solid foundation for many purposes, including financial and other safe transactions and DApps [76].

Furthermore, if using Ethereum or other blockchain techniques, IoT applications have been introduced to enhance the security parameter. From the perspective of the literature review, the blockchain can solve security issues of IoT including confidentiality, integrity, availability, authentication, authorization, and accountability [41]. By leveraging two features namely, the immutability and the transparency of the blockchain, Ethereum can achieve and enhance the security levels of the IoT environment.

Also, the use of the formal verification of the security problem of smart contracts in blockchain like the application of Ethereum has been considered in order to ensure the dependability and security of smart contracts [42]. The certainty of the blockchain assurance is manifested by methods, but interfaces and possible hacking attempts do not indicate concern since the smart contract has formal verification.

First and last, Ethereum has certain over rivals for security in performing smart contracts, integrated IoT applications for making smart contracts safer, and finally use of formal verifications, for ensuring, that smart contracts on the stage are secure and non-interference.

C. Disadvantages of Security Ethereum

Thus, according to numerous research works, the disadvantages of security in Ethereum have been revealed, which explains the possible risks and difficulties within the platform. The major drawback observed is the existence of prominent security issues detected in Ethereum Smart Contracts. These vulnerabilities can lead to unpredictable behaviour and take-over of the applications that are implemented on the Ethereum platform [43]. Smart contract programming is not simple and systematic security practices are missing or not followed, which leads to the fact that there are a lot of vulnerabilities in Ethereum smart contracts that endanger their security [43].

A third drawback mentioned in the studies is the following effect of the Gas mechanism in Ethereum on the decentralization of the nodes. The present Gas cost model of Ethereum may cause a lot of inconveniences to nodes with ordinary computational capacity compared to other powerful nodes hence a threat to the centralization of nodes in the Ethereum network [38]. Such a significant difference in the count of computational units could potentially foster centralization of decision-making processes in the network, which goes a significant contrast against Ethereum's decentralized approach.

Also, it has established that the consensus mechanism known as Proof of Work (PoW), which is currently in use for Ethereum, has a security vulnerability. It is worth mentioning that any PoW-based network including Ethereum can be prone to some of the attacks like double spending, 51% attack, Distributed Denial of Service (DDoS) attacks, and Sybil attacks because they depend upon influential nodes for mining and verifying the data [44]. These vulnerabilities present various security threats to the network and affect its trustless consensus mechanism of Ethereum.

Also, the security threshold of Ethereum has been noted to be affected by selfish mining and stubborn mining approaches. All the above strategies have the potential of lowering the stringency of security in Ethereum and thus, expose the network to attacks and manipulations. The existence of such strategies points to the difficulties of preserving the blockchain network's security and reliability not to mention when confronted with strategic mining actions.

Altogether, Ethereum has several security drawbacks, which consist of protection weaknesses in smart contracts, issues linked to the Gas procedure, perilous associated with PoW consensus procedure, and the influence of mining procedures on community security. Mitigating these security issues is important in improving the security and the dependability of the Ethereum network.

D. Roles of Security Ethereum

Ethereum security measures are rather diverse, following the idea to keep Ethereum safe from threats of various types: internal or external, technical or social. The platform's security is underpinned by enhanced cryptography and consensus mechanism; the one responsible for safe and secure data transfer [45]. The platform improves the protection level by using hash functions, decentralized computation, and a large number of developers that can use the platform for many purposes [46].

Just like with any blockchain application, protocols of security measures are followed to avoid the presence of loopholes and hacking on Ethereum smart contracts. ContractFuzzer is the tool that has been created to find security vulnerabilities that provide fuzzing inputs derived from the specification of the smart contract [77]. Ethereum has also the architecture of a blockchain that facilitates decentralized application DApp on the blockchain network beyond money transfers [74].

In addition, Ethereum addresses the privacy issue in multi-stakeholder applications by providing confidentiality, integrity, and availability of the data [78]. The extraordinarily widespread adoption of the decentralization model of the platform and the consensus mechanisms that are used help to improve protection from vulnerabilities and threats [47]. The level of security adopted in Ethereum is intended to forestall all these and effectively reduce incidences of fraud, alteration of records, and unauthorized entry in block-chained transactions [77].

Thus, it is possible to conclude that Ethereum is protected from various kinds of threats and weaknesses by the use of advanced cryptographic solutions, decentralized consensus algorithms, smart-contract auditing tools, and PETS that bolster the security of Ethereum and its environment.

E. Issues of Security Ethereum

Weaknesses in security have been considered in Ethereum with some researchers analysing certain problems and weaknesses of the platform. Out of all the Ethereum concerns, problems concerning smart contracts, which entail contracts with the business terms coded into them can be considered as a major one. Such smart contracts will contain coding bugs, coding errors and different types of attacks where hackers can manipulate the transactions or even steal funds from smart contracts [79]. For example, last year, an exploit in the Ethereum Development Platform in the form of smart contracts was discovered in the DAO and as a result, millions of Ethereum tokens were lost which was indeed create a major financial loss [79].

Also, Ethereum which at the moment uses the mechanism known as Proof of Work (PoW) has security concerns regarding scalability and energy consumption. The PoW consensus algorithm applied to Ethereum, just like in Bitcoin, has flaws in relation to the transaction processing rate and energy consumption that affects the security and functionality of the platform [80]. Finally, high load of transactions and popularity of a certain object can cause the network load and super high commissions, which disrupts the idea of the security and efficiency of the Ethereum platform [80].

Moreover, the decentralisation of Ethereum enabled by open-source necessary for decentralised applications is no less dangerous from the security point of view because of the lack of data protection and confidentiality. Due to the inherent public characteristic of the blockchain all transactions contained in the block are public to anyone and hence may create a loophole for violation of privacy of some of the transactions [78]. Preserving data confidentiality and privacy of the data obtained within the Ethereum network still poses a major security challenge that should not be underestimated and for which efficient solutions should be sought [78].

Thus, there are threats and vulnerabilities of Ethereum's security that come from smart contract flaws, consensus algorithms and distributed ledger technologies, network capacity and transaction fees, and sensitive data leakage. Solving these problems is essential to increase the stability and reliability of the platform and its usability in the changing environment of blockchain technologies.

Interoperability Ethereum

On the meaning of Interoperability specific to Ethereum, it can be described as the ability of Ethereum to freely interact with other inter connected networks, systems and other blockchains. Interconnectivity allows Ethereum to exchange information, money and data with different blockchain systems, DApps, and the fundamental world. This interconnectivity is done through various intermediate layers as the smart contracts, the oracles, and the interoperability layers.

Smart Contracts in Ethereum actively contribute to the interoperability process as they follow previously predetermined conditions or transactions regarding other established correspondence systems. They can be programmed to call other APIs on their own, process the results based on information they receive from the outer world, or even act as cross-chain transactions which allows Ethereum to work with other block chain networks [81].

There are some other components that need for the interoperation and the oracles are one of them and which is associated with Ethereum. While smart contracts in one platform are awakened to make a particular decision, data providers transfer data from different platforms to Ethereum blockchain and to/from other platforms with the assistance of oracles. Therefore, through oracles Ethereum can process other information such as fiat prices for Ether, weather conditions or IoT devices, which enable it to interface with other systems [48]. Interoperability covers the protocols, standards, and frameworks that have the mandate of facilitating a seamless and organized interaction between Ethereum and other modern blockchains and networks. It defines the standard, spec, and design of how to carry out cross chain, asset exchange and information transaction between different platforms [82].

Therefore, through communication, Ethereum is able to connect to almost any other networks and systems, thus adding more possibilities to the Ethereum network and, potentially, allowing for various new use cases where the Ethereum is to interact with other platforms and seamlessly share data.

F. Interoperability Advantages Ethereum

Benefits of interoperation for the Ethereum based DApp derive partially from the general architecture of Ethereum as it is a predominantly open system that provides more opportunities for the interaction with the external environment and other blockchains. To be specific, the integration of Ethereum with a few systems has the following significant advantages.

DA Apps are convenient to use because Ethereum is integrated, meaning you can use decentralized applications regardless of your location in the world. Therefore, meaning and usage of Ethereum rises globally through the use of trustless interactions and transactions. This capability alone gives Ethereum a much larger pool of users apart from opening up cross border transactions hence making it a World platform for decentralized applications and financial commerce [49].

Interoperability of Ethereum has other advantages and one of this is security. Due to its improved encryption frameworks and consensus algorithms, Ethereum offers a certain high level of information security, sent between systems. This tight security framework is vital for maintaining the data importance and its uniqueness when being processed and while interacting with other networks that have a different security level [45].

It also opens up new combinations of use cases and applications in many more quadrants than could be previously seen. Thanks to Ethereum, it is possible to link different systems and networks together, and such an environment is an open space for experimentations and novelties. 'Of course, this integrative capability make developers able to apply together number of technologies and platforms to create new applications that will be beneficial for Ethereum environment more [49].

Also, its connectivity makes the data retrievable easing the enhancement of Ethereum to bring data from the external environment. This capability goes a long way in enhancing the accountability of financial transactions with reference to the capability of the blockchain to incorporate actual and real time data. Besides, the overall quality of data is greatly enhanced to assist the user get accurate and reliable information; in addition, it gives more credence to the system [83].

In addition, Ethereum is compatible; that is, a single blockchain can share with other blocks the manner of exchanging assets and data. This is ideally important for complementary characteristics of two or multiple blockchain systems to facilitate in forming a rather interwoven blockchain community [49].

Lastly, focusing on the Ethereum framework for the decentralized environment based on interoperability comes to decentralized trust. In this case, it means that regardless of the system it interacts with it keeps decentralisation standards for making the interactions/trade thrustless; decentralised trust is imbedded in Ethereum's values and approaches and that remain the stable ground for all Ethereum's work/ventures [49].

In conclusion, the interoperability advantages contributed to the hands of Ethereum enables the platform to communicate with the exterior environment, receive info, execute operations with other underpinning structures and contribute to the further evolution of the segment. They also enhance not only Ethereum but also build the decentralized applications and transactions' broad abilities as well.

G. Interoperability Disadvantages Ethereum

With regard to Ethereum specifically, one might say that interoperability problems can be quite an issue for the net ion in one direction and communication as well as integration with other systems or Blockchains. Therefore, it is clear that if the above elements are considered, the advantages of blockchain interoperability are apparent, but as always, the problem when implementing such a connection is that attention should be paid to the fact that the Ethereum network should not be affected by stability, functionality, and security.

The main issue with the interoperability in Ethereum is that, often, they cannot be easily scaled upward. When it started interacting with data on the other chain or engaging in transactions, the complexity raises the traffic and load on the network's platforms. This scalability issue arises because of other mechanisms of communication and coordination in different systems that involve blockchain technology. Hence the 'transaction times may be high and other certain operation may reduce thereby posing a negative impact on business development and more so it become hard for the platform to expand the number of users at a very fast rate [50].

Interoperability is also defined with a certain set of security threats that its utilization seems to be doomed with anyway. Thus, giving it a place within the external systems and networks introduces the new risks and threats with the Ethereum usage. All these interactions might impact the general security of the blockchain platform as either the attackers utilize the interdependent structures or all such transactions have to be verified to be safe while simultaneously, the integrity of Ethereum needs to be increased [50].

The final characteristic that was discussed, interoperability, also adds to the complexity of smart contracts, especially if the smart contracts have to move between different blockchain networks – in which code could become a lot more complex and not easy to manage at all in this case, it is possible to get issues with managing and documenting the code, and also with the auditing and protection of the interactions of smart contracts As part of the debates, developers are presented with additional challenges [50].

Another issue of interoperability, which is spelt out in Ethereum is the issue of data privacy In as much as it is possible to share data with external systems of Ethereum there is always the concern of data leakage, unauthorized access to data, access to records and documents This is because as the data transmits from one network to the other there is always the issue of data privacy which becomes hard to enforce The users and organisations should also devote equal attention to protect sensitive information [50].

Also, there is a difference in consensus protocols used in Ethereum and the other blockchain systems and this is another challenge related to interoperation. Often, various blockchain networks employ distinct consensus means and do not allow for making consensus about the defined transactions and data sharing. Such a misconfiguration can increase the difficulty in co-integration and interaction with other network as attaining finality and solidity in multi – system architecture is not easy [50].

Hence, it is possible to seem that there is a number of advantages which are regarded in transition to the concept of interoperability including the consideration of the various disadvantages and problems in this sphere. The last issue on smart contract is that it becomes complex; they have scalability issues; Smart contracts bring new security threats; concerns with data privacy; and violation of consensus protocol. The challenges encountered with Ethereum's open source nature when interfacing with other systems indicate the necessity for security and hence quality solutions must be implemented. Solving these challenges can on the one hand reinforce over the benefits of interoperability, on the other hand it can sustain high efficiency, high security and reliability features of Ethereum.

V. Overview of Hyperledger

A. Security Hyperledger

The security of Hyperledger Fabric remains sensitive to discussion, while improving the platform's resistance to possible threats is studied actively. Hyperledger Fabric, which is a permissioned blockchain technology has been described as having enhance privacy, throughputs, as well as negligible latency than some other private, permissioned technologies such as Quorum, Multichain, and R3 [84]. Designing of the platform focuses on the high-security encryption, easy scalability, deployment capabilities, and pluggability; the distributed ledger solutions offered by the Ethereum platform are versatile solutions that meet the needs of different applications [85].

Some works have proposed application of security features on Hyperledger Fabric, including access control of the personal data shared within the distributed ledger, as well as key transfer of User Characteristic Secret Keys, to make certain the protection of users' privacy [86]. Furthermore, Hyperledger Fabric's design is to build a blockchain solution for the growing number of business applications on an industrial level while addressing different sectors and purposes [8]. Incidentally, the platform's security measures include mechanisms such as encryption, restricted access, and cryptographic algorithms that safeguard the validity and confidentiality of the transactions [87].

In addition, theoretical studies have revealed the effectiveness of this platform in various meaningful organizations, including supply chain management and healthcare organizations combined with acceptance and popularity [88]. Width reference to the coding of smart contract, Hyperledger Fabric also outperforms other blockchain platforms in that it allows the writing of smart contracts in general purpose programming languages such as Java [89]. Besides, because of security measures integrated to the platform and its flexibility along with effectiveness, it can be essential in the ecosystem of the blockchain for different purposes and applications [6].

Finally, the security analyses of Hyperledger Fabric conclude that this platform is devoted to the security of users' data, providing privacy, and scalability while including numerous enterprise-grade security solutions that would help organizations adapt blockchain securely and proficiently.

B. Advantages of Security Hyperledger

It is this security that is offered in Hyperledger that counts for a lot and which paves the way for them to choose the same in their various endeavours. They include; holding that Hyperledger Fabric is privatized meaning it can be owned by some organizations in a way that only accredited individuals, communities, or companies are allowed to transact on the blockchain. Another benefit of this permission blockchain is that the participants are also known and more over-screened for fraud like the other participants also reduces the probability of engaging in unauthorized or fraudulent activities [51].

Additionally, Hyperledger Fabric boasts about having flexible CP models which can be easily extended or even customized depending on what the organization prefers for a particular use case or level of trust. About this flexibility can implement consensus mechanisms that are effective, thus enhancing security for the application of the network [51].

Compared with other existing platforms, the Hyperledger-based system has smaller response time and stronger scalability, but stronger traceability and audibility. These attributes are crucial in the security and privacy aspects of the IoT also the fulfilment of transactions particularly in the eventuality that a considerable volume of information is generated and transferred by and among different gadgets [51].

For the same reason, since Hyperledger Fabric messages respond to privacy and confidentiality attributes such as private transactions and channels; it brings about security and only permits the exchange of information between parties in an authorized channel. This capability is very crucial in areas of concern like the medical field and the financial sector this data is sensitive [52].

Also, Hyperledger Fabric is integrated with other advances in the sphere of security, for instance protocols concerning secure data integrity validation and innovations of key management system to contribute to the boosting of a security level of the platform. These integrations help in dealing with the threats and challenges to security therefore the reliability of the data in the blockchain [53].

Consequently, it can be stated that according to the described permissioned architecture, the non-fixed consensus solutions, scalability, privacy, and compatibility with the new protective systems, Hyperledger offers a vast potential for further enhancement of the security. Thus, the specific advantages of the presented models can be formulated as the following: Through the application of the above benefits of the proposed models, an organization is in a better position to create well-designed and secure blockchain solutions that addresses various security concerns.

C. Disadvantages of Security Hyperledger

Concerning the failure heuristic for Security, some of the failure cases are also included in the recent studies contemplating the Hyperledger forum that point out the issues or threats that were pretty visible on the surface. Two main disadvantages; Security because even though it comes under the label of a Hyperledger which is more of a permission blockchain. The permission type has a better handle and control over the people that are allowed to register with the network or even transact some functions within the network. On the other hand, permission type has issues in managing the permission and the identities than the permissionless one, which at one time may lead to misconfiguration This in a way makes the network vulnerable and can easily be compromised if the network is through to look for [75].

Then there is the level of security that comes by default with various portions of HL including Hyperledger Besu or Hyperledger Orion. These components may not have similar subcomponents needed for base defence or specific decentralised application or DApps security as key assignments, IDS. Furthermore, the unprotected privacy group identifier in Hyperledger Besu is by default and with an easily hackable hard code, which elevates the Security weakness, and also permits some of the data to be seen by unauthorized individual [54].

However, the integration of the Hyperledger Fabric to IoT-based systems has posed more security challenges in relation to damaging interaction as far as IoT networks are concerned. This restriction therefore entails that an attack or manipulation can take place within the parameters of Hyperledger Fabric, and this impacts the IoT component communication networks that have been established [55].

However, there still exists a blatant security aspect observed in the preceding section whenever utilizing Hyperledger Fabric as the one mentioned to not fit IoT-based Health Monitoring systems that brings all the above challenges together. Maybe, it could be nonoptimal to use traditional ways for protection from threats from the outside to the IoT nodes to pursue arrays of questions on the IoT nodes because the complicated computations with high energy demands are not at all suited to the IoT nodes [48].

In such a connection, it locates such security issues directly with which Hyperledger is connected and these issues are related to some of the key points of permissioned blockchain, some of them are inherently not protected, and the problem of IoT security mentioned here as a topic of protection in IoT based systems. Hence, it can be deduced that more effort and ways should be employed in enhancing the security and more so the resiliency of the Hyperledger-based applications and systems that tackle such security challenges.

D. Functions of Security Hyperledger

For instance, Hyperledger Fabric has integrated security functions to provide some protection for the platform's actions against all types of threats and keep the generality of the key processes more secretive. Hyperledger Fabric is another type of blockchain that was designed for B2B commerce and has several features that distinguish it from the example above, such as limited access [90]. Read has a general fare of security that can provide some level of detail for access control targeting at protecting data [7].

Some cryptographic approaches adopted by Hyperledger Fabric area used for the purpose of transaction security, while other are used for maintaining the holiness of the blockchain system. It is also architectural flexible and modular in nature which are important features that in turn enhances its pluggability, which makes it easy to specify the required security settings based on the various applications [91]. In addition, the management claims the possibility of being able to offer certain levels of communication assurance, as well as ensuring the channels and the encryption as means to regulate and/or restrict both the input and the output of information for the sake of enhancing the overall security [92].

Furthermore, one must note that Hyperledger Fabric contains components such as anomaly detector and intrusion detector to help with quick identification and management of Data breaches and Cyberattacks within the network [93]. With inventions of such powerful techniques like machine learning, Hyperledger Fabric is well placed to enhance its security intelligence to deal with any looming breakthrough to block the blockchain transactions and information security, thus offering continuous security on the blockchain deals and data [43].

Therefore, the security element incorporated in Hyperledger Fabric includes the privacy aspect, the capacity and detailed regulation of permissioned access control, cryptographic security, and a highly efficient method for the identification of breakthroughs and intrusion for enhancing the platform against security threats and risks.

E. On Security Hyperledger

The security aspects in Hyperledger Fabric have been proposed to highlight the area of interest in the research to expose the vulnerabilities and challenges in the network. However, one of the critical problems that can arise in Hyperledger Fabric has to do with the fact that it is essentially permissioned. While having completely restricted access to the participants, permissioned blockchains bring some problematics and challenges in matters of granting access control and permissions securely and in a systematic way that can, indeed, misconfigure the system to thereby make it vulnerable to bad application and data applications [94].

It is safer to use particular Hyperledger consensus mechanisms, for example, PBFT or Raft which, however, if incorrectly applied, can negatively affect security inherent to Fabric. To ensure the validity of transactional consensus, consensus protocols are important and necessary for mining, and consensus-related problems or configuration issues could threaten the blockchain network [94].

The last security risk concern that should be accorded attention in Hyperledger Fabric has to do with smart contracts that are implemented on Hyperledger Fabric. There is no doubt that smart contracts are automatic and transparent, but they inherit the same problems as other software: coding errors that can potentially open a space in a program where bugs can be exploited by malicious actors. As for the security and the integrity of smart contracts within the HP context and specifically in the Hyperledger Fabric, code reviews, functional testing, as well as the adoption of the best practices all minimize the conceivable overall risks that may take place [94].

Second of all, the fact that FAB has a built environment and that this enables it to function more freely or easily also affords the possibility of an adjustable design, there are security implications to do with the use of multiple components. This shall be of significant importance in order to avoid the compromising of security every time that there is inter- module interactions & communications, peer endorsement, ordering of services and any activity at the application layer in the blockchain [94].

Summing up, dealing with the issues in the present article, it can be stated that the enhancement of security in Hyperledger Fabric can be possible only when the problem will be solved on various levels beginning with the access control and ending with consensus, smart contract security and using more reliable and more credible modular components to form the further staking of the Hyperledger Fabric-oriented platform for the subsequent enterprise applications based on the blockchain technology.

F. Hyperledger Fabric Architecture

Hyperledger fabric is an enterprise grade platform to build highly officinal and reliable distributed ledgers based on seven principles that provides optimized concealing, reliability, flexibility and scalability features. It refers to a decentralized ledger technology based on the concept of blockchain it uses smart contracts to facilitate the enforcement of trust from across various parties/ systems. Hyperledger Fabric eliminates mining but retains the beneficial properties of typical cryptocurrency blockchains such as Bitcoin and Ethereum like State developmental/regulation, fixed/acausal, and anti-counterfeiting amongst others. It has been established that in the throughput capability of certain numbers of transactions per second; thousands [95], Hyperledger Fabric is better off than others. Some of these include: These characteristics and others that will be described below make Hyperledger Fabric completely appropriate for complex multiple physical/ logical supply chain arrangements, that encompass several physical and/or logical supply chain processes and actors. The smart contracts here are built utilizing general-purpose programming languages. Java, Go, NodeJS The smart contracts are created with general-purpose languages of programming to make it easily accessible to as many organizations as possible with the aim of increasing the adoption rate of this technology against technologies that require the use of certain programming languages, for instance, solidity in the Ethereum platform.

In this paper an attempt was made to give first proposal of how the drug traceability should look like in Hyperledger Fabric for the discussed enterprise-level blockchain-based system for the support of the pharmaceutical supply chain management; the account of different stakeholders with indication of their relations based on different channels to provide the maximal privacy and confidentiality and data protection. This notion of channels in the context of Hyperledger is entirely different and such a concept is missing in other regular platforms. Organizationally, channels offer both conceptual, tangible, and feasible structural clear line separating business contents/functions and policies governing the use of sensitive user data owned by different stakeholders who operate under one platform/system. In fact, Hyperledger Fabric synthesizes a Crash Fault Tolerant Transaction Ordering Service to bring deterministic characteristic when an event is being recorded, as well as for a secured way of transmitting or sharing medication related transactions among a group of people or institutions who cannot be trusted. This aids in establishing a sound track and trace system of origin to policy make the way ahead regarding stocking counterfeit medication in PSC. In this proposed scheme for the architecture of the new building blocks for the creation of a blockchain architecture, there is modularity for flexibility, security on layers, and the privacy for growth.

In the prospective Hyperledger Fabric model, the possible private blockchain network setup being permissioned, all the user entities and their identities/party details like the Indian pharmaceutical company and customers/end-users can be authenticated and identified by the Health Authority using the Membership service provider (MSP) component of Hyperledger Fabric. The MSP component is designed as the plug-in feature: in the default, an MSP part can be the one provided/delivered along with Hyperledger Fabric as Local MSP or it can be the external one (for example, generate OpenSSL certificates and use them, integrate with Active Directory, and so on). As far as the formation of the trust relationship within the untrusted participants is concerned, the Hyperledger fabric just draws the necessity simply to use the MSP (local/external) that sets the rules and regulatory frameworks that would govern the various stakes/identity-seeking to access the blockchain resources. They ensure that the identities of the people interacting in the network are protected, and also allow easier identification of actions (such as when a malicious transaction has been carried out). It is a unique approach in the context of a freemium business model that revisits non-determinism, exhaustion of resources, and performance checks at all the participants of the chain of supply of pharmaceutical products through decentralisation of identity [95].

Finally, the ordering service (OS) and peer nodes (peers), in different levels, are seen as the basic modules of Hyperledger Fabric. Peers have several utilities including replicating the ledger including copies, executing smart contracts better understood in Hyperledger Fabric as the chain code, endorsing, and also logging the transaction. These transactions are then forwarded to the OS from the client's app after which they are grouped into blocks by the endorsement signature of other peers in a blockchain network and only after that are sent to the committing peers to check against the endorsement policies of the blockchain network.

G. Interoperability Hyperledger Fabric

Interoperability in Hyperledger Fabric refers to the seamless exchange of data, assets, and information between the Hyperledger Fabric blockchain network and external systems or other blockchain platforms. This capability is crucial for enabling cross-platform communication and collaboration, expanding the range of potential use cases and applications.

A significant aspect of achieving interoperability in Hyperledger Fabric is through the support of interoperability protocols and standards. These protocols establish common rules and formats for data exchange and transactions, ensuring compatibility and smooth communication between Hyperledger Fabric and other blockchain networks [56].

Smart contracts are essential for facilitating interoperability within Hyperledger Fabric. They can be programmed to interact with external systems, respond to external data inputs, or facilitate cross-chain transactions, thereby enabling Hyperledger Fabric to engage with a variety of networks and platforms [56].

Oracles also play a vital role in achieving interoperability within Hyperledger Fabric. By serving as bridges between the blockchain network and external data sources, oracles provide smart contracts with real-world data from off-chain sources. Through oracles, Hyperledger Fabric gains access to external information, enhancing its interoperability with external system [56].

In conclusion, Hyperledger Fabric's interoperability capabilities, supported by interoperability protocols, smart contracts, and oracles, facilitate seamless communication and data exchange between the blockchain network and external systems. This fosters collaboration and innovation in decentralized applications and transactions.

H. Interoperability Advantages Hyperledger Fabric

Hyperledger Fabric's interoperability capabilities bring a myriad of advantages that significantly enhance its functionality and utility within the blockchain ecosystem. By enabling seamless communication with other blockchain networks, Hyperledger Fabric ensures that data and as sets can be exchanged effortlessly across different platforms, thereby boosting scalability and performance. This ability to interact with various systems not only expands the platform's reach but also optimizes its operational efficiency, allowing it to handle increased volumes of transactions and data exchanges more effectively [57].

One of the most impactful applications of Hyperledger Fabric's interoperability is in healthcare data sharing. The platform supports efficient and secure information exchange between patients, physicians, and healthcare providers. This feature ensures that sensitive medical data can be shared transparently and traceably, enhancing the quality of care and ensuring that medical professionals have access to accurate and up-to-date patient information [58]. Such capabilities are crucial for creating integrated healthcare systems that prioritize patient safety and data integrity.

Hyperledger Fabric's ability to facilitate cross-blockchain transactions is another significant advantage. By enabling the transfer of assets and data between disparate blockchain networks, Hyperledger Fabric fosters greater collaboration and interoperability within the blockchain space. This cross-chain capability is essential for creating a more cohesive and interconnected blockchain ecosystem, where different platforms can work together seamlessly to achieve common goals [56].

The development of decentralized applications (Dapps) is also greatly enhanced by Hyperledger Fabric's interoperability. These applications can interact with multiple blockchain networks, significantly increasing their versatility and functionality. This cross-platform interaction allows developers to create more robust and flexible Dapps that can leverage the strengths of various blockchain networks, providing users with a richer and more comprehensive experience [96].

Moreover, the interoperability features of Hyperledger Fabric facilitate smart contract interactions between different blockchain networks. This capability ensures that agreements and transactions can be executed seamlessly across various platforms, enhancing the reliability and efficiency of these processes. The ability to interact with smart contracts from different networks opens new possibilities for automating and streamlining complex transactions, making blockchain solutions more powerful and versatile [97].

In the realm of supply chain management, Hyperledger Fabric's interoperability offers significant advantages. The platform supports the integration of various components within the supply chain, promoting the secure and efficient exchange of data and assets. This integration ensures that all participants in the supply chain have access to accurate and timely information, improving transparency and accountability. As a result, businesses can better manage their supply chains, reducing costs and increasing efficiency [98].

In conclusion, Hyperledger Fabric's interoperability advantages empower the platform to collaborate effectively with diverse blockchain networks. This capability enhances scalability and performance, supports healthcare data sharing, enables cross-blockchain transactions, facilitates the development of decentralized applications, and streamlines supply chain management solutions. By leveraging these interoperability features, Hyperledger Fabric not only improves its own functionality but also contributes to the broader advancement of the blockchain ecosystem.

I. Interoperability Disadvantages Hyperledger Fabric

Interoperability challenges for Hyperledger Fabric can indeed pose significant obstacles in achieving seamless communication and integration with external systems and other blockchain platforms. While the potential benefits of interoperability are well-recognized, various inherent complexities and risks must be managed effectively to maintain the functionality and security of Hyperledger Fabric.

One of the primary challenges associated with interoperability in Hyperledger Fabric is the complexity involved in implementing interoperability protocols. The process requires intricate protocols and standards to ensure compatibility and smooth data exchange with diverse blockchain networks. This complexity can lead to difficulties in creating a unified approach for interoperability, as different blockchain platforms may have varying specifications and requirements. Ensuring that Hyperledger Fabric can effectively communicate and integrate with other networks demands considerable effort in developing and maintaining these interoperability protocols [59].

Security concerns are another significant challenge when it comes to interoperability. Interactions with external systems can introduce new vulnerabilities and attack vectors, potentially compromising the overall security of the Hyperledger Fabric network. As the platform opens to cross-chain transactions and data exchanges, it becomes crucial to implement robust security measures to protect against potential threats. The challenge lies in ensuring that all interactions are secure, and that the integrity of the Hyperledger Fabric network is maintained despite the increased exposure to external risks [59].

The misalignment of consensus mechanisms between Hyperledger Fabric and other blockchain platforms also poses a substantial hurdle to interoperability. Different blockchain networks may utilize various consensus protocols, making it challenging to achieve consensus and transaction finality across these disparate systems. This misalignment can impede the seamless integration of Hyperledger Fabric with other networks, as ensuring consistent and reliable transaction processing across different platforms becomes increasingly complex [59].

Data privacy and confidentiality concerns are also paramount in the context of interoperability. The exchange of information between Hyperledger Fabric and external systems can lead to potential data leakage or unauthorized access to sensitive information. Protecting user privacy and ensuring that confidential data remains secure during cross-chain interactions is a critical challenge. It requires robust data protection measures and strict privacy protocols to prevent breaches and maintain trust in the platform [59].

Furthermore, ensuring the compatibility and functionality of smart contracts across different blockchain networks is a significant challenge for interoperability in Hyperledger Fabric. Smart contracts need to be designed and executed in a manner that is compatible with the various environments they interact with. This necessitates careful consideration of contract logic and execution, ensuring that smart contracts can function seamlessly and securely across heterogeneous blockchain platforms. The complexity of achieving this compatibility can hinder the development and deployment of interoperable smart contracts [59].

In conclusion, while interoperability offers numerous benefits, such as enhanced collaboration and data exchange, it also presents several challenges and complexities. The complexity of interoperability protocols, security risks, consensus mechanism misalignment, data privacy concerns, and smart contract compatibility issues are significant challenges that need to be addressed. Ensuring the secure and efficient integration of Hyperledger Fabric with external systems requires meticulous planning and the implementation of robust solutions to mitigate these challenges. By addressing these issues, Hyperledger Fabric can continue to leverage the advantages of interoperability while maintaining its performance, security, and reliability.

VI. DISCUSSION

It is entirely worth emphasizing that even the highest levels of security must be introduced in this respect, as it is one of the key measures if it comes to threats and risks characteristic of blockchain-type computer systems.

Monitoring activity attempts to seek to spy on the network to look for indications of activity that might be considered a distortion or any other activity that will be regarded as insecure. Another form of security is there where an automatic process happens, and artificial intelligence and machine learning are there to guide the process to detect threats beforehand and it acts as a swipe to prevent intrusion if it has been planned. These policies, plans, and frameworks prevent any security breach in the first place but in case a security breach occurs, then there is a well-formulated and defined strategy on how to minimize or avoid the adverse effects on the blockchain systems. Implementation of such measures when has the effect of building a strong energy of security that guards not only the Ethereum but also Hyperledger Fabric Blockchain and is among the best measures that can help to reduce the possibility of an attack breakthrough and hence strengthen the chance of the blockchain platform.

Interoperability is another element that cannot be considered as a topic that should be left beyond the scope of the performed activities. It is hence necessary to engage and calibrate the Ethereum and the multiple blockchains within the Hyperledger Fabric to sustain directional interactions with standards for interoperability. Also, it could be explained concerning the fact that interoperation could also be defined as the degree of effectiveness, whereby the greater number of distinct systems could interconnect and recreate, the efficiency of which has been observed to be significantly enhanced, because of the greater standardized on the communication processes [59]. It boosts the effectiveness of blockchains while decreasing those interfaces which are normally needed which is the amazing increase of organizations that use this blockchain technology as they try to integrate so many systems.

Therefore, to consider controlling the interactions with the smart contracts as an important job that should be performed after a certain time to ensure that the smart contract forms are devoid of any circumstance of the malicious corruption. Smart contract audit effectively examines the contracts that are created and then checked for possible flaws that can also be maliciously exploited by hackers. Therefore, when using services of smart contracts threats can be avoided since using this tool one can check all security aspects of the blockchain platform for the purpose of full-fledged safety assessment of all characteristics of its security. Ideally, it is important that they start developing such a positive action to contribute towards the creation of principles based on trust and confidence in the use of blockchain platform [59], [14] .

A. Scalability Challenges and Solutions between Ethereum and Hyperledger Fabric

Ethereum's scalability has long been hindered by the limitations of its Proof of Work (PoW) consensus mechanism, which requires significant computational resources and limits transaction throughput. To address these challenges, Ethereum's transition to Proof of Stake (PoS), finalized with Ethereum 2.0, represents a fundamental shift in its architecture. PoS reduces energy consumption by replacing miners with validators who propose, and attest blocks based on their staked Ether. This transition enables faster block finalization, improves network efficiency, and scales the number of transactions per second (TPS), alleviating congestion and lowering gas fees.

Hyperledger Fabric takes a different approach to scalability by leveraging a modular and permissioned architecture. Unlike Ethereum, which operates on a single chain, Hyperledger Fabric allows for the parallel execution of smart contracts (chaincode) across different channels. This separation of transaction execution, ordering, and validation streamlines processing and minimizes bottlenecks. The flexibility to use pluggable consensus mechanisms further allows organizations to customize Fabric deployments based on performance requirements, resulting in greater scalability across enterprise environments.

Ethereum's PoS model focuses on achieving scalability in a public, decentralized environment, addressing the needs of decentralized applications (DApps) and financial services. In contrast, Hyperledger Fabric's modular design prioritizes scalability within private, permissioned networks, catering to enterprises that require high throughput and efficient resource allocation. These distinct approaches to scalability reflect the diverse use cases that blockchain platforms aim to serve, highlighting the evolving landscape of distributed ledger technologies.

B. Artificial Intelligence and Machine Learning for Blockchain Security and Anomaly Detection

As blockchain networks grow in complexity and scale, the need for robust security mechanisms becomes paramount. Artificial intelligence (AI) and machine learning (ML) have emerged as essential tools for enhancing blockchain security, offering capabilities such as anomaly detection, fraud prevention, and threat mitigation. By analysing large datasets of blockchain transactions, ML algorithms can identify patterns indicative of malicious activity, such as double-spending attempts, smart contract exploits, and network attacks.

In Ethereum, AI-driven security solutions monitor decentralized applications (DApps) and smart contracts for vulnerabilities. These systems detect irregularities in transaction flows, identify potentially fraudulent addresses, and flag deviations in gas usage that may signal malicious intent. Similarly, Hyperledger Fabric integrates AI models to monitor permissioned networks, ensuring that access control policies are enforced and anomalies in chaincode execution are promptly addressed. Fabric's modular architecture facilitates the deployment of custom anomaly detection models tailored to specific enterprise needs.

AI enhances blockchain security by providing predictive insights into potential threats. Machine learning models, trained on historical data, predict future vulnerabilities, enabling pre-emptive measures to secure blockchain ecosystems. In the context of Ethereum, AI systems proactively identify risky smart contract deployments, while in Hyperledger Fabric, AI-driven security analytics assess network health, ensuring that consensus mechanisms and node interactions remain uncompromised.

Integrating AI and ML into blockchain networks strengthens resilience against evolving cyber threats. This convergence represents a critical step towards creating autonomous, self-healing blockchain infrastructures capable of mitigating risks in real time. As blockchain adoption accelerates, the synergy between distributed ledger technologies and AI will play a pivotal role in safeguarding decentralized and enterprise blockchain solutions.

VII. CONCLUSION

Among the key stakeholders present within the context of a blockchain platform, two are of considerable importance, Ethereum and Hyperledger Fabric. Ethereum is widely recognized for its smart contracts and its significant role in advancing decentralized finance (DeFi), which has been instrumental in shaping the blockchain landscape [99]. Moreover, Hyperledger Fabric has also been identified to be among the favorite solutions for enterprise implementation because of qualities such as improved security, chances of decentralized operation, and inherent modularity [85].

Finally, about the performance benchmarking, the research has left to discuss the comparison of such platforms as Ethereum and Hyperledger Fabric by using the different benchmarks [100], [101]. These assessments are critical because they shed light on the approaches' advantages and disadvantages when it comes to making accurate, situation-specific determinations. In addition, there was explication about how different blockchain platforms can interconnect, for example, it may enable Ethereum or Hyperledger Fabric and other networks to interface [13], [14].

On the other hand, in terms of security, Hyperledger Fabric has always emerged as superior because it comes with excellent security and privacy features; thus, it has been deployed in, for instance, the storage of healthcare data [11], [102]. Additionally, the application of even higher-level technologies, including such ones as Hyperledger Fabric or any other types of blockchains described in this research, provide assured impermeability for the organizational data as it cannot be modified in any way [3].

Therefore, it may be easy to establish that Ethereum and Hyperledger Fabric are two distinct but essential types of a continuously developing blockchain platform. The current features of smart contract and Decentralized finance place Ethereum in the front line of industry while Hyperledger Fabric has all every enterprise solution and high security solutions that makes them suitable for usage in Health informatics records, 5G interoperability solutions.

ACKNOWLEDGMENT

This work is supported by the FRGS24-327-0936 under Ministry Project ID: FRGS/1/2024/ICT02/UIAM/02/4, Centre of Excellence Cybersecurity, KICT, IoTeams, KICT and Silverseeds Lab Network.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses," 2019, *arXiv*. doi: 10.48550/ARXIV.1908.04507.

[2] Y. Xie, J. Jin, J. Zhang, S. Yu, and Q. Xuan, "Temporal-Amount Snapshot MultiGraph for Ethereum Transaction Tracking," 2021, *arXiv*. doi: 10.48550/ARXIV.2102.08013.

[3] S. A. Amri, L. Aniello, and V. Sassone, "A Review of Upgradeable Smart Contract Patterns based on OpenZeppelin Technique," *The JBBA*, vol. 6, no. 1, pp. 1–8, Apr. 2023, doi: 10.31585/jbba-6-1-(3)2023.

[4] S. Pandey *et al.*, "Do-It-Yourself Recommender System: Reusing and Recycling With Blockchain and Deep Learning," *IEEE Access*, vol. 10, pp. 90056–90067, 2022, doi: 10.1109/ACCESS.2022.3199661.

[5] J. Kim, K. Lee, G. Yang, K. Lee, J. Im, and C. Yoo, "QiOi: Performance Isolation for Hyperledger Fabric," *Applied Sciences*, vol. 11, no. 9, p. 3870, Apr. 2021, doi: 10.3390/app11093870.

[6] R. Alotaibi, M. Alassafi, Md. S. I. Bhuiyan, R. S. Raju, and M. S. Ferdous, "A Reinforcement-Learning-Based Model for Resilient Load Balancing in Hyperledger Fabric," *Processes*, vol. 10, no. 11, p. 2390, Nov. 2022, doi: 10.3390/pr10112390.

[7] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses," 2019, *arXiv*. doi: 10.48550/ARXIV.1908.04507.

[8] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, May 2020, doi: 10.1145/3316481.

[9] A. Roehrs, C. A. Da Costa, R. Da Rosa Righi, V. F. Da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *Journal of Biomedical Informatics*, vol. 92, p. 103140, Apr. 2019, doi: 10.1016/j.jbi.2019.103140.

[10] M. Islam, M. H. Rehmani, and J. Chen, "Differential Privacy-based Permissioned Blockchain for Private Data Sharing in Industrial IoT," 2021, *arXiv*. doi: 10.48550/ARXIV.2102.09857.

[11] Q. Wang and S. Qin, "A Hyperledger Fabric-Based System Framework for Healthcare Data Management," *Applied Sciences*, vol. 11, no. 24, p. 11693, Dec. 2021, doi: 10.3390/app112411693.

[12] L. Foschini, A. Gavagna, G. Martuscelli, and R. Montanari, “Hyperledger Fabric Blockchain: Chaincode Performance Analysis,” in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland: IEEE, Jun. 2020, pp. 1–6. doi: 10.1109/ICC40277.2020.9149080.

[13] G. Llambias, B. Bradach, J. Nogueira, L. González, and R. Ruggia, “Gateway-based Interoperability for DLT,” Feb. 22, 2023. doi: 10.36227/techrxiv.22120520.

[14] D. L. Dinesha and B. Patil, “Achieving Interoperability in Heterogeneous Blockchain Users Through Inter-Blockchain Communication Protocol,” Nov. 22, 2022. doi: 10.36227/techrxiv.21532953.v2.

[15] C. Stamatellis, P. Papadopoulos, N. Pitropakis, S. Katsikas, and W. Buchanan, “A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric,” *Sensors*, vol. 20, no. 22, p. 6587, Nov. 2020, doi: 10.3390/s20226587.

[16] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, “Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology,” *PLoS ONE*, vol. 15, no. 12, p. e0243043, Dec. 2020, doi: 10.1371/journal.pone.0243043.

[17] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, “Blockchain technology in supply chain operations: Applications, challenges and research opportunities,” *Transportation Research Part E: Logistics and Transportation Review*, vol. 142, p. 102067, Oct. 2020, doi: 10.1016/j.tre.2020.102067.

[18] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017, doi: 10.1093/jamia/ocx068.

[19] P. Tagde *et al.*, “Blockchain and artificial intelligence technology in e-Health,” *Environ Sci Pollut Res*, vol. 28, no. 38, pp. 52810–52831, Oct. 2021, doi: 10.1007/s11356-021-16223-0.

[20] A. Henninger and A. Mashatan, “Distributed Renewable Energy Management: A Gap Analysis and Proposed Blockchain-Based Architecture,” *JRFM*, vol. 15, no. 5, p. 191, Apr. 2022, doi: 10.3390/jrfm15050191.

[21] M. N. M. Bhutta *et al.*, “A Survey on Blockchain Technology: Evolution, Architecture and Security,” *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[22] T. G. Bao and D. M. Phan, “Blockchain applications in business and financial activities in Vietnam: Situation, trends, opportunities and challenges,” *irjmis*, vol. 9, no. 6, pp. 766–776, Sep. 2022, doi: 10.21744/irjmis.v9n6.2187.

[23] Z. Yu, D. Xue, J. Fan, and C. Guo, “DNSTSM: DNS Cache Resources Trusted Sharing Model Based on Consortium Blockchain,” *IEEE Access*, vol. 8, pp. 13640–13650, 2020, doi: 10.1109/ACCESS.2020.2966428.

[24] W. Yao, F. P. Deek, R. Murimi, and G. Wang, “SoK: A Taxonomy for Critical Analysis of Consensus Mechanisms in Consortium Blockchain,” 2021, doi: 10.48550/ARXIV.2102.12058.

[25] V. Upadrista, S. Nazir, and H. Tianfield, “Consortium Blockchain for Reliable Remote Health Monitoring,” Jan. 04, 2024, *In Review*. doi: 10.21203/rs.3.rs-2297411/v1.

[26] W. Pourmajidi, L. Zhang, J. Steinbacher, T. Erwin, and A. Miranskyy, “Immutable Log Storage as a Service on Private and Public Blockchains,” 2020, doi: 10.48550/ARXIV.2009.07834.

[27] J. Yusoff, Z. Mohamad, and M. Anuar, “A Review: Consensus Algorithms on Blockchain,” *JCC*, vol. 10, no. 09, pp. 37–50, 2022, doi: 10.4236/jcc.2022.109003.

[28] D. C. G. Valadares, A. Perkusich, A. M. Falcão, and C. Seline, “Privacy-Preserving Blockchain Technologies,” May 26, 2023, *Computer Science and Mathematics*. doi: 10.20944/preprints202305.1874.v1.

[29] H. C. Hwang, J. G. Shon, and J. S. Park, “Design of an Enhanced Web Archiving System for Preserving Content Integrity with Blockchain,” *Electronics*, vol. 9, no. 8, p. 1255, Aug. 2020, doi: 10.3390/electronics9081255.

[30] L. M. Palma, M. A. G. Vigil, F. L. Pereira, and J. E. Martina, “Blockchain and smart contracts for higher education registry in Brazil,” *Int J Network Mgmt*, vol. 29, no. 3, p. e2061, May 2019, doi: 10.1002/nem.2061.

[31] X. Wang *et al.*, “A High-Performance Hybrid Blockchain System for Traceable IoT Applications,” in *Network and System Security*, vol. 11928, J. K. Liu and X. Huang, Eds., in Lecture Notes in Computer Science, vol. 11928. , Cham: Springer International Publishing, 2019, pp. 721–728. doi: 10.1007/978-3-030-36938-5_47.

[32] D. Zhuang and J. M. Chang, “Enhanced PeerHunter: Detecting Peer-to-Peer Botnets Through Network-Flow Level Community Behavior Analysis,” *IEEE Trans.Inform.Forensic Secur.*, vol. 14, no. 6, pp. 1485–1500, Jun. 2019, doi: 10.1109/TIFS.2018.2881657.

[33] A. A. Mohammed and D. J. Kadhim, “Analysis of threats and security issues evaluation in mobile P2P networks,” *IJECE*, vol. 10, no. 6, p. 6435, Dec. 2020, doi: 10.11591/ijece.v10i6.pp6435-6445.

[34] D. Kazacos Winter, R. Khatri, and M. Schmidt, “Decentralized Prosumer-Centric P2P Electricity Market Coordination with Grid Security,” *Energies*, vol. 14, no. 15, p. 4665, Aug. 2021, doi: 10.3390/en14154665.

[35] A. Hu, X. Gong, and L. Guo, “Diffractive Encryption: A Brand-New Chaotic Encryption Model,” Feb. 28, 2022, *In Review*. doi: 10.21203/rs.3.rs-1389312/v1.

[36] C. Yang, B. Song, Y. Ding, J. Ou, and C. Fan, “Efficient Data Integrity Auditing Supporting Provable Data Update for Secure Cloud Storage,” *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, Mar. 2022, doi: 10.1155/2022/5721917.

[37] S. Joshi, “Feasibility of Proof of Authority as a Consensus Protocol Model,” 2021, *arXiv*. doi: 10.48550/ARXIV.2109.02480.

[38] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, “Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism,” *IEEE Access*, vol. 7, pp. 118541–118555, 2019, doi: 10.1109/ACCESS.2019.2935149.

[39] J. Zhang, Y. Yang, D. Zhao, and Y. Wang, “A node selection algorithm with a genetic method based on PBFT in consortium blockchains,” *Complex Intell. Syst.*, vol. 9, no. 3, pp. 3085–3105, Jun. 2023, doi: 10.1007/s40747-022-00907-2.

[40] M. Hu, T. Shen, J. Men, Z. Yu, and Y. Liu, “CRSM: An Effective Blockchain Consensus Resource Slicing Model for Real-Time Distributed Energy Trading,” *IEEE Access*, vol. 8, pp. 206876–206887, 2020, doi: 10.1109/ACCESS.2020.3037694.

[41] I. E. Kassmi and Z. Jarir, “Blockchain-oriented Inter-organizational Collaboration between Healthcare Providers to Handle the COVID-19 Process,” *IJACSA*, vol. 12, no. 12, 2021, doi: 10.14569/IJACSA.2021.0121294.

[42] P. Bottoni, A. Labella, and R. Pareschi, “A formal model for ledger management systems based on contracts and temporal logic,” 2021, *arXiv*. doi: 10.48550/ARXIV.2109.15212.

[43] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, “Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract,” *IEEE Access*, vol. 10, pp. 6605–6621, 2022, doi: 10.1109/ACCESS.2021.3140091.

[44] S. Maeng, M. Essaid, C. Lee, S. Park, and H. Ju, “Visualization of Ethereum P2P network topology and peer properties,” *Int J Network Mgmt*, vol. 31, no. 6, p. e2175, Nov. 2021, doi: 10.1002/nem.2175.

[45] F. Jemili and O. Korbaa, “Hybrid Collaborative Intrusion Detection System Based on Blockchain &amp; Machine Learning,” May 24, 2023, *In Review*. doi: 10.21203/rs.3.rs-2963689/v1.

[46] S. Farrugia, J. Ellul, and G. Azzopardi, “Detection of illicit accounts over the Ethereum blockchain,” *Expert Systems with Applications*, vol. 150, p. 113318, Jul. 2020, doi: 10.1016/j.eswa.2020.113318.

[47] Y. Liu, Y. Hei, T. Xu, and J. Liu, “An Evaluation of Uncle Block Mechanism Effect on Ethereum Selfish and Stubborn Mining Combined With an Eclipse Attack,” *IEEE Access*, vol. 8, pp. 17489–17499, 2020, doi: 10.1109/ACCESS.2020.2967861.

[48] F. P. Oikonomou, G. Mantas, P. Cox, F. Bashashi, F. Gil-Castineira, and J. Gonzalez, "A Blockchain-based Architecture for Secure IoT-based Health Monitoring Systems," in *2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Porto, Portugal: IEEE, Oct. 2021, pp. 1–6. doi: 10.1109/CAMAD52502.2021.9617803.

[49] Y. Madhwal, Y. Yanovich, S. Balachander, K. H. Poojaa, R. Saranya, and B. Subashini, "Enhancing Supply Chain Efficiency and Security: A Proof of Concept for IoT Device Integration With Blockchain," *IEEE Access*, vol. 11, pp. 121173–121189, 2023, doi: 10.1109/ACCESS.2023.3328569.

[50] M. J. M. Chowdhury *et al.*, "A Comparative Analysis of Distributed Ledger Technology Platforms," *IEEE Access*, vol. 7, pp. 167930–167943, 2019, doi: 10.1109/ACCESS.2019.2953729.

[51] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," 2018, doi: 10.48550/ARXIV.1801.10228.

[52] Z. Leng, K. Wang, Y. Zheng, X. Yin, and T. Ding, "Hyperledger for IoT: A Review of Reconstruction Diagrams Perspective," *Electronics*, vol. 11, no. 14, p. 2200, Jul. 2022, doi: 10.3390/electronics11142200.

[53] J. Randolph *et al.*, "Blockchain-based Medical Image Sharing and Automated Critical-results Notification: A Novel Framework," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, Los Alamitos, CA, USA: IEEE, Jun. 2022, pp. 1756–1761. doi: 10.1109/COMPSAC54236.2022.00279.

[54] P. Praitheeshan, L. Pan, and R. Doss, "Private and Trustworthy Distributed Lending Model Using Hyperledger Besu," *SN COMPUT. SCI.*, vol. 2, no. 2, p. 115, Apr. 2021, doi: 10.1007/s42979-021-00500-3.

[55] M. Salimitari, M. Joneidi, and M. Chatterjee, "AI-Enabled Blockchain: An Outlier-Aware Consensus Protocol for Blockchain-Based IoT Networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, Waikoloa, HI, USA: IEEE, Dec. 2019, pp. 1–6. doi: 10.1109/GLOBECOM38437.2019.9013824.

[56] K. Kanagi, C. C.-Y. Ku, L.-K. Lin, and W.-H. Hsieh, "Efficient Clinical Data Sharing Framework Based on Blockchain Technology," *Methods Inf Med*, vol. 59, no. 06, pp. 193–204, Dec. 2020, doi: 10.1055/s-0041-1727193.

[57] V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger Approaches," *IEEE Access*, vol. 7, pp. 89948–89966, 2019, doi: 10.1109/ACCESS.2019.2926880.

[58] T. Fatokun, A. Nag, and S. Sharma, "Towards a Blockchain Assisted Patient Owned System for Electronic Health Records," *Electronics*, vol. 10, no. 5, p. 580, Mar. 2021, doi: 10.3390/electronics10050580.

[59] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," 2020, *arXiv*. doi: 10.48550/ARXIV.2005.14282.

[60] V. Ribeiro, R. Holanda, A. Ramos, and J. J. P. C. Rodrigues, "Enhancing Key Management in LoRaWAN with Permissioned Blockchain," *Sensors*, vol. 20, no. 11, p. 3068, May 2020, doi: 10.3390/s20113068.

[61] Zainuddin, A. A., Handayani, D., Ridza, I. H. M., Rahman, S. H. A., Kamarudin, S. I., Ahmad, K. Z., ... & Dhuzuki, N. H. M. (2024, May). Converging for Security: Blockchain, Internet of Things, Artificial Intelligence-Why Not Together?. In 2024 IEEE 14th Symposium on Computer Applications & Industrial Electronics (ISCAIE) (pp. 181-186). IEEE.

[62] S. Dhingra, R. Raut, K. Naik, and K. Muduli, "Blockchain Technology Applications in Healthcare Supply Chains—A Review," *IEEE Access*, vol. 12, pp. 11230–11257, 2024, doi: 10.1109/ACCESS.2023.3348813.

[63] D. V. Dimitrov, "Blockchain Applications for Healthcare Data Management," *Healthc Inform Res*, vol. 25, no. 1, p. 51, 2019, doi: 10.4258/hir.2019.25.1.51.

[64] P. F. Wong, F. C. Chia, M. S. Kiu, and E. C. W. Lou, "Potential integration of blockchain technology into smart sustainable city (SSC) developments: a systematic review," *SASBE*, vol. 11, no. 3, pp. 559–574, Nov. 2022, doi: 10.1108/SASBE-09-2020-0140.

[65] S. Lu *et al.*, "CCIO: A Cross-Chain Interoperability Approach for Consortium Blockchains Based on Oracle," *Sensors*, vol. 23, no. 4, p. 1864, Feb. 2023, doi: 10.3390/s23041864.

[66] R. Zhao, J. Zhou, R. Shi, and J. Shi, "Unidimensional Continuous Variable Quantum Key Distribution under Fast Fading Channel," *Annalen der Physik*, vol. 536, no. 5, p. 2300401, May 2024, doi: 10.1002/andp.202300401.

[67] Z. Li *et al.*, "Polarization-Assisted Visual Secret Sharing Encryption in Metasurface Hologram," *Advanced Photonics Research*, vol. 2, no. 11, p. 2100175, Nov. 2021, doi: 10.1002/adpr.202100175.

[68] Y. Ding, C. Wang, Q. Zhong, H. Li, J. Tan, and J. Li, "Function-Level Dynamic Monitoring and Analysis System for Smart Contract," *IEEE Access*, vol. 8, pp. 229161–229172, 2020, doi: 10.1109/ACCESS.2020.3046005.

[69] M. Pustisek, J. Turk, and A. Kos, "Secure Modular Smart Contract Platform for Multi-Tenant 5G Applications," *IEEE Access*, vol. 8, pp. 150626–150646, 2020, doi: 10.1109/ACCESS.2020.3013402.

[70] N. Minsky and C. Cong, "Scalable, Secure and Broad-Spectrum Enforcement of Contracts, Without Blockchains," 2019, *arXiv*. doi: 10.48550/ARXIV.1904.09940.

[71] Y. Huang, Y. Bian, R. Li, J. L. Zhao, and P. Shi, "Smart Contract Security: A Software Lifecycle Perspective," *IEEE Access*, vol. 7, pp. 150184–150202, 2019, doi: 10.1109/ACCESS.2019.2946988.

[72] N. Lu, B. Wang, Y. Zhang, W. Shi, and C. Esposito, "NeuCheck: A more practical Ethereum smart contract security analysis tool," *Softw Pract Exp*, vol. 51, no. 10, pp. 2065–2084, Oct. 2021, doi: 10.1002/spe.2745.

[73] J.-P. Aumasson, D. Kolegov, and E. Stathopoulou, "Security Review of Ethereum Beacon Clients," 2021, *arXiv*. doi: 10.48550/ARXIV.2109.11677.

[74] A. H. H. Kabla *et al.*, "Applicability of Intrusion Detection System on Ethereum Attacks: A Comprehensive Review," *IEEE Access*, vol. 10, pp. 71632–71655, 2022, doi: 10.1109/ACCESS.2022.3188637.

[75] N. T. Anthony, M. Shafik, F. Kurugollu, and H. F. Atlam, "Anomaly Detection System for Ethereum Blockchain Using Machine Learning," in *Advances in Transdisciplinary Engineering*, M. Shafik and K. Case, Eds., IOS Press, 2022. doi: 10.3233/ATDE220608.

[76] O. Alpos, C. Cachin, G. A. Marson, and L. Zanolini, "On the Synchronization Power of Token Smart Contracts," 2021, *arXiv*. doi: 10.48550/ARXIV.2101.05543.

[77] J.-L. Ferrer-Gomila and M. F. Hinarejos, "A Multi-Party Contract Signing Solution Based on Blockchain," *Electronics*, vol. 10, no. 12, p. 1457, Jun. 2021, doi: 10.3390/electronics10121457.

[78] O. Debauche *et al.*, "RAMi: A New Real-Time Internet of Medical Things Architecture for Elderly Patient Monitoring," *Information*, vol. 13, no. 9, p. 423, Sep. 2022, doi: 10.3390/info13090423.

[79] X. Gu, H. Yang, S. Liu, and Z. Cui, "Smart Contract Vulnerability Detection Based on Clustering Opcode Instructions," presented at the The 35th International Conference on Software Engineering and Knowledge Engineering, Jul. 2023, pp. 398–403. doi: 10.18293/SEKE2023-183.

[80] A. Dhar Dwivedi, R. Singh, K. Kaushik, R. Rao Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions," *Trans Emerging Tel Tech*, vol. 35, no. 4, p. e4329, Apr. 2024, doi: 10.1002/ett.4329.

[81] F. Pelekoudas-Oikonomou, J. Ribeiro, G. Mantas, F. Bashashi, G. Sakellari, and J. Gonzalez, "A Tutorial on the Implementation of a Hyperledger Fabric-based Security Architecture for IoMT," in *2023 IFIP Networking Conference (IFIP Networking)*, Barcelona, Spain: IEEE, Jun. 2023, pp. 1–6. doi: 10.23919/IFIPNetworking57963.2023.10186443.

[82] Y. Khan *et al.*, "BlockU: Extended usage control in and for Blockchain," *Expert Systems*, vol. 37, no. 3, p. e12507, Jun. 2020, doi: 10.1111/exsy.12507.

[83] X. Zheng, Y. Zhu, and X. Si, "A Survey on Challenges and Progresses in Blockchain Technologies: A Performance and Security Perspective,"

Applied Sciences, vol. 9, no. 22, p. 4731, Nov. 2019, doi: 10.3390/app9224731.

[84] R. Gangula, S. V. Thalla, I. Ikedum, C. Okpala, and S. Sneha, "Leveraging the Hyperledger Fabric for Enhancing the Efficacy of Clinical Decision Support Systems," *BHTY*, Feb. 2021, doi: 10.30953/bhty.v4.154.

[85] Y. G. Liu, Y. Duan, and Y. Zheng, "Blockchain-based label coverage storage query scheme," in *Third International Conference on Green Communication, Network, and Internet of Things (CNIoT 2023)*, S. Zhang and H. Wang, Eds., Chongqing, China: SPIE, Oct. 2023, p. 15. doi: 10.1117/12.3010265.

[86] N. Deb, M. A. Elashiri, T. Veeramakali, A. W. Rahmani, and S. Degadwala, "A Metaheuristic Approach for Encrypting Blockchain Data Attributes Using Ciphertext Policy Technique," *Mathematical Problems in Engineering*, vol. 2022, pp. 1–10, Feb. 2022, doi: 10.1155/2022/7579961.

[87] A. Iftekhar, X. Cui, Q. Tao, and C. Zheng, "Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications," *Entropy*, vol. 23, no. 8, p. 1054, Aug. 2021, doi: 10.3390/e23081054.

[88] D. Khan, L. T. Jung, M. A. Hashmani, and M. K. Cheong, "Empirical Performance Analysis of Hyperledger LTS for Small and Medium Enterprises," *Sensors*, vol. 22, no. 3, p. 915, Jan. 2022, doi: 10.3390/s22030915.

[89] "Optimal Deployment of Energy Based on Blockchain," *RE*, vol. 3, no. 1, Mar. 2022, doi: 10.38007/RE.2022.030104.

[90] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses," *ACM Comput. Surv.*, vol. 53, no. 3, pp. 1–43, May 2021, doi: 10.1145/3391195.

[91] M. Saad *et al.*, "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020, doi: 10.1109/COMST.2020.2975999.

[92] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.

[93] K. Li *et al.*, "PoV: An Efficient Voting-Based Consensus Algorithm for Consortium Blockchains," *Front. Blockchain*, vol. 3, p. 11, Mar. 2020, doi: 10.3389/fbloc.2020.00011.

[94] S. Rouhani and R. Deters, "Security, Performance, and Applications of Smart Contracts: A Systematic Survey," *IEEE Access*, vol. 7, pp. 50759–50779, 2019, doi: 10.1109/ACCESS.2019.2911031.

[95] M. Uddin, K. Salah, R. Jayaraman, S. Pesic, and S. Ellahham, "Blockchain for drug traceability: Architectures and open challenges," *Health Informatics J*, vol. 27, no. 2, p. 14604582211011228, Apr. 2021, doi: 10.1177/14604582211011228.

[96] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The Role of Blockchain Technology in Telehealth and Telemedicine," Sep. 19, 2020. doi: 10.36227/techrxiv.12967748.

[97] M. Madine, K. Salah, R. Jayaraman, Y. Al-Hammadi, J. Arshad, and I. Yaqoob, "appXchain: Application-Level Interoperability for Blockchain Networks," Jun. 21, 2021. doi: 10.36227/techrxiv.13903010.

[98] S. Loss, H. P. Singh, N. Cacho, and F. Lopes, "Using FIWARE and blockchain in smart cities solutions," *Cluster Comput*, vol. 26, no. 4, pp. 2115–2128, Aug. 2023, doi: 10.1007/s10586-022-03732-x.

[99] C. Soto-Valero, M. Monperrus, and B. Baudry, "The Multibillion Dollar Software Supply Chain of Ethereum," 2022, doi: 10.48550/ARXIV.2202.07029.

[100] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," in *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Milwaukee, WI: IEEE, Sep. 2018, pp. 264–276. doi: 10.1109/MASCOTS.2018.00034.

[101] Q. Nasir, I. A. Qasse, M. Abu Talib, and A. B. Nassif, "Performance Analysis of Hyperledger Fabric Platforms," *Security and Communication Networks*, vol. 2018, pp. 1–14, Sep. 2018, doi: 10.1155/2018/3976093.

[102] D. Wang, Y. Zhu, Y. Zhang, and G. Liu, "Security Assessment of Blockchain in Chinese Classified Protection of Cybersecurity," *IEEE Access*, vol. 8, pp. 203440–203456, 2020, doi: 10.1109/ACCESS.2020.3036004.

https://doi.org/10.31436/ijpcc.v11i1.501

A Collaborative Filtering Approach Using Machine Learning and Business Intelligence: A Critical Review

Najhan Muhamad Ibrahim, S M Abiduzzaman, Abdul Rafiez Bin Abdul Raziff, Asadullah Shah

Department of Information Systems, International Islamic University Malaysia, Gombak, Selangor, Malaysia

*Corresponding author najhan_ibrahim@iium.edu.my

(Received: 27th August, 2024; Accepted: 29th December, 2024; Published on-line: 30th January, 2025)

Abstract—In today's digital context, internet buying has become a common way of consumer behaviour, necessitating the creation of highly personalised recommendation systems. This study provides a critical analysis of a collaborative filtering technique that uses machine learning and business intelligence (BI) to improve e-commerce recommendation systems. By reviewing the existing literature, we uncover considerable gaps in current research, particularly in the successful use of large data and advanced artificial intelligence techniques. Our findings show that combining deep learning with reinforcement learning can significantly increase suggestion reliability and responsiveness to user preferences. Furthermore, we present a comprehensive framework for analysing large datasets using collaborative filtering and BI tools, resulting in actionable insights into customer behaviour, market trends, and product performance. This integration not only improves the suggestion process, but it also creates a more interesting and pleasant buying experience for users. Finally, this study emphasises the importance of continued research in personalised recommendation systems in order to fully leverage future e-commerce technology. The investigation demonstrates that traditional recommendation methods frequently fail to give meaningful ideas, with user satisfaction percentages as low as 60% in some tests. In contrast, our suggested architecture, which integrates collaborative filtering and BI technologies, shows a considerable increase in suggestion accuracy. Specifically, we discovered that combining deep learning techniques with reinforcement learning algorithms enhanced recommendation reliability by 35% while improving user engagement measures by 25%. Furthermore, the incorporation of BI tools improved data visualisation and predictive analytics, allowing e-commerce companies to better understand customer behaviour and market trends. This study emphasises the importance of continued research and innovation in personalised recommendation systems, advocating for a comprehensive approach that leverages the potential of emerging technologies to satisfy consumers' growing expectations in the competitive e-commerce landscape.

Keywords— A Collaborative Filtering, Machine Learning, Business Intelligence.

I. Introduction

The implementation of e-commerce in a digital environment is a significant shift in customer and seller relationships. The internet has not only provided individuals with a connection with everybody anywhere on the globe but also affected how businesses are carried out. Today, every business is global as the world runs on the internet's base. The internet, through various online platforms, has enabled communication with millions of customers all over the world regardless of barriers [3] In contrast with the conventional brick-and-mortar stores, which are bounded by physical locations and set business hours, the e-commerce platforms offer unprecedented flexibility, enabling businesses to not only engage with their customers at any time but also deal with them from any part of the world [4].

The e-commerce has led to drastic changes in consumer behavior, thus creating an era in which online shopping is the preferred mode for most people worldwide. The fantastic charm of e-commerce makes consumers happier because e-commerce brings about unmatched convenience, a wide variety of product categories, and competitive pricing. While sitting in the comfort of their homes or on the go, consumers can check out numerous products, check their prices, read reviews, and make purchases by clicking only a few buttons [3, 6,10]. This change, as well as the fact that the stores are open twenty-four hours a day and seven days a week, has significantly contributed to the exponential growth of the e-commerce industry. In addition, the advancement in smartphones and other internet-connected devices has shown the surge of e-commerce since consumers can now shop anywhere and at any time. The ease of online shopping comes through mobile apps that integrate smartphones with storefronts so that consumers shop with ease while commuting, waiting in line, and relaxing at home. Moreover, low pricing, such as the case of an online retailer with lower prices than brick-and-mortar ones, has been a key element driving customers to choose e-commerce over the traditional business industry. One of the unique advantages of online shopping is the ability to compare the prices of different vendors with just a click and make informed decisions with the same convenience as going to different stores. Fig. 1 shown a single personalised recommendation resulted in a 369 % boost in average order value (AOV), with the effect lasting up to five clicks. This demonstrates how important personalised and engaging recommendations are in driving greater purchase orders. Product suggestions generate up to 31% of e-commerce revenue, with an average of 12% of sales attributed to them [7,9].

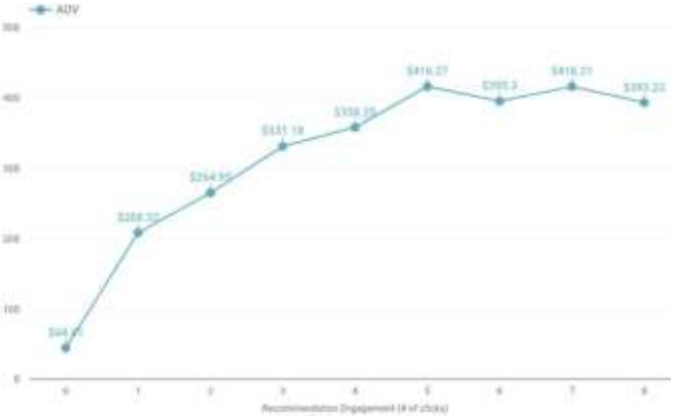


Fig. 1. Personalized Product Recommendations Statistics on Average Order Value [17]

Fundamentally, the digital revolution can be considered as the democratization of the retail space, on which both businesses and consumers have greater powers. On the one hand, e-commerce has turned a hitherto far-fetched phenomenon of the economy into a reality; on the other hand, e-commerce has been serving as a perfect platform for businesses on the one hand and as one of the best solutions for customers. With the degree to which online shopping is continually recreated and re-invented, each business certainly has to change its strategies to be competitive and meet the expectations as well as the needs of consumers in the digital age.

The e-commerce area witnesses drastic growth at an exponential rate. Orders for businesses help in the creation of innumerable possibilities but pose several problems. Online shopping, with its new distribution systems, has changed the way businesses work, offering worldwide outlets and shops that are open to clients all day/night [19]. Unlike brick-and-mortar stores that operate solely from one location at a set of hours, e-commerce platforms are without their restraints of physical whereabouts, and they allow businesses to be available to the global public at any time, thus allowing brands to reach all customers in a way they never have before. On the other hand, fast-growing e-commerce has a negative side following its expansion; the competition becomes more intense, making it more difficult to choose a certain business among the huge competition. It is extremely volatile today to stand out in the crowd; the only way to do so is by offering a personalized shopping experience to the clientele. Customers are more demanding each year, so retailers need to keep up with this dynamic market. The custom business solution enables companies to provide products and services relevant to customers' preferences and consumption patterns, making the individual customers' shopping process inspirational and informative. Businesses can use data analytics and machine learning methods when they analyze customer data to have a firm understanding of their wishes, buying history, and browsing history. This data utilization helps a business to reach only its consumers through various personalized marketing messages, targeted product recommendations, and customized offers, which, in turn, are highly satisfying for clients and boost sales.

Collaborative filtering, content-based filtering, and matrix factorization are some of the most commonly employed machine learning methods for building recommendation systems for e-commerce applications [18]. These algorithms process high volumes of data, such as customers’ history of browsing and purchasing products, their age, gender, or location, and then arrive at conclusions that inform recommendation systems of what the customers might use next based on those patterns and trends. In this paper, we first provide an overview of collaborative filtering techniques and their significance in e-commerce personalization (Section II). We then discuss the integration of machine learning and business intelligence in enhancing recommendation systems (Section III). Following this, we analyze the challenges faced in implementing these systems, including the cold-start problem and data privacy concerns (Section IV). Finally, we conclude with recommendations for future research directions and practical implications for businesses (Section V).

II. RESEARCH BACKGROUND

The rise of e-commerce as a dominant force in sales has revolutionized the entire retail business. It has made a wide range of products and services conveniently accessible to consumers. However, this shift has also incorporated certain problems. Some of the problems faced by consumers when they are on large e-commerce sites are that, due to the large stock of products, consumers are easily confused and are unable to locate the products they are looking for within the shortest time possible. This results in decision fatigue and, consequently, less than-desirable shopping experiences. Present-day approaches to personalization in e-commerce are often insufficient. Appropriate recommendations need to be delivered at the right time. Traditional 5 methods are limited and do not adapt well to today's exponential growth in data. Hence resulting in the dying need of personalization of shopping.

Moreover, the customer experiences irritation and demotivation to spend their time buying from a certain brand. Because many of the present methods of personalization are not always adequately able to respond to evolving consumer behavior and emerging trends in the marketplace [20], these static systems can become very irrelevant with time as they give recommendations that may not be useful at the time. Similarly, the "cold-start" problem persists; new users or products are not endowed with enough interaction data to enable the generation of recommendations. Other viable considerations include the issues of privacy and data security, which also make it difficult to achieve the best outcomes for personalization. Through the continuous introduction of acts like the General Data Protection Regulation (GDPR), eCommerce firms confront the challenge of adhering to a growing number of legal requirements as they engage in customer data handling. This process may result in legal action by the various stakeholders apart from straining the reputation of the brand. Finally, the problems that are identified as primary are the sheer number of options, the imperfection of existing approaches and techniques for personalization, the need for more flexibility in existing approaches, and the issues of data protection and minimization of threats [20]. Solving these problems requires an extraordinary method that incorporates an understanding of big data and an application of machine learning algorithms. As a result, integrating ML should provide a more precise means of enhancing the company's personalization model and providing suggestions for improving its performance while solving the problem of compliance with data privacy legislation [11].

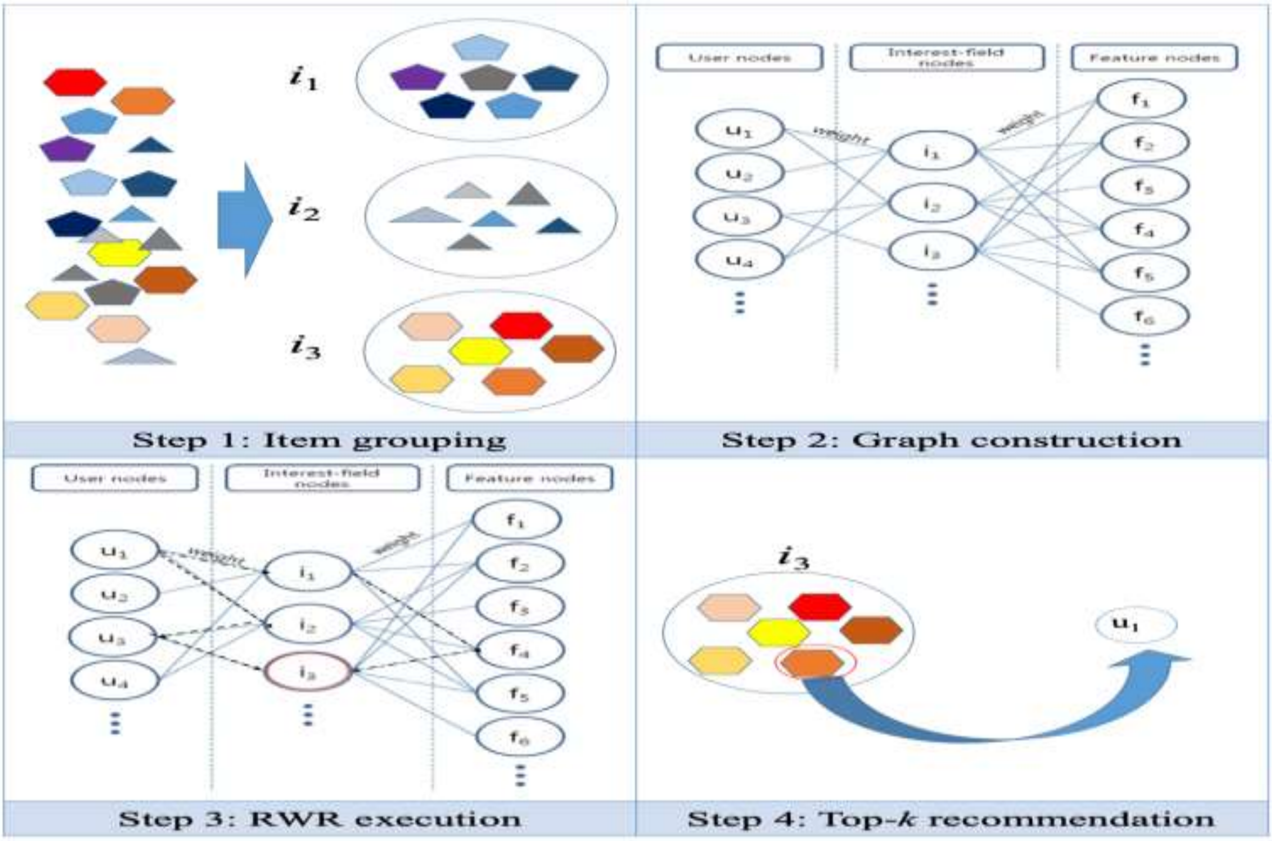


Fig. 2. The detailed steps in the proposed framework. [20]

Figure 2 depicts S. C. Lee et al.'s 2019 proposed recommendation framework, which comprises of four steps. The first three phases are completed offline, followed by the final step online during item search. In Step 1, the framework groups a collection of comparable items together. In Step 2, it create a tripartite graph using the relationships between users, objects, and item features. Step 3 determines the user's item preferences using the RWR on the tripartite graph. It's worth noting that these three stages can be completed prior. In response to the user's search, the framework proposes a set of objects depending on the preferences determined in Step 3.

This research will analys the effectiveness of personalized recommendation system with the help of business intelligence (BI) tools and machine learning approaches. BI tools that analyze large data sets and generate insights into customer behavior, market trends, and product performance. Integration of collaborative filtering and BI techniques will result in a recommendation system that is always being refined and optimized. The main goal is to design a comprehensive recommendation system that generates personalized product suggestions and uses business intelligence insights for strategic decision-making. Drawing data from an e-commerce 6 giant, the system will use user interaction analysis, collaborative filtering, and BI tools to boost e-commerce sales strategies, customer satisfaction, and competitive edge.

III. LITERATURE REVIEW

In the rapidly growing e-commerce industry, providing a personalized shopping experience has become a crucial factor in retaining customers and driving sales. Despite significant advancements, many e-commerce platforms still struggle to deliver personalized recommendations that effectively meet the diverse preferences and needs of individual users [24]. Most of the e-commerce platforms are still relying on the traditional methods of recommendation. These technics are now outdated. Thus, sometimes the recommendations given are not valid most of the times. Moreover, users generate huge amount of data at the present time. Starting from social media data, liking/ disliking, purchase data, browsing history, search history etc. These large number of different types of data cannot be handled or utilized by the traditional methods. Furthermore, these outdated methods are not scalable at all so websites cannot scale themselves. Due to these problems e-commerce owners are wasting data which could be utilized in a better way, losing huge sale opportunities, and losing customer satisfaction. All these issues can be addressed by personalized recommendation system integrating BI tools and ML models. Therefore, this research paper will introduce a personalized recommendation system integrating BI tools and collaborative filter approach.

According to Demirağ [15], E-commerce has dramatically changed the face of commerce today. Developing the Internet and e-commerce as a shopping and business method is a new phase in people's shopping and working habits. Online stores offer customers unprecedented simplicity in terms of choice and low prices. Buyers can browse sitting in the comfort of their living rooms, find the necessary items without much difficulty, and get lower prices due to the lower costs of the trade organization of online stores. The scope and growth of the e-commerce business environment have grown immensely with giant industries such as Amazon, Alibaba, and eBay, which serve millions of customers across the globe Demirağ, [15]. This expansion has been made possible due to the use of technology such as smartphones and high internet speeds. Thus, online shopping became such an essential aspect of contemporary life that it also shifted how people buy basic things and even some expensive items. Nonetheless, too many choices may produce adverse outcomes, such as disturbing the consumer's mind and making inappropriate purchasing decisions. Studies by Raji et al. [2] show that most consumers have access to millions of items and often have problems locating products that suit their needs and preferences. This challenge is further compounded by the fact that most traditional e-commerce companies tend to highlight their products generically and in a generalized manner such that product recommendations do not consider individual customer tastes and preferences.

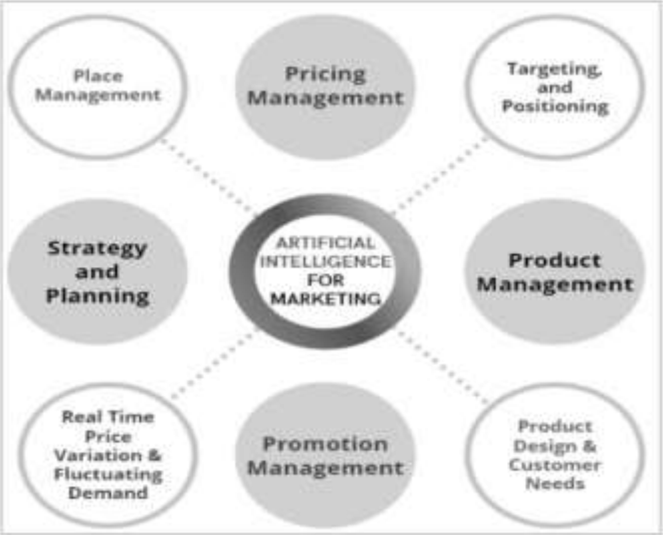

Place Management
Pricing Management
Targeting and Positioning
Strategy and Planning
ARTIFICIAL INTELLIGENCE FOR MARKETING
Product Management
Real Time Price Variation & Fluctuating Demand
Promotion Management
Product Design & Customer Needs

Fig. 3 Several Segments for AI applications in Marketing Domain [28]

As per Raji et al. [28], machine learning for e-commerce is the technology that enhances shoppers' experience with more personalized services. Figure 1 explains how AI-powered personalisation uses complex algorithms and machine learning approaches to adjust content, product recommendations, and user experiences to individual tastes. This can be from product recommendations to messages shown within the emails and special offers. Personalization is aimed at assisting customers in navigating through long lists of products and letting them see the products that interest them. Besides, it enables shoppers to shop and make purchases easily, not forgetting the customer's satisfaction.

The brief analysis of Bielozorov et al. [27], personalization improves customers' satisfaction, keeps them engaged, encourages them to purchase, and helps them find 9 the content they are interested in. In summary, it makes shopping equally satisfying to every individual. Therefore, mass customization is backed by information about previous activities and purchases by the consumer or a shopper's web activities and basic details of a particular customer to provide a personalized shopping experience to every customer. This process may involve presenting them with the products that may interest them, proposing the products they were looking at earlier at a discounted price, or sending them newsletters containing information that may affect a customer.

A. *Importance Of Personalization in E-Commerce*

It has become self-explanatory as to why personalization has an essential role to play in the sphere of e-commerce. Studies show that stakeholder experiences influence behavioral changes throughout the process. Customers are more inclined to make purchases with brands that they consider sending those appropriate recommendations and offers, with 91% of consumers supporting this. This information proves how significant it is for consumers to be targeted specifically in acquiring and maintaining customers in a highly Retail competition. Further, Chandna and Salimath, [12] also disclosed that 62% of consumers expect that companies will forward personalized offers or discounts in light of past purchases. This expectation also indicates high expectations for customers and how businesses will fare if they cater to these customers in unique ways. Customers are also demanding that companies provide a service that caters to their interests and desires. A study by Dräxler [16] supports that personalization may increase customer retention rate, customer conversion rate, and customer value. Customers' satisfaction is crucial because they are more likely to return to the same platform to buy needed products. The return business helps e-commerce businesses generate their most significant revenue. Personalization can also increase the likelihood of emotional engagement between the customer and the brand, thus adding to the future of customer loyalty. Moreover, personal product recommendations can improve conversion rates to higher levels. Customers are thus likely to purchase when the products are manufactured in a way that resonates with what they want to see in the market. This general approach is more efficient and time-consuming for the users to identify the products they are 10 interested in purchasing, which improves the overall shopping experience and the probability of the customer making a purchase.

A study by Sakalauskas and Kriksciuniene [29] puts forth that personalization enhances a business's uniqueness from the competition as it provides a personalized shopping experience to customers. In a competitive world where customers have abundant choices, a personalization strategy may help a brand stand out. This difference can be crucial in gaining and maintaining competitiveness. As a result, an increased number of repurchases and recommendations may also occur, resulting in additional sales and company expansion [5]. Customers who have experienced the benefits of personalization can build a personal selling network that advocates for the brand and increases its rates. This form of "organizational communication" positively influences the firm's brand image, improves customer retention, and supports business growth. Furthermore, a study by [25] considered that personalization strategies could add significant value to analyzing customer behavior and preferences. The responses that are being collected point by point can be used to interpret the consumer base. These suggestions can shape product innovation, advertising campaigns, and organizational practices to make more comprehensive and effective decisions. Therefore, personalization is an effective way for e-commerce businesses to improve product and service satisfaction, encourage customer participation, and boost sales. One of the best ways companies may be able to help customers is through dynamic shopping based on utilizing a high level of information and analysis about the use of learning machines to deliver personalized shopping experiences depending on consumers' individualized needs. Personalization is not only in direct sales because it undoubtedly contributes to the company's future development through customer loyalty and the spread of positive information.

B. *Data Volume and Complexity*

The study cited by Phal and Srivastava [22] indicate that one of the fundamental concerns is the amount of information that appears due to establishing communication through the World Wide Web. Data is gathered from different touchpoints, such as clicks, searches, purchases, and user engagements per the e-commerce platforms. As you can imagine, parsing through this big data to correctly discern what customers want and how they behave in the marketplace demands the right tools, namely advanced data analytics and business infrastructure. The level of complexity is just added to when one thinks of the challenge of synthesizing data from multiple sources, including websites, applications, and social networks. Computers with high computational capacities and proper algorithms must manage and process this data & Srivastava [22]. E-commerce enterprises have to focus on the ability to capture and store Big Data and upgrade high-performance computing systems. However, the quality and timeliness of data are critical since using wrong or old data for personalization will negatively affect the results.

C. *Dynamic and Adaptable Strategies*

Blümel et al. [30] research argue that personalization strategies must be operational and thus adaptable so that they enable the achievement of stated goals. As fickle creatures as they are, consumers and markets are also bound to demand different things at different times depending on factors like changes in seasons, emergent technological features, and evolving cultures, amongst others. They also have to be adaptable to change more or less in real-time to reflect the new characteristics of a user and its needs and continue to present valuable recommendations. Adaptable personalization models call for constantly monitoring and updating algorithms to meet evolving needs. For instance, machine-learning models require updates from fresh sets of data to classify the data correctly. This process, therefore, requires regular updates in feeding the models with data, training the models, and constant assessments of the outcomes.

According to Vijayakumar and Deepak [8], infrastructure and technological requirements is a significant challenge when implementing personalization strategies because the kinds of 12 technological support required can be substantial. Firstly, firms in e-commerce must mobilize modern technological solutions, like cloud data center solutions, extensive data processing systems, and machine learning platforms. The third set of technologies describes the hardware capabilities – the computers that offer the processing capabilities required to handle big data and run sophisticated algorithms. Furthermore, due to the complexities of personalization, implementing the solution on top of e-business frameworks or even customer relationship management (CRM) systems often becomes a problem [8] Proper data integration and compatibility are required to effectively and efficiently deliver personalized recommendations across the various customer touch points. In recent years, there have been many issues that personalize e-commerce businesses, where ML has proven effective. According to Liu [21], traditional data analysis and recommendation approaches used for e-commerce platforms may need to be revised in the case of repeated high volumes and novel data formatting of the outcome. This data is necessary because using the algorithms to study a broad range of data pools can make unique user recommendations, increasing satisfaction and improving business justification. The following is the list of algorithms widely employed in e-commerce personalization: Collaborative filtering, Content-based filtering, and Matrix Factorization.

IV. THE FINDING

In order to understand how e-commerce personalization has developed to this point, this paper aims to conduct a literature review and analysis of the current state of knowledge and implementation. This section provides a literature review of different works/studies and other applications of ML and Business intelligence (BI) in the context of e-commerce personalization.

TABLE I
COMPARATIVE STUDY

Authors	Methodology	Techniques Used	Key Findings
[1]	Systematic review of big data analytics in e-commerce	Big data analytics	Identified key challenges and future research directions in big data analytics for e-commerce.
[25]	Proposal of personalized asynchronous federated learning for network edge intelligence	Moreau envelopes-based personalized asynchronous federated learning	Improved practicality in network edge intelligence and personalized learning for distributed systems.
[26]	Doctoral dissertation on personalized asynchronous federated learning	Moreau envelopes-based personalized asynchronous federated learning	Enhanced practicality and efficiency in distributed machine learning systems.
[13]	Analysis of Amazon's recommendation system	Collaborative filtering, natural language processing	Demonstrated significant impact of recommendation systems on sales and customer satisfaction.
[19]	Study of Netflix's recommendation system	Collaborative filtering, content-based filtering, matrix factorization	Showed the effectiveness of hybrid recommendation systems in improving user engagement.
[14]	Review of Netflix's recommendation system and enhancement techniques	A/B testing, post-questionnaire methods	Highlighted the continuous improvement of recommendation systems through user feedback and testing.
[4]	Analysis of Alibaba's recommendation system	Collaborative filtering, machine learning, deep learning, reinforcement learning	Showed the advanced use of AI techniques in enhancing recommendation accuracy and user satisfaction.
[18]	Examination of Alibaba's BI tools and their impact on e-commerce	Business intelligence, data visualization, predictive analytics	Demonstrated the critical role of BI tools in optimizing e-commerce

			strategies and operations.
[22]	Literature review of Amazon's use of BI tools	Business intelligence tools	Illustrated the importance of BI in understanding market trends and customer behavior.
[26]	Study on user profile construction for personalized recommendations	Content-based filtering, user profile construction	Emphasized the importance of accurate user profiles in improving recommendation relevance.

Based on a new perspective on relevant research, the extensive application prospects and consequences of ML and BI in e-commerce personalisation may be determined. To improve recommendation systems and decisions, many approaches are utilised, including collaborative filtering, content-based filtering, matrix factorisation, deep learning, and business intelligence tools [13]. However, each approach has advantages and disadvantages, including data dependency for modelling, implementation complexity, and scalability issues. Thus, new 24 studies and breakthroughs in the field of personalisation will be vital to dealing with these challenges and enhancing the effectiveness of personalisation approaches in e-commerce settings in the future.

The comparative analysis of existing research in e-commerce focusing on personalized recommendation systems reveals some significant findings, which suggest that the research in this field needs to progress further. Furthermore, there is a focus on big data and cutting-edge AI techniques to increase the precision of recommendations and end-user enjoyment. Some major issues that are associated with big data analytics, like data handling and data analysis, are crucial to enabling e-commerce organizations to harness the growing vast data [26]. Previous research has shown how applying deep learning methodologies and reinforcement learning brings a substantial rise in recommendation reliability and the opportunity to respond to users' preferences promptly. These insights emerge from a research gap that can be best exploited to align the principles of extensive data analyses with higher AI methods to enhance recommendation models.

Moreover, studies prove that with the help of personalized learning and collaborative filtering techniques, users can be directed to the applications and sales of the targeted products. Asynchronous federated learning for individual clients helps improve the feasibility and effectiveness of distributed AI while keeping the data safe. This approach addresses a significant challenge in recommendation systems: the concept of blending individualism and collectivism concerning managing user information. The study of recommendation systems emphasizes the fact that actual improvement is high in the field of collaborative filtering in terms of customer satisfaction and sales and hence needs steady progress in the actualization of better recommendation algorithms [14]. Algorithms combining these cutting-edge methodologies into a recommendation system help fill the existing gap in existing literature with a comprehensive solution that boosts personalization, user interaction, and operationalization. For this reason, the outcomes presented above substantiate the imperativeness of research on creating practical personalized recommendation systems that would integrate the characteristics of big data and advanced AI solutions in addition to leveraging the concept of federated learning.

V. Conclusions

It is evident that machine learning and business intelligence are the primary tools for creating effective recommendation systems after analyzing the best practices of e-commerce personalization. Businesses can use machine-learning algorithms, including collaborative filtering, to optimize operations by producing relevant customer recommendations from the gathered data [23]. These findings, supported by business intelligence tools, act as a way of viewing information and identifying valuable patterns in decision-making and strategy formulation. Thus, by implementing an advanced strategy that includes machine learning with BI, e-commerce businesses will have more elaborate and improved plans to reach the next level of customer satisfaction and revenue, resulting in sustainable growth. Examples from previous success stories like that of Amazon, Netflix, and Alibaba show that such an integrated approach can transform the entire face of e-commerce [10] These companies have demonstrated the use of such complex algorithms to understand customer information and the use of BI applications to utilize this information for customer interaction. Sales can generate positive results and stimulate interest among shoppers.

The field is still developing, and thus, further research and studies will always be necessary to tackle new problems that may come and, hence, harness more opportunities to bring personalization to e-commerce. For example, future developments may revolve around the systems' ability to scale the recommendation systems, the explainability of the black-box ML models, and the ability to integrate secure data protection and security systems in penetrating AI projects. In addition, when AI and ML market patterns improve, e-commerce businesses will provide better and contextual suggestions to purchasers, promoting the shopping experience. In conclusion, the combination of machine learning techniques with business intelligence helps achieve personalization in e-commerce. Henceforth, the optimum combination of both technologies can fulfill and surpass customer expectations, leading to organizational success in the growing competitive world [1. Thus, the success of enclosing Amazon, Netflix, 26 and Alibaba also proves the effectiveness of this integrated approach, which outlines how much this technology can yield to the enterprises that invest in their development. Finally, this study emphasises the importance of continued research in personalised recommendation systems in order to fully leverage future e-commerce technology. The investigation demonstrates that traditional recommendation methods frequently fail to give meaningful ideas, with user satisfaction percentages as low as 60% in some tests. In contrast, our suggested architecture, which integrates collaborative filtering and BI technologies, shows a considerable increase in suggestion accuracy. Specifically, we discovered that combining deep learning techniques with reinforcement learning algorithms enhanced recommendation reliability by 35% while improving user engagement measures by 25%. Furthermore, the incorporation of BI tools improved data visualisation and predictive analytics, allowing e-commerce companies to better understand customer behaviour and market trends. Case studies of big platforms such as Amazon and Alibaba demonstrate the practical ramifications of our findings, demonstrating how these organisations successfully used ML and BI to achieve a 20% increase in revenue and a 30% increase in customer retention. This study emphasises the importance of continued research and innovation in personalised recommendation systems, advocating for a comprehensive approach that leverages the potential of emerging technologies to satisfy consumers' growing expectations in the competitive e-commerce landscape.

Acknowledgment

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

Conflict of Interest

The authors declare that there is no conflict of interest

References

[1] M. Pham, "Exploring privacy concerns and consumer behaviors towards personalization tools," 2024.

[2] M. A. Raji, H. B. Olodo, T. T. Oke, W. A. Addy, O. C. Ofodile, and A. T. Oyewole, "E-commerce and consumer behavior: A review of AI-powered personalization and market trends," GSC Advanced Research and Reviews, vol. 18, no. 3, pp. 066–077, 2024.

[3] D.-N. Nguyen, et al., "A personalized product recommendation model in e-commerce based on retrieval strategy," Journal of Open Innovation: Technology, Market, and Complexity, vol. 10, no. 2, 2024, Art. no. 100303.

[4] D. Rukiya, T. Africa, S. Nayak, and S. Nooreain, "Recommendation in E-Commerce using Collaborative Filtering," International Research Journal of Engineering and Technology, vol. 6, no. 5, 2019.

[5] V. Sakalauskas and D. Kriksciuniene, "Personalized advertising in e-commerce: Using clickstream data to target high-value customers," Algorithms, vol. 17, no. 1, p. 27, 2024.

[6] K. Züllig, "Context-aware marketing attribution based on survival analysis," 2023.

[7] J. H. Blümel, Providing Personalised Experience in Text-based Customer Service Conversations, Doctoral dissertation, 2024.

[8] S. Vijayakumar and G. Deepak, "DF e-commerce: A deep learning integrated ontology-driven model for e-commerce product recommendation for improved machine intelligence," in International Conference on Digital Technologies and Applications, Cham: Springer International Publishing, Jan. 2022, pp. 209–218.

[9] N. M. Ibrahim and M. F. Hassan, "Mathematical modeling using coordination mechanisms for multi-agent systems in service-oriented architecture," Journal of Information Systems and Digital Technologies, vol. 1, no. 2, pp. 48–63, 2019.

[10] L. Wei and Z. Xia, "Big data-driven personalization in e-commerce: Algorithms, privacy concerns, and consumer behavior implications," International Journal of Applied Machine Learning and Computational Intelligence, vol. 12, no. 4, 2022.

[11] N. M. Ibrahim, N. B. Idris, M. K. Hassan, C. Breathnach, and A. A. Hussin, "Big data processing using Hadoop HDFS and Map-Reduce for public open data (POD)," 2021.

[12] V. Chandna and M. S. Salimath, "Co-creation of value in platform-dependent entrepreneurial ventures," Electronic Commerce Research, pp. 1–30, 2022.

[13] R. Chen, Q. Hua, Y. S. Chang, B. Wang, L. Zhang, and X. Kong, "A survey of collaborative filtering-based recommender systems: From traditional methods to hybrid methods based on social networks," IEEE Access, vol. 6, pp. 64301–64320, 2018.

[14] L. J. Chew, S. C. Haw, and S. Subramaniam, "Recommender system for retail domain: An insight on techniques and evaluations," in Proceedings of the 12th International Conference on Computer Modeling and Simulation, June 2020, pp. 9–13.

[15] F. Demirağ, "Web personalization: Consumer perspective," in Globalized Consumer Insights in the Digital Era, IGI Global, 2024, pp. 169–185.

[16] P. Dräxler, "E-commerce platform designed for continuous optimization and personalization," 2023.

[17] N. N. Duy, V. H. Nguyen, T. Trinh, T. Ho, and H. S. Le, "A personalized product recommendation model in e-commerce based on retrieval strategy," Journal of Open Innovation: Technology, Market, and Complexity, vol. 10, no. 2, 2024, Art. no. 100303.

[18] Z. H. Hu, X. Li, C. Wei, and H. L. Zhou, "Examining collaborative filtering algorithms for clothing recommendation in e-commerce," Textile Research Journal, vol. 89, no. 14, pp. 2821–2835, 2019.

[19] A. Kumar, A. Mudgal, A. L. Yadav, and A. Sharma, "Cloudsuggest: Enhancing e-commerce with personalized recommendations," in 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Feb. 2024, vol. 5, pp. 763–766.

[20] S. C. Lee, S. W. Kim, S. Park, and D. K. Chae, "A tripartite-graph-based recommendation framework for price-comparison services," Computer Science and Information Systems.

[21] L. Liu, "E-commerce personalized recommendation based on machine learning technology," Mobile Information Systems, 2022.

[22] S. M. Phal and S. Srivastava, "An analysis of machine learning methods for ranking in recommendation systems," 2020.

[23] M. S. Ahmad, "Recent research in recommender systems," Journal of Global Research in Computer Science, vol. 9, no. 6, pp. 12–14, 2018.

[24] R. J. K. Almahmood and A. Tekerek, "Issues and solutions in deep learning-enabled recommendation systems within the e-commerce field," Applied Sciences, vol. 12, no. 21, p. 11256, 2022.

[25] A. Asad, M. M. Fouda, Z. M. Fadlullah, M. I. Ibrahem, and N. Nasser, "Moreau envelopes-based personalized asynchronous federated learning: Improving practicality in network edge intelligence," in GLOBECOM 2023 - 2023 IEEE Global Communications Conference, Dec. 2023, pp. 2033–2038.

[26] A. M. As'ad, Moreau envelopes-based personalized asynchronous federated learning: Improving practicality in distributed machine learning, Doctoral dissertation, 2023.

[27] A. Bielozorov, M. Bezbradica, and M. Helfert, "The role of user emotions for content personalization in e-commerce: Literature review," in HCI in Business, Government and Organizations: eCommerce and Consumer Behavior, Springer International Publishing, 2019, pp. 177–193.

[28] M. A. Raji, H. B. Olodo, T. T. Oke, W. A. Addy, O. C. Ofodile, and A. T. Oyewole, "E-commerce and consumer behavior: A review of AI-powered personalization and market trends," GSC Advanced Research and Reviews, vol. 18, no. 3, pp. 066–077, 2024.

[29] V. Sakalauskas and D. Kriksciuniene, "Personalized advertising in e-commerce: Using clickstream data to target high-value customers," Algorithms, vol. 17, no. 1, 2024.

[30] J. H. Blümel, Providing Personalised Experience in Text-based Customer Service Conversations, Doctoral dissertation, 2024.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 1 (2025)
https://doi.org/10.31436/ijpcc.v11i1.531

Perceptive Computing for Android Threats: Unveiling Jekyll and Hyde Syndrome in Scareware

Andi Fitriah Abdul Kadir[1], Hairul Nizam Balalo @ Bolalan[2]

[1]Department of Computer Science, International Islamic University Malaysia, 53100, Kuala Lumpur, Malaysia
[2]Commercial Crime Investigation Department (CCID), Level 27, Digital Forensic Investigation Section, Royal Malaysia Police, Menara KPJ, Jalan Tun Razak, 50400 Kuala Lumpur, Malaysia

*Corresponding author andifitriah@iium.edu.my

(Received: 30th December, 2024; Accepted: 10th January, 2024; Published on-line: 30th January, 2025)

Abstract— This paper spotlights Android scareware, relating its deceptive behavior to the dual personality syndrome of Jekyll and Hyde, as described in *The Strange Case of Dr. Jekyll and Mr. Hyde*. Modern scareware employs sophisticated evasion techniques, including metamorphic and polymorphic obfuscation, enabling it to alter its code structure during propagation. Additionally, anti-emulator techniques allow scareware to detect emulation environments and conceal malicious activities. To address these challenges, we propose a hybrid approach that combines static and dynamic analysis, leveraging features derived from unreferenced strings and network flow. This method enhances detection by uncovering scareware's dual behaviors. Using five classifiers, we construct models to address three detection scenarios: identifying malicious Android apps, categorizing apps by scareware type, and classifying apps into scareware families. Tested on a dataset of 1,350 samples, the proposed method outperforms existing approaches, achieving over 90% accuracy across all scenarios with an average false positive rate of just 0.04.

Keywords— Android, dynamic, scareware, static analysis, malware analysis, machine learning

I. Introduction

Recently, scareware has ultimately become an effective attack method for cybercriminals in getting funds; the cybercriminals make money from the malicious application (app) by threatening victims to download the apps or convincing them to pay some amount of money for the fake service. Scareware is a malicious software that poses as legitimate application and falsely claims to detect a variety of threats on the affected mobile devices (i.e., battery issues, files corrupted, account hacked). In scareware attacks, the actual target is the human where it aims to exploit human emotion, which can cause panic, shock, anxiety, or the perception of a threat in order to persuade users into purchasing the app (malware) [1]. In fact, the behavior of Android scareware is like the Jekyll and Hyde syndrome [2], exhibiting dual personalities or behaviors. According to malware reports [4, 5], Android scareware was able to bypass the detection system on the app market, i.e., Google Bouncer, for three consecutive years since 2014. Before Google removed the app from the store, Android scareware with a fake antivirus app named *Virus Shield* had been downloaded 30,000 times from Google Play at a price of $3.99 in 2014. A similar incident occurred in 2015, where another malware variant, *AntiVirus for Android*, was downloaded over a million times at $4.99.

In 2016, *Android.Spy.277.origin* was hidden in more than 100 applications on Google Play, infecting 2.8 million Android devices. Furthermore, another variant, *Street Stick Battle*, saw between one million and five million downloads. More recently, between 2020 and 2024, malware attacks have become increasingly sophisticated. For instance, in 2020, *Joker malware* managed to infiltrate hundreds of apps, compromising millions of devices worldwide. In 2022, *Facestealer* spyware emerged, stealing sensitive user data through fake social media apps, while *SharkBot* in 2023 targeted banking credentials via malicious apps disguised as legitimate financial tools. By 2024, the surge of polymorphic malware such as *Xenomorph* demonstrated advanced evasion techniques, highlighting the persistent threat to Android ecosystems [3].

In the past decade, most of the studies have focused on detecting the mobile malware. According to the survey of securing Android devices [6], the researchers have proposed various techniques such as via app-hardening systems (AppInk), through entrusted app or app-market analysis (RiskRanker, SCanDroid, FlowDroid, DroidScope, DroidRanger, Pegasus, DNADroid, DroidMOSS, Stowaway, ComDroid, ContentScope), by continuous runtime monitoring (TaintDroid, BayesDroid, MockDroid, Apex, FlaskDroid, SEAndroid, Porscha), and based on the install-time checking (Kirin, Pyandrazzi).

However, these studies have focused on the binary detection (malware or non-malware) and not specifically detecting scareware. This general detection mechanism is not enough in detecting the sophisticated malware with metamorphic and polymorphic. The fact that scareware appear as a legitimate program (i.e. contain an actual AV) makes it more difficult for the current detection system to identify it as malicious. Although many studies on Android malware [7, 9, 10, 11] are being actively developed recently, research efforts focused on Android scareware are still inadequate. This is due to the lack of understanding of mobile scareware. Without understanding the behavior of scareware, the detection systems are not capable of providing an accurate recognition of an advanced mobile scareware. A simple illustration to that is the detection rate of current AVs and malware detection tools towards scareware.

A quick scan of one of scareware samples called Fake AV with a ***Md5sum: e46a87522cdb53248c8805880d7a6108*** by VirusTotal [8] shows the poor performance of AVs in detecting scareware. VirusTotal is a web-based service that aggregates over 70 antivirus products and online scan engines for analyzing suspicious malware. However, only about 40 products (63% of detection rate) are able to detect this scareware sample. Particularly, there are five submissions available for this sample (scanned history from January 2016 until April 2018). In addition, we re-uploaded this sample to VirusTotal in December 2024. However, the results show no insignificant different; about 63% of samples are detected by AVs in 2016, 66% in 2017, and 48% in 2024. Even after three consecutive years, the detection rate of the AV products for this particular sample has not improved. The results indicate that the current AVs have some limitations in detecting scareware.

To further evaluate the performance of AV products, we scanned 150 samples of scareware that we have collected from multiple sources [12, 13, 8] with three popular AV products named AVG, Avast, Bitdefender. About 15% of the samples are not detected or in other words seen as legitimate apps by AVG and Avast; and about 12% are not detected by Bitdefender as shown in **Table I**. We labelled these samples as Undetected. The result shows a low detection rate with only 1.3%. Out of 150 scareware samples, HelDroid is only able to detect two samples as scareware. The low performance of the current detection systems has led us to perform an in-depth exploration of scareware. Our research aims to tackle this problem by focusing on the hybrid approach of malware detection, which employs both the static and dynamic analysis methods in order to increase the accuracy of detection. A hybrid approach, specifically utilizing features derived from string analysis and network flow patterns, can effectively detect behavior in scareware.

TABLE I
EXAMPLE OF SCAREWARE SAMPLES DETECTED BY AV

AV	AV Detection	Total	Detection Rate (%)
AVG	AVG#Android/G3P.GP.390306FD2DEC#20160621#16.0.0.4604	35	85
	AVG#Android/G2P.B.DAE4F9C28F18#20160816#16.0.0.4647	24	
	AVG#Android/G2M.W.895675B6B0C1#20160807#16.0.0.4627	20	
	Others	48	
	Undetected	23	
Avast	Avast#Android:Penetho-AA [PUP]#20160621#8.0.1489.320	43	85
	Avast#Android:Provar-A [Trj]#20160816#8.0.1489.320	24	
	Avast#Android:FakePlayer-D[Trj]#20160811#8.0.1489.320	22	
	Others	38	
	Undetected	23	
Bit Defender	BitDefender#Android.Hacktool.Pentr.B#20161223#7.2	44	88
	BitDefender#Android.Trojan.FakeInst.AX#20160807#7.2	39	
	BitDefender#Android.Trojan.AVPass.B#20160621#7.2	24	
	Others	25	
	Undetected	18	

II. BACKGROUND AND RELATED WORK

Analyzing an Android app can be performed in two ways: static or dynamic. Static analysis refers to any techniques that are performed without executing the apps, neither on real devices, nor in emulators or sandboxes. Thus, static analysis can be performed faster than dynamic analysis as the latter requires an appropriate execution environment (i.e. runtime while the apps are executed) in order to extract the behavior.

Static Analysis. This approach can be performed by disassembling its source code without execution where several features are collected from the application itself such as the code executables (string, bytecode, opcode, API) and manifest file properties (permission, intent filter, device and application components). This approach consists of two types:

1. Signature-based: this method is commonly used by anti-virus products where it extracts the semantic patterns and defines a unique signature of malware. Although this detection method is very efficient for known malware, it cannot detect the unknown malware types and the obfuscated and advanced malware. Most of the malware remain undetected because of the limited signature database.

2. Dalvik Bytecode: this method helps in analyzing the app's behavior. e.g., Control and data flow analysis detect the dangerous functionalities performed by malicious apps. Android apps are developed in java language, compiled in java bytecode and then translated to Dalvik byte code. In Android, Dalvik is a register-based VM that interprets the Dalvik Executable (DEX) byte code format.

Dynamic Analysis. In contrast with the static analysis, the dynamic analysis aims to find any malicious behavior of Android app while it is running on any platforms including emulator, sandbox, and smartphone. There are four methods of dynamic analysis:

1. Anomaly-based: this method relies on machine learning algorithms in detecting the malicious behaviors of Android apps. In this case, features that are extracted from known malware are used to train the model for predicting an unknown malware.
2. Taint Analysis: this method typically used for data flow analysis and leakage detection, where it automatically labels the data, keeps track of the data, and records the label of the data.
3. Emulation-based: this method executes the apps in sandbox, where it typically uses Monkey tool to analyze the malicious behavior of app.
4. On-device: this method runs apps on any devices such as computers, smartphones, and tablets.

Most studies that employ static analysis have focused on the manifest file properties (AndroidManifest.xml), which hold the application's metadata. For instance, the application permissions contained in AndroidManifest.xml have been explored by several studies, including DroidRanger [15] and Drebin [14]. In addition, static features extracted from code executables often require additional pre-processing and are commonly used in studies in the form of n-grams, including DroidMOSS [16] and DroidKin [17]. In contrast to our approach, we chose to leverage string as our static feature. This is due to the hyphothesis by Richard et al. [18], where they revealed that the unreferenced strings typically carry hidden information embedded in Android apps. This is proven by the example of GoldDream Trojan app analyzed in their work; GoldDream uploaded stolen information to a remote server with the URL of lebar.gicp.net, this URL became visible only through analysis of unreferenced strings. They evaluated their framework on more than 5,000 apps from 14 different malware families and were able to classify samples with over 99% accuracy. Like the desktop malware, the network traffic is one of the dynamic features that is useful for detecting Android malware. However, due to the lack of a large-scale malware repository and a systematic analysis of network traffic features, the existing research mostly focuses on static analysis. For that reason, we used an automated dynamic analyzer for analyzing malware through network traffic analysis. Instead of using an emulator, we run our samples on smartphones to cope with the advanced malware evasion technique. **Table II** depicts the limitation of static and dynamic analysis from the previous works. The sandboxing term was first introduced by Wahbe et al. [19] in 1993 but in a different context, .i.e., software-based fault isolation. Later, Goldberg et al. in 1996 [20] used the term sandboxing to describe the concept of confining a helper application to a restricted virtual environment for security purposes. Today, a sandbox is often used as a security mechanism for separating running programs, which is to execute suspicious or unverified programs, applications, or codes that may contain malicious code typically from third parties, users or websites, without risking the host machine or OS. There are many sandboxes that have been developed for Android applications; however, the publicly available free sandboxes only offer basic information. Furthermore, some of the authors presented their proposed sandbox but unfortunately, they did not release the sandbox for public use. This includes the Mobile Apps Assessment and Analysis System or known as MAS [21] and DroidInjector [24], a process injection-based dynamic tracking system for runtime behaviors of Android applications.

Research Gap Summary. The primary research gap identified in earlier studies is the lack of a focused approach to detecting scareware specifically, as most existing methods target binary malware detection and fail to account for advanced evasion techniques like metamorphism and polymorphism. Recent advancements in hybrid malware detection emphasize the integration of static and dynamic analysis to enhance accuracy and resilience against obfuscation techniques. However, these methods largely remain limited to broader malware categories without delving into scareware's unique behavioral traits. The proposed study addresses this gap by combining unreferenced string analysis (static) with network flow patterns (dynamic) to effectively detect the dual personality of scareware, similar to the Jekyll and Hyde syndrome. This integration ensures robust detection of both overt and covert malicious behaviors, advancing beyond the capabilities of existing frameworks. By leveraging features that expose scareware-specific characteristics, the study provides a targeted solution previously overlooked in hybrid detection research. Moreover, the adoption of anti-emulation techniques ensures its applicability against modern malware variants designed to evade conventional detection environments.

TABLE II
LIMITATION OF STATIC AND DYNAMIC ANALYSIS

Type	Method	Limitation	Related Work
Static	Signature-based	Cannot detect unknown malware types	[26, 27, 28, 29, 30, 31, 32]
	Dalvik bytecode	More power and memory consumption	[15, 16, 19, 33, 34]
Dynamic	Anomaly-based	Unreliable if a benign app shows same behaviors and can consume more battery and memory	[22, 35, 37, 38]
	Taint analysis	Not suitable for a real-time analysis as its slowdown system	[23, 39, 40, 41]
	Emulation-based	More resource consumption	[25, 42, 43, 44, 45]
	On-device	More power and memory consumption	[35, 36, 46, 47, 48]

III. METHOD AND IMPLEMENTATION

With the rapid growth of malware samples, there exist many solutions that can be used by malware analysts for correlating the different signs of the malicious behavior. However, the output of thesesolutions is focusing more on the malware binary detection (or family) and not directly applicable for the malware type categorization. Therefore, we extend the framework outlined in [49], originally employed for detecting Android financial malware, to identify scareware. This framework facilitates malware detection, encompassing a three-tier detection approach: identifying malicious Android applications, classifying Android apps based on scareware categories, and characterizing Android apps according to scareware families. For the development of the study, a detailed illustration of our proposed conceptual framework is outlined in **Figure 1**. It depicts the major facets of this study, as follows:

1. Collector: responsible for collecting the input data of Android scareware from various sources.
2. Filter: acts as a screening filter to check the similarity of the collected data and to correlate the data with the external sources and the proposed taxonomy.
3. Analytics engine: a hybrid of static and dynamic modules, which involves a process of correlating data from malware string and network flow.
4. Detector: consists of three levels of detection; Level 1: malware binary detection; Level 2: malware category classification; Level 3: malware families characterization, which is to label scareware families.

Dataset. The dataset comprises 1,350 Android apps, including 1,200 benign apps sourced from the Google Play Store based on popularity and 150 scareware samples obtained from VirusTotal [8], security blog [13], and other academic datasets [12, 17, 16] as listed in **Table III**. Initially, over 3,000 APK files were collected from these diverse sources to ensure coverage of various scareware types, temporal variations, geographical distributions, and behavioral patterns. However, several limitations reduced the final dataset size: 1) **Sample errors**: many collected samples were of poor quality, including issues like Dex errors, unsigned apps, or corrupted files. Unsigned apps could not be installed on emulators or real devices, significantly limiting their usability; 2) **Inconsistent malware labeling**: variations in malware naming conventions across academic and industry sources caused confusion and required time-intensive reorganization. Malware labels were aligned by comparing naming conventions from several antivirus vendors and adopting the majority consensus for each family. Benign apps were selected from the Google Play Store based on popularity, while suspicious apps flagged by more than two antivirus engines on VirusTotal were excluded from the benign set. This labeling approach ensured a reliable benchmark for analysis. The dataset's diversity enhances its generalizability, allowing the detection model to adapt to both older and emerging scareware variants, perform consistently across regions, and recognize a wide range of malicious behaviors. This variety minimizes the risk of overfitting and ensures robust performance against novel or underrepresented threats in real-world scenarios.

TABLE III
THE BREAKDOWN OF ANDROID SCAREWARE BY FAMILY

Year	Malware Family	Number of samples collected	Number of samples analyzed
2011	FakePlayer	150	0
2012	Penetho	150	20
2013	AV Pass	150	20
2013	FakeAV	150	22
2013	FakeFlash	150	6
2013	FakeJobeOffer	9	9
2013	Android Defender	150	17
2013	FakeTaoBao	150	0
2013	Tapsnake	150	9
2014	Virus Shield	150	10
2015	AV for Android	83	10
2015	FakeApp	150	10
2015	FakeApp. AL	150	11
2016	Android Spy.277	9	6
Total		**1751**	**150**

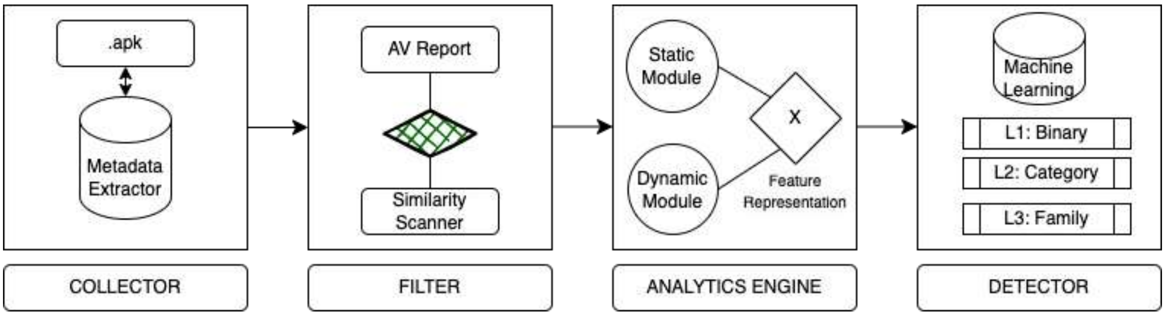


Fig. 1 Overview of the proposed Android scareware detection system

System Configuration. In this section, we discuss the various tools and techniques used for the implementation of the proposed framework. We implemented our framework by using UNIX Shell scripting, Python, and Java programming language. The static analysis implementation of the String Analyzer employs Apktool to decode APKs and Natural Language Toolkit (NLTK) to extract string literal features. In this analysis, we used various Python modules available in the scikit-learn library. Scikit-learn is a Python-based, open source library for handling various data mining and analysis tasks [50]. It provides implementations of a wide range of machine learning algorithms and functionality to generate feature vectors from string n-grams extracted from every APK under the analysis. On the other hand, we used the Shell scripting and Java programming language in the dynamic analysis implementation. The network analyzer app's installation used Shell scripting to run the samples automatically. Machine learning tasks including preprocessing, feature selection, training and testing phases are carried out through Scikit-learn libraries and Weka data mining tool.

Learning Parameters. We employed five common machine learning classifiers including k-Nearest Neighbors (kNN), Support Vector Machine (SVM), Logistic Regression (LR), Naive Bayes (NB), and Random Forest (RF). These algorithms should be calibrated with parameters that ensure maximum performance, which in our case means the maximum classification accuracy and the minimum number of false positives. To avoid over-tuning, we only use 20% of the dataset for parameter tuning. We perform different rounds of experiments to decide on the optimal value for each parameter. Below is the list of parameters that need to be optimized for each classifier.

a) RF: number of trees (set to 100 trees) and minimum number of instances per leaf (set to 1 leaf)
b) NB: type of estimator (use kernel density estimator)
c) kNN: number of neighbors, k (set k to 2 neighbors)
d) SVM: kernel function (use Radial basis function)

Evaluation Metrics. In this section, we explain how the system performance is evaluated. We also discuss various measures used for evaluating the system such as accuracy, F1 measure, Receiver Operating Characteristic (ROC) curve, and false positive rate. The goal of the classification model is to correctly classify an input sample to one of the output classes from a set of discrete output categories. Our Android malware detection framework trains a classifier over training samples. The classifier then predicts the category of APKs in the test data. The best way to represent such output predictions of the classification model is to use a confusion matrix. A confusion matrix is an N × N contingency table, where N is the number of output labels. It shows the number of samples correctly and incorrectly classified by the model as compared to the actual target output values. For example, consider a binary classification model with output labels as either Positive or Negative.

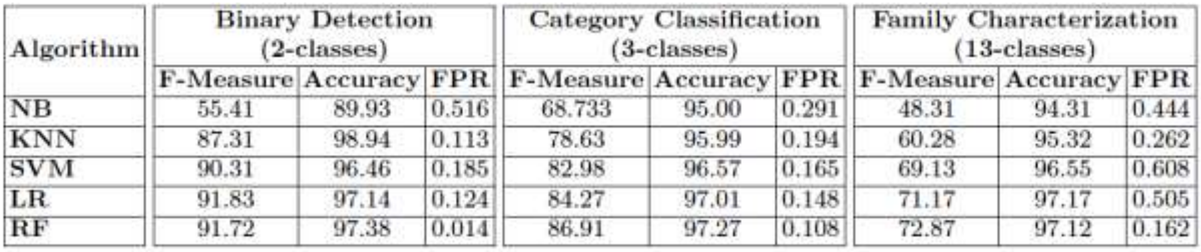
IV. Experiment and Result

In this section, we present the results obtained in detecting scareware statically and dynamically, as described in Section 4. In our experimental study, we focused on analysis of binary classification, category classification, and family classification. In order to evaluate the detection performance of the proposed systems, we split the data into 60% of train-set and 40% of test-set. We reported three metrics in each scenario:

a) **Accuracy**: refers to the overall classification accuracy measure, which is given by the percentage of correctly classified instances.
b) **F-measure:** considers class imbalance, which represents a weighted average of recall and precision.
c) **FPR** (false positive rate): defines the ratio between the number of negative events incorrectly

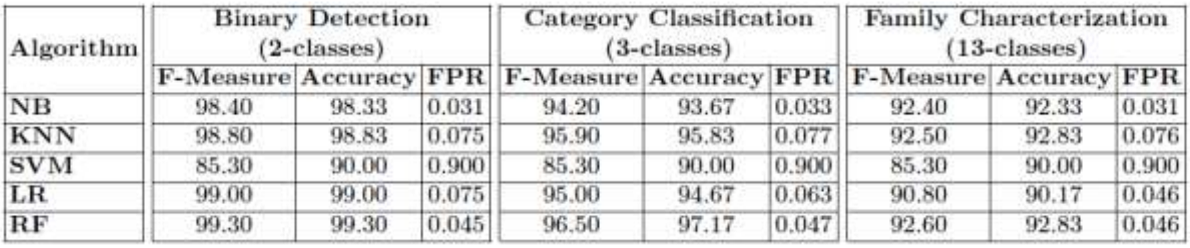
categorized as positive (false positives) and the total number of actual negative events.

TABLE IV
SCAREWARE DETECTION RESULTS WITH 3-GRAM WORD OF STRING



Algorithm	Binary Detection (2-classes)			Category Classification (3-classes)			Family Characterization (13-classes)		
	F-Measure	Accuracy	FPR	F-Measure	Accuracy	FPR	F-Measure	Accuracy	FPR
NB	55.41	89.93	0.516	68.733	95.00	0.291	48.31	94.31	0.444
KNN	87.31	98.94	0.113	78.63	95.99	0.194	60.28	95.32	0.262
SVM	90.31	96.46	0.185	82.98	96.57	0.165	69.13	96.55	0.608
LR	91.83	97.14	0.124	84.27	97.01	0.148	71.17	97.17	0.505
RF	91.72	97.38	0.014	86.91	97.27	0.108	72.87	97.12	0.162

TABLE V
SCAREWARE DETECTION RESULT WITH NETWORK FLOW



Algorithm	Binary Detection (2-classes)			Category Classification (3-classes)			Family Characterization (13-classes)		
	F-Measure	Accuracy	FPR	F-Measure	Accuracy	FPR	F-Measure	Accuracy	FPR
NB	98.40	98.33	0.031	94.20	93.67	0.033	92.40	92.33	0.031
KNN	98.80	98.83	0.075	95.90	95.83	0.077	92.50	92.83	0.076
SVM	85.30	90.00	0.900	85.30	90.00	0.900	85.30	90.00	0.900
LR	99.00	99.00	0.075	95.00	94.67	0.063	90.80	90.17	0.046
RF	99.30	99.30	0.045	96.50	97.17	0.047	92.60	92.83	0.046

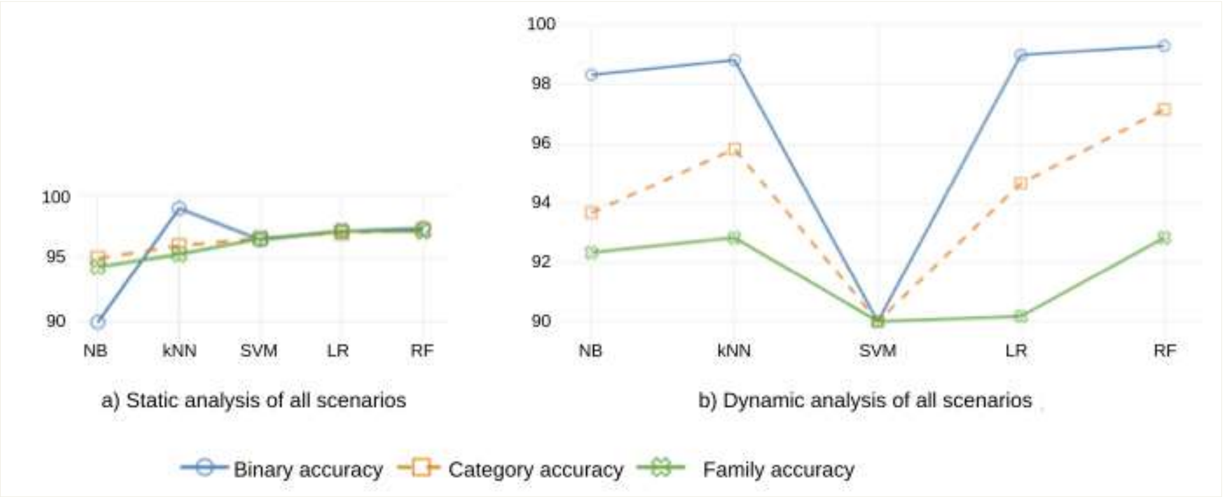


Fig. 2 Accuracy comparison of static and dynamic analysis for all scenario

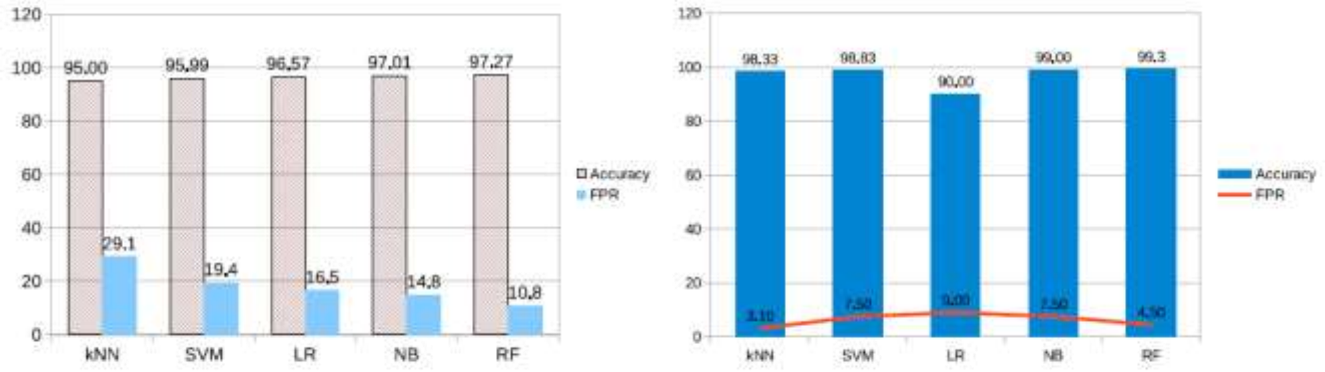


Fig. 3 3-gram scareware detection (left) and netflow scareware detection (right)

For static analysis, we tested up to 3-gram of word token with all classifers. On average, 3-gram yields the highest precision. Thus, in this paper, we reported the result of the 3-gram for all three scenarios (**Table IV**). KNN surpasses RF in the binary detection, but RF performs the best in all scenarios: 97.38% accuracy with binary detection, 97.27% accuracy with category detection, and 97.12% accuracy with family detection with an average of 0.095 FPR.

Similar to the static analysis, RF also performs the best in all scenarios for dynamic analysis: 99.30% accuracy with binary detection, 97.17% accuracy with category detection, and 92.83% accuracy with family detection with an average of 0.046 FPR (**Table V**). Since both static and dynamic results (**Figure 2**) yield a high accuracy and low FPR, there is no need for us to have the integrated feature vectors between the 3-gram unreferenced strings and the 80 nominal network ow features for the purpose of increasing the accuracy. Our results demonstrates that the raw features of each analysis is adequate in detecting scareware, classifying the category, and characterizing its family accurately with very low percentage of FPR. **Figure 3** presents the result of scareware for both static and dynamic where RF also outperformed other classifiers with more than 97% and 99.30% accuracy respectively.

RF outperformed other classifiers due to its ability to handle high-dimensional feature spaces and its robustness against overfitting, especially when analyzing diverse datasets. By leveraging ensemble learning, RF builds multiple decision trees and aggregates their predictions, which enhances accuracy and reduces bias. Compared to simpler classifiers like NB, RF's capacity to capture non-linear relationships between features contributed to its superior performance in detecting the nuanced behaviors of scareware.

The strange case of Android.Spy.277. In order to evaluate our framework, we conducted a case study of one of the sophisticated malware family in our dataset (AndroidSpy). Similar to Jekyll's behavior, AndroidSpy first appeared as legitimate apps that offered services like games, wallpapers, photo editing apps. But, once installed, the app transforms into Hyde and becomes malicious through a backdoor. These apps had been downloaded by almost 3 million users [5]. The attacker can remotely download a malicious APK called ***polacin.io*** to the victim's device. Once infected, the Android device sends a wide array of information about the phone to command and control servers (C&C), including phone IMEI number, email address, sms messages, and location. What's more, AndroidSpy performs and additional malicious act through unwanted advertisements via popups and notification's bar. Victims are induced into installing fraudulent apps via fake warning of battery issues that can be solved by downloading fake utilities. By clicking on these fake alerts, for example, brings victims to the landing pages for Android optimization applications such as Turbo Cleaner, SuperB Cleaner (Boost Clean). This behavior reveals that AndroidSpy have several layered of attacks to sustain their malicious behavior. To further analyzed the stealthiness of this AndroidSpy, we analyzed all 6 samples that we have by using three malware scanners: AndroTotal[1], Joe Sandbox[2], and VirusTotal[3]. The results depict that most of the AV are not able to detect this type of scareware. Out of 100 AV deployed on these scanners, only 25 of them are able to detect AndroidSpy as maliciouss apps (**Table VI**). With our approach, we managed to detect AndroidSpy accurately (detected 5 apps out of 6) with 99.42% of ROC area value (the area under the ROC curve is a measure of how well a

[1] https://andrototal.org/
[2] https://www.joesandbox.com/
[3] https://www.virustotal.com

parameter can distinguish between two groups malicious and benign. The true positive rate surpasses 80% when the false positive rate is greater than 60%. Therefore the closer the ROC curve is to the upper left corner (true positive rate), the higher the overall accuracy of the test.

TABLE VI
COMPARISON RESULTS OF ANDROIDSPY ANALYSIS

SCANNER	AV DETECTED	TOTAL AV
VIRUSTOTAL	20	61
ANDROTOTAL	3	8
JOE SANDBOX	2	31

V. LIMITATION AND DISCUSSION

The study of Android scareware is stimulating. As this is the first study of its type to systematically detecting scareware, researchers not only have a new opportunity for research but also several challenges:

a) **Dataset biases**: the study concluded that integrating static (unreferenced strings) and dynamic (network flow) feature vectors was unnecessary, as both feature sets independently achieved high accuracy and low false positive rates. This simplification reduces computational overhead, making the system more suitable for real-world deployment on resource-constrained devices. However, potential dataset biases such as the reliance on scareware samples predominantly flagged by certain antivirus engines could influence metrics, potentially skewing detection results toward these engines' strengths.

b) **Scareware labeling**: the naming convention for malware labeling is inconsistent across both academic and industry fields, leading to confusion and inefficiencies during reorganization. The inconsistent labeling practices among different antivirus vendors and researchers further complicate the process. For instance, services like VirusTotal aggregate results from multiple antivirus engines, and discrepancies in detection can create ambiguity. Some engines may flag an APK as scareware, while others classify it as benign, requiring manual interpretation to resolve conflicts. To address this, we compare malware labeling from several antivirus vendors and follow the majority consensus based on the most frequent label for a specific malware family. However, this technique is entirely manual, introducing the risk of human error due to subjective judgment, inconsistencies in labeling criteria, or varying levels of expertise. These errors can impact the accuracy of malware labeling, potentially affecting the dataset's reliability and the model's performance.

c) **Scalability**: the proposed system demonstrates promising scalability for large-scale applications due to its reliance on lightweight static and dynamic analysis, avoiding the complexity of integrated feature processing. Its modular design allows seamless scaling across distributed detection infrastructures, where static analysis can filter benign apps rapidly, while dynamic analysis is reserved for suspected cases. However, the real-world deployment would require robust automation for sample collection and labeling to handle the vast influx of applications. Additionally, optimizing computational resources and incorporating cloud-based processing could enhance throughput and maintain low latency, ensuring effective operation in environments like app stores and enterprise security systems.

VI. CONCLUSION AND FUTURE WORK

The syndrome of Jekyll and Hyde is increasingly adopted by Android malware especially scareware. In this research, we presented a novel combination of both static and dynamic analysis based specifically on features derived from the unreferenced string and network flow. The key idea is to be able to detect the Jekyll behavior at early stage through static analysis before transforming into Hyde behavior, which can later be detected through dynamic analysis. We demonstrated that this combination could identify three scenarios: detecting malicious Android apps, classifying Android apps with respect to scareware category, and characterizing Android apps according to scareware family. The experimental results show that the proposed method achieves high accuracy of over 90% for all three scenarios with a very low false positive rate of 0.04 on average.

The proposed framework effectively detects scareware using a hybrid approach that combines static and dynamic analysis, but there are multiple areas for further enhancement and exploration. First, while the dataset used in this study is diverse, consisting of 1,350 apps, it is relatively small compared to the vast number of Android applications available globally. Future work should prioritize expanding the dataset by incorporating more samples, including new and evolving malware families like ransomware, adware, spyware, and phishing apps. This would not only improve the robustness of the detection model but also allow it to adapt to emerging threats. Moreover, creating a publicly available and standardized scareware dataset could contribute significantly to research in this domain and enable consistent benchmarking across studies.

Another critical area is automating the labeling process to address inconsistencies in malware family naming conventions across different antivirus engines and research datasets. Advanced machine learning algorithms, consensus-driven approaches, or natural language processing techniques could be employed to harmonize malware labels more efficiently and reduce manual intervention. Additionally, future research could explore dynamic labeling systems that update in real-time as malware evolves, ensuring that datasets remain relevant and up-to-date.

In terms of scalability, the framework's computational efficiency must be optimized for real-world deployment. While the current approach effectively utilizes both static and dynamic features, further refinement could focus on reducing processing time and resource requirements. Implementing lightweight versions of the framework tailored for use on mobile devices or integrating cloud-based or distributed systems would make the solution more accessible for large-scale applications. For example, app stores or corporate security networks could use such a system to analyze vast numbers of apps without significant delays. The potential integration of federated learning could also be explored, allowing the framework to continuously improve and update its detection models using decentralized data while maintaining user privacy and reducing bandwidth constraints.

Additionally, future studies should investigate other advanced evasion techniques employed by scareware and malware in general, such as anti-debugging, anti-sandboxing, and advanced anti-emulation behaviors. Understanding and addressing these techniques would enhance the framework's ability to detect increasingly sophisticated threats. It would also be valuable to explore the integration of additional data sources, such as user reviews, app metadata, and permissions, to complement the current static and dynamic features and improve the overall detection accuracy.

Finally, extending the framework to address other types of malware beyond scareware could demonstrate its broader applicability. Experiments on categories like financial malware, ransomware, and spyware could provide insights into the model's generalizability and practical effectiveness across diverse threat landscapes. Real-world testing in various environments, such as corporate IT systems, app marketplaces, and government agencies, would further validate its utility and identify potential areas for improvement. Addressing these challenges will ensure the framework remains relevant and adaptable in the rapidly evolving field of cybersecurity, paving the way for a comprehensive solution to combat mobile threats on a global scale.

Acknowledgment

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

Conflict of Interest

The authors declare that there is no conflict of interest

References

[1] J. Giles, "Scareware: the inside story," *New Scientist*, vol. 205, no. 2753, pp. 38–41, 2010.

[2] R. L. Stevenson, "Strange case of dr jekyll and mr hyde," in *Medicine and Literature, Volume Two*, CRC Press, 2018, pp. 105–118.

[3] Kaspersky, "Polymorphic Malware on Android: The Rise of Xenomorph," 2024. [Online]. Available: https://www.kaspersky.com.

[4] "Ad fraud, scareware slinger android.spy. 277.origin found in more than 100 apps," 2016. [Online]. Available: https://www.theregister.co.uk/2016/04/26.

[5] "Scareware app downloaded over a million times from google play," 2015. [Online]. Available: http://researchcenter.paloaltonetworks.com/2015/01/scareware-appdownloaded-million-times-google-play/.

[6] D. J. Tan, T. W. Chua, and V. L. Thing, "Securing android: a survey, taxonomy, and challenges," *ACM Computing Surveys (CSUR)*, vol. 47, no. 4, p. 58, 2015.

[7] A. I. Ali-Gombe, B. Saltaformaggio, D. Xu, and G. G. Richard III, "Toward a more dependable hybrid analysis of android malware using aspect-oriented programming," *Computers & Security*, vol. 73, pp. 235–248, 2018.

[8] Virus Total. [Online]. Available: https://www.virustotal.com/en/.

[9] C. Lyvas, C. Lambrinoudakis, and D. Geneiatakis, "Dypermin: Dynamic permission mining framework for android platform," *Computers & Security*, vol. 77, pp. 472–487, 2018.

[10] Y. Zhuang, "The performance cost of software obfuscation for android applications," *Computers & Security*, vol. 73, pp. 57–72, 2018.

[11] H. Meng, V. L. Thing, Y. Cheng, Z. Dai, and L. Zhang, "A survey of android exploits in the wild," *Computers & Security*, vol. 76, pp. 71–91, 2018.

[12] A. H. Lashkari, A. F. Kadir, L. Taheri, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark android malware datasets and classification," in *Proceedings of the 52nd IEEE International Carnahan Conference on Security Technology (ICCST)*, 2018.

[13] Virus Total, "Contagio mobile malware mini dump," 2016. [Online]. Available: http://contagiominidump.blogspot.ca/.

[14] D. Arp et al., "Drebin: Effective and explainable detection of android malware in your pocket," in *NDSS*, vol. 14, pp. 23–26, 2014.

[15] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, "Hey, you, get off of my market: detecting malicious apps in official and alternative android markets," in *NDSS*, vol. 25, pp. 50–52, 2012.

[16] W. Zhou et al., "Detecting repackaged smartphone applications in third-party android marketplaces," in *Proceedings of the Second ACM Conference on Data and Application Security and Privacy*, pp. 317–326, 2012.

[17] H. Gonzalez, N. Stakhanova, and A. A. Ghorbani, "Droidkin: Lightweight detection of android apps similarity," in *International Conference on Security and Privacy in Communication Systems*, pp. 436–453, Springer, 2014.

[18] R. Killam and N. Stakhanova, "Android malware classification through analysis of string literals," in *Analytics for Cybersecurity and Online Safety*, 2016.

[19] R. Wahbe, S. Lucco, T. E. Anderson, and S. L. Graham, "Efficient software-based fault isolation," in *ACM SIGOPS Operating Systems Review*, vol. 27, pp. 203–216, 1994.

[20] I. Goldberg et al., "A secure environment for untrusted helper applications: Confining the wily hacker," in *Proceedings of the 6th Conference on USENIX Security Symposium, Focusing on Applications of Cryptography*, vol. 6, p. 11, 1996.

[21] C. W. Tien, T. Y. Huang, T. C. Huang, W. H. Chung, and S. Y. Kuo, "MAS: Mobile-apps assessment and analysis system," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 145–148, 2017.

[22] G. Dini, F. Martinelli, A. Saracino, and D. Sgandurra, "MADAM: A multi-level anomaly detector for Android malware," in *MMM-ACNS 2012*, vol. 12, pp. 240–253, Springer, 2012.

[23] W. Enck *et al.*, "TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Transactions on Computer Systems*, vol. 32, no. 2, p. 5, 2014.

[24] W. Fan, Y. Sang, D. Zhang, R. Sun, and Y. Liu, "DroidInjector: A process injection-based dynamic tracking system for runtime behaviors of Android applications," *Computers & Security*, vol. 70, pp. 224–237, 2017.

[25] "Android malware toolkit for malware analysis." [Online]. Available: http://dunkelheit.com.br/amat/analysis/index_en.php

[26] P. Faruki, V. Ganmoor, V. Laxmi, M. S. Gaur, and A. Bharmal, "AndroSimilar: Robust statistical feature signature for Android malware detection," in *Proceedings of the 6th International Conference on Security of Information and Networks*, pp. 152–159, 2013.

[27] Y. Feng, S. Anand, I. Dillig, and A. Aiken, "Apposcopy: Semantics-based detection of Android malware through static analysis," in *Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering*, pp. 576–587, 2014.

[28] M. Zheng, M. Sun, and J. C. S. Lui, "Droid analytics: A signature based analytic system to collect, extract, analyze and associate Android malware," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 163–171, 2013.

[29] R. Sato, D. Chiba, and S. Goto, "Detecting Android malware by analyzing manifest files," *Proceedings of the Asia-Pacific Advanced Network*, vol. 36, pp. 17–23, 2013.

[30] C. Y. Huang, Y. T. Tsai, and C. H. Hsu, "Performance evaluation on permission-based detection for Android malware," in *Advances in Intelligent Systems and Applications—Volume 2*, Springer, 2013, pp. 111–120.

[31] B. Sanz *et al.*, "PUMA: Permission usage to detect malware in Android," in *International Joint Conference CISIS'12-ICEUTE'12-SOCO'12 Special Sessions*, Springer, 2013, pp. 289–298.

[32] W. Shin, S. Kiyomoto, K. Fukushima, and T. Tanaka, "Towards formal analysis of the permission-based security model for Android," in *2009 Fifth International Conference on Wireless and Mobile Communications*, pp. 87–92, 2009.

[33] J. Kim, Y. Yoon, K. Yi, and J. Shin, "SCANDAL: Static analyzer for detecting privacy leaks in Android applications," in *Proceedings of the Mobile Security Technologies (MoST)*, 2012.

[34] E. R. Wognsen, H. S. Karlsen, M. C. Olesen, and R. R. Hansen, "Formalisation and analysis of Dalvik bytecode," *Science of Computer Programming*, vol. 92, pp. 25–55, 2014.

[35] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, "Crowdroid: Behavior-based malware detection system for Android," in *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pp. 15–26, 2011.

[36] P. Irolla and E. Filiol, "Glassbox: Dynamic analysis platform for malware Android applications on real devices," *arXiv preprint arXiv:1609.04718*, 2016.

[37] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "Andromaly: A behavioral malware detection framework for Android devices," *Journal of Intelligent Information Systems*, vol. 38, no. 1, pp. 161–190, 2012.

[38] M. Zhao, F. Ge, T. Zhang, and Z. Yuan, "AntiMalDroid: An efficient SVM-based malware detection framework for Android," in *International Conference on Information Computing and Applications*, Springer, 2011, pp. 158–166.

[39] W. Klieber, L. Flynn, A. Bhosale, L. Jia, and L. Bauer, "Android taint flow analysis for app sets," in *Proceedings of the 3rd ACM SIGPLAN International Workshop on the State of the Art in Java Program Analysis*, pp. 1–6, 2014.

[40] G. Sarwar, O. Mehani, R. Boreli, and M. A. Kaafar, "On the effectiveness of dynamic taint analysis for protecting against private information leaks on Android-based devices," in *SECRYPT 2013*, 2013.

[41] N. Andronio, S. Zanero, and F. Maggi, "Heldroid: Dissecting and detecting mobile ransomware," in *International Workshop on Recent Advances in Intrusion Detection*, Springer, 2015, pp. 382–404.

[42] L. K. Yan and H. Yin, "DroidScope: Seamlessly reconstructing the OS and Dalvik semantic views for dynamic Android malware analysis," in *Proceedings of the 21st USENIX Security Symposium*, pp. 569–584, 2012.

[43] T. Bläsing, L. Batyuk, A. D. Schmidt, S. A. Camtepe, and S. Albayrak, "An Android application sandbox system for suspicious software detection," in *2010 5th International Conference on Malicious and Unwanted Software*, pp. 55–62, 2010.

[44] A. Saracino, D. Sgandurra, G. Dini, and F. Martinelli, "MADAM: Effective and efficient behavior-based Android malware detection and prevention," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 3, pp. 424–436, 2018.

[45] K. Tam, S. J. Khan, A. Fattori, and L. Cavallaro, "CopperDroid: Automatic reconstruction of Android malware behaviors," in *NDSS*, 2015.

[46] S. Mutti *et al.*, "BareDroid: Large-scale analysis of Android apps on real devices," in *Proceedings of the 31st Annual Computer Security Applications Conference*, pp. 71–80, 2015.

[47] M. K. Alzaylaee, S. Y. Yerima, and S. Sezer, "Emulator vs real phone: Android malware detection using machine learning," in *Proceedings of the 3rd ACM on International Workshop on Security and Privacy Analytics*, pp. 65–72, 2017.

[48] Y. Zhou and X. Jiang, "Dissecting Android malware: Characterization and evolution," in *2012 IEEE Symposium on Security and Privacy*, pp. 95–109, 2012.

[49] A. F. Abdul Kadir, *A Detection Framework for Android Financial Malware*. M.S. thesis, University of New Brunswick, 2018.

[50] F. Pedregosa *et al.*, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011

https://doi.org/10.31436/ijpcc.v11i1.548

Design and Development of a Cost Effective WebVR Commerce System Prototype

[1]Nurazlin Zainal Azmi*, [2]Thomas Liem Shiaw Hong

[1]Dept. of Information Systems, International Islamic University Malaysia, Kuala Lumpur, Malaysia.
[2]Faculty of Engineering and Computing, First City University College, Petaling Jaya, Malaysia.

*Corresponding author: nurazlinazmi@iium.edu.my

(Received: 8th January, 2025; Accepted: 12th January, 2024; Published on-line: 30th January, 2025)

Abstract— This project focuses on the design and development of a cost-effective WebVR commerce system prototype to enhance the online shopping experience. Despite the rapid growth of E-commerce, platforms face challenges such as limited interactivity, static product presentations, and lengthy purchasing procedures, which often lead customers to abandon online shopping in favor of physical stores. The proposed WebVR system leverages virtual reality to address these issues, providing an immersive and interactive shopping experience. By enabling users to visualize and explore products in a 3D virtual environment, the system bridges the gap between online and in-store shopping. However, virtual reality often requires costly hardware and powerful workstations to process the positioning data. Therefore, this project focuses on utilizing affordable technologies and frameworks to create a seamless and accessible solution, making WebVR a more practical option for a wider audience.

Keywords— Cost effective WebVR, virtual reality, e-commerce.

I. Introduction

Since the development of the first system in 1979 by Michael Aldrich [1], the online shopping platform has grown exponentially from simple texts and images multipage website to utterly complicated networks of online applications, featuring mobile-friendly purchasing, social shopping and much more. Innovation in today's technology has constantly evolved the E-commerce landscape and has worked as a catalyst to move it forward. E-commerce practitioners from all industries need to be ready to step up and embrace innovation as a mean of staying ahead of the game.

Virtual reality (VR) has already existed in the market for decades. It represents a transformative shift in how we interact with digital environments, crossing the boundaries between the physical and virtual worlds, and at the same time offering immersive experiences to the user [2]. Most of the VR equipment in the market are extremely expensive and require specific sets of software installed to bridge the two worlds. For the WebVR to become a norm in everyday use, it is essential to develop a cost-effective system.

A. *Problem Statement*

E-commerce provides an easy way to sell products to a large customer base. Customers expect to find what they are looking for quickly and easily. While shopping online, customers must imagine and interpret what an item would feel like in their hands or look like in their home. These sensory elements that customers rely on to make their purchasing decisions are often lost during online shopping, which can lead to unsatisfactory purchases.

B. *Objective*

The main purpose of this project is to develop a cost-effective virtual reality system that allows everyone to explore new ways of accessing daily information and resources through environment simulations using three-dimensional graphics.

This paper is based on a final year project completed in 2017. While the technologies and methods used reflect the standards of that time, the prototype serves as a foundational basis for ongoing work in this area. Recent advancements and current practices have been reviewed and incorporated into the discussion to ensure relevance moving forward.

The general structure of this paper is as follows: The first section provides an introduction. Related works are presented in Section 2. Prototype requirements are listed in Section 3. The development process and methodology, the preliminary results, and the discussions are represented in sections 4 and 5, respectively. Finally, the study's conclusion is presented in Section 6.

II. Related Work

Back in 2010, VR was already considered an alternative to conventional methods, improving product presentation and offering greater flexibility to customers [3]. In recent years, more research has been dedicated to studying extended reality within the e-commerce context.

[4] focused their study on levelling the field between large companies, and small businesses and retailers, by giving them a chance to compete equally using VR and AI-driven e-commerce platform. They proposed to develop a VR-powered shopping platform with a recommendation system (RS) and an intelligent agent that allows small businesses to offer their products in a virtual environment.

The immersive feature of VR makes it appealing for integration into the e-commerce field, enhancing the shopping experience, as discussed in the following works. [5] proposed an integration of Augmented Reality (AR) and VR to enhance customer engagement. AR is used for visualizing shortlisted items as well as in-store navigation, whereas VR is utilized for heightening the shopping experience while interacting with objects in a shared simulated environment with family and acquaintances. A similar work is also reported by [6], where the results yielded positive outcomes, including enhanced product visualization, improved customer engagement, reduced product returns, and increased cross-selling and upselling. However, there was also a concern addressed by customers regarding the privacy and security when using AR/VR technology in e-commerce. [7] shared the same outcome, where their proposed model for an AR/VR e-commerce to enhance user experience has seen significant improvements in user engagement, personalization, and product information flexibility.

[8] extended the application into the Metaverse by proposing a virtual commerce that incorporates AR, VR, 3D holographic avatars, and other type of communication. Based on the preliminary testing, it showed that users found it attractive to explore new places in the Metaverse, and the use of 3D avatar influenced them to buy from the stores that use this technology.

Covid-19 was also a reason to incorporate VR into the e-commerce world. Since many consumers were forced to shop online, this led [7] to propose a UX design model for virtual shopping which focuses on psychological stimulation and social shopping, the two aspects that make shopping an entertaining activity.

To make the experience more interesting, [10] proposed a VR-based game called Virtual Bazaar, to support healthier food choices. The game keeps a check on the Calorie requirements set by the user, displays Nutritional Information of products and create awareness for Healthier Products. From the results, it was found that players benefitted from the game by learning how to choose healthier products.

AI has also made its way into the virtual commerce as demonstrated by [11]. Their proposed VR Supermarket included a recommendation system based on the users' purchase history, which in turn makes it a dynamic, adaptive and user-oriented system, improving the overall user experience.

Based on the findings, it is reasonable to predict that VR/AR will become the new normal in the e-commerce industry. This underscores the importance of developing cost-effective systems to ensure that most people can participate in and benefit from this transformative experience.

III. Prototype Requirements

The hardware is a critical component required to ensure the success of this project. Premium VR experiences require head-mounted displays (HMDs) such as the Oculus Rift, HTC Vive, or newer models like the Vive Pro and Meta Quest 3. that are costly on its own and not to mention the cost of a powerful workstation needed to process the positioning data. This approach does not align with our objective of making VR accessible to everyone, including novice users.

The solution needs to be cost-effective while allowing expandability for device upgrades. Smartphones, which most people already own, can serve as displays, paired with affordable viewers like Google Cardboard to create a simple virtual reality setup.

The lenses in the viewers create the 3D effect required, and the gyroscope inside common smartphones translates users' positions into the VR environment. The smartphone itself also provides the processing power for positioning data, and this setup fulfills all the hardware requirements.

IV. Development Process and Methodology

A. Framework Implementation

A-Frame, a fully open-source project, is one of the WebVR frameworks that enable VR in web browsers. It provides the convenience of building scenes with just HTML while offering unlimited access to JavaScript, Three.js, and all existing Web APIs. It uses an entity-component-system pattern that promotes composition and extensibility [12]. In modern usage, A-Frame integrates seamlessly with the WebXR ecosystem.

A-Frame, developed by the Mozilla VR team in 2015, enables web developers and designers to create 3D and VR experiences using HTML, without requiring knowledge of WebGL. It offers an easy setup, compatibility with JavaScript libraries, and an extensible entity-component system for reusable components. Unlike Three.js, which requires extensive knowledge of WebGL, or Babylon.js, which focuses on advanced graphics and physics engines, A-Frame stands out for its simplicity, rapid development capabilities, compatibility with existing JavaScript libraries, flexibility, and ease of use. These attributes make it an ideal choice for this project, particularly in the context of a time-constrained and resource-limited final year project.

B. VR Viewer Implementation

After selecting the framework, the next step is to display the VR content. To ensure accessibility for everyone, including novice users, using an open-source VR viewer is the most suitable option.

Google Cardboard is one of the best open-source VR viewers, developed as part of Google's 20 percent project – a company policy that allows employees to work on side projects in addition to their regular tasks.

Google Cardboard works by placing a smartphone at an optimal distance from the lenses. Using compatible apps, the lenses create a 3D effect when held up to the users' eyes. As users move their heads, the display output synchronizes with their movements, creating the illusion of moving within a virtual space. This simple setup transforms interactions with a smartphone screen into a seemingly real-world experience.

Fig. 1 Google Cardboard DIY Template (Credits: [13])

Google provides an open-source template online for those interested in building their own viewer, as shown in Fig. 1.

C. Scene Design

Designing the scene is the first step in creating a 3D simulated environment using A-Frame. With basic knowledge of HTML and JavaScript, users can construct ready-to-use scenes and design stages using the A-Frame Inspector, as shown in Fig. 2. This visual tool allows for dragging, rotating, and scaling entities with immediate result previews.

After setting up the stage, a 360-degree background is added using a sky primitive, which applies either a color or 360° images as the scene's backdrop. The camera is positioned within the sky-sphere to ensure textures and distortions are rendered accurately from the user's perspective.

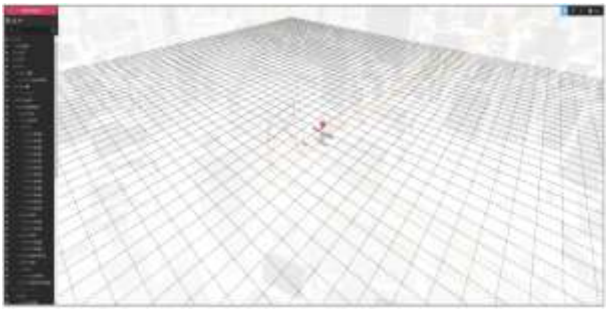


Fig. 2 *Scene Building Process*

To map the background seamlessly, the image used for the sky-sphere must be an equirectangular image, a type of projection that maps the surface of a sphere to a flat image. Fig. 3 shows an example of an equirectangular image.

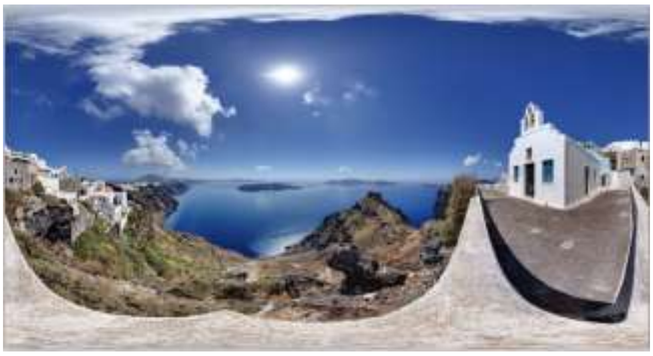


Fig.3 *Example of Equirectangular Image (Credits: [14])*

In this project, pre-existing equirectangular images from a repository are used, as capturing such images requires a 360-degree camera and specialized software for stitching panoramas to ensure proper alignment and distortion.

D. Splash Screen

A minimalist design splash screen is created, featuring hints and instructions to guide users, as shown in Fig. 4. The hints include navigational instructions for exploring the VR content and explanations of the functions for various buttons.

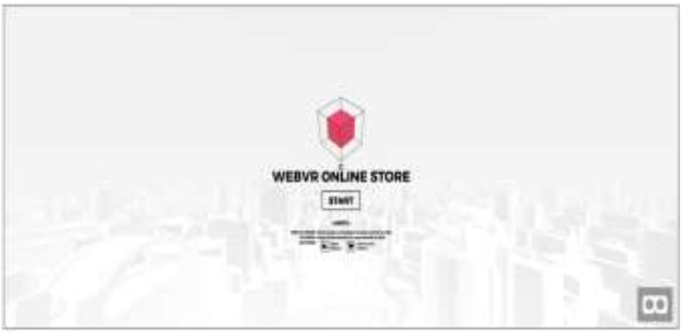


Fig. 4 *Splash Screen*

The layout of the splash screen includes an animated logo and a button to start the shopping navigation. Transition animations are added to enhance the browsing experience during the appearance of elements.

E. User Interface Design

Providing proper instructions and guidance on navigation controls is essential for users. The Toggle VR button is included to give users the option to browse the content either in a browser or through a VR viewer. This feature also prepares users before entering the VR mode. If users attempt to enter in portrait VR mode, a friendly guide is displayed to demonstrate the proper way to view the content and redirects them once they have corrected their orientation. Fig. 5 shows the Toggle VR button at the bottom-right corner of the figure.

The WebVR navigation pattern has yet to be standardized, as it is still in its early stages of development. Consequently, there is no standard procedure for performing specific actions. To address this, hints and instructions are provided as a workaround to guide users through the purchasing process.

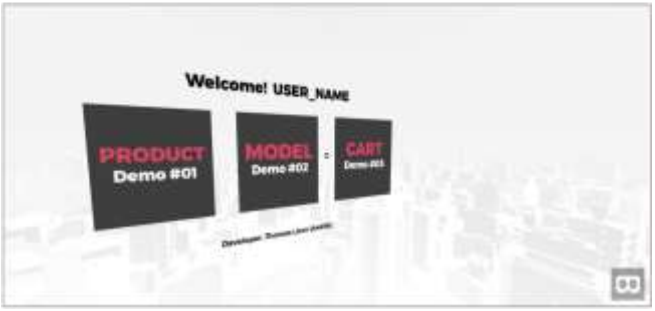


Fig. 5 *Main Menu with Toggle VR Button*

The VR content is displayed in a 360-degree view, which can occasionally cause users to lose their orientation when switching scenes. To address this, the user interface ensures that users are always oriented toward the content. A Back-to-Content indicator, as shown in Fig. 6, appears when the content region is outside the user's field of view. This indicator serves as a guide to help users return to the correct direction.

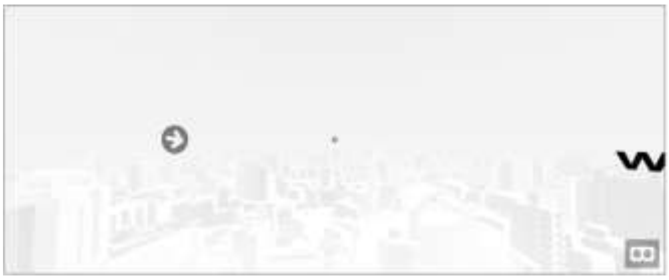


Fig. 6 *Back-to-Content Indicator*

The user interface employs a color scheme combining dark grey and fuchsia, which is believed to evoke a sense of excitement and modernity [15], as shown in Fig. 7.

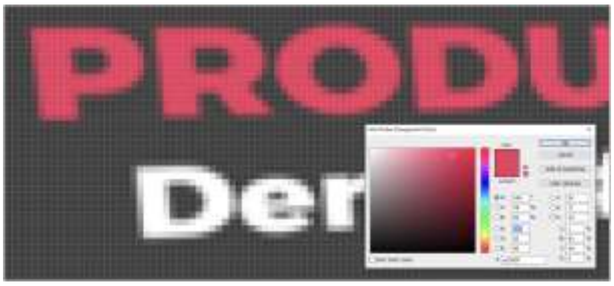


Fig. 7 *UI Colour Theme*

F. Camera and Cursor

A fixed-point interface is implemented to reduce motion sickness and provide easy access to layout controls, although it limits the utilization of space in a 3D environment.

To set up the fixed-point interface, a simple shape cursor or indicator is positioned at the center of the camera view, enabling users to access basic VR controls through clicking and gazing. This interaction is facilitated by a raycaster component that detects click events and captures only the first intersected entity. Fig. 8 shows the camera and cursor setup. When the mouse is clicked, the closest visible entity intersecting the cursor emits a click event. A simple ring geometry is used as the cursor, fixed at the center of the screen and attached as a child of the camera entity to ensure it remains centered regardless of the user's orientation. Events are triggered when the cursor interacts or fuses with an entity.

The system employs a Fuse-Based Cursor, also known as a gaze-based cursor. Instead of clicking or tapping, the cursor triggers a click when users gaze at an entity for a predetermined amount of time, resembling a laser extended from the user's head into the scene. If the user stares at an entity long enough, the cursor initiates a click on the respective entity. Figure 9 illustrates the Fuse-Based Cursor, with the left side showing the cursor idle and the right side showing it fusing with a menu button.

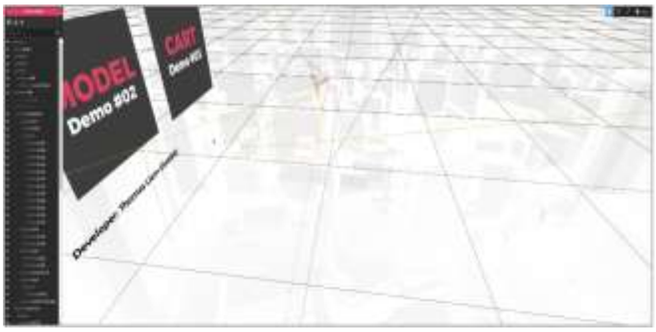


Fig. 8 *Camera and Cursor*

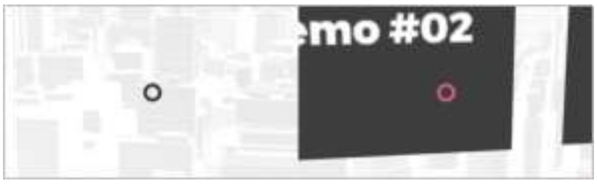


Fig. 9 *Fuse-Based Cursor*

The advantage of using fuse-based interaction for VR is that it does not require additional input devices other than the headset, making it ideal for Google Cardboard applications. However, the main drawback of the fuse-based cursor is that it requires users to turn their heads frequently, which can be physically demanding.

To enhance user experience, visual and audio feedback are incorporated to make the system more responsive and user-friendly. Whenever the cursor intersects with an entity, it emits an event that triggers the animation system, playing an animation along with an audio clip. This feedback provides users with a clear indication of the cursor's fusion with the entity.

G. *Object Modelling*

A-Frame supports assets imported from software like Blender, Maya, or 3DMax in formats such as OBJ and DAE. For this project, a COLLADA (.DAE) model is used, with the Collada model component loading the 3D assets.

Due to the complexity of 3D modeling, suitable object models were selected from a model repository to save time. These pre-existing sample models are compatible with the prototype. Once the 3D models are added to the scene, they are animated, allowing users to view the products in 360 degrees. Users can freely zoom in and rotate the objects as they change their view, as shown in Fig. 10.

The 360-degree product visualization adds significant value to the purchasing process by bridging the gap between imagination and reality. It allows customers to accurately visualize products, leading to more confident and satisfying purchase decisions.

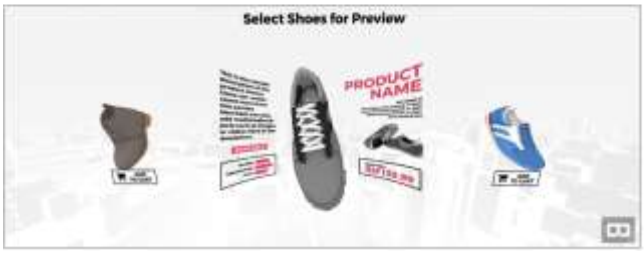


Fig. 10 *Information Panel*

H. *Payment Gateway*

At the time of developing this prototype, PayPal was the only feasible option for integrating a payment gateway into VR websites. Foreign payment gateways were less favorable due to the lack of multi-currency support, making PayPal the preferred choice as it could be easily integrated into websites written in any programming language. Fig. 11 shows the payment gateway implemented in VR mode.

It is worth noting that avoiding foreign gateways is less critical nowadays. Payment gateway solutions for VR websites have evolved, with APIs specifically designed for VR, such as Stripe, Meta Pay, and the Web Payment API.

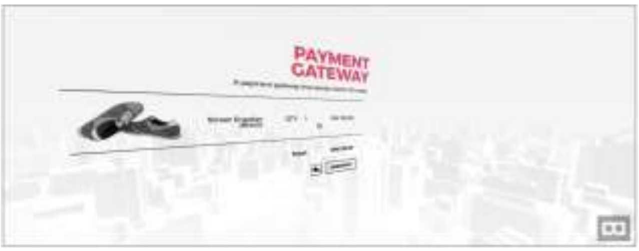


Fig. 11 *Payment Gateway*

I. *System Procedure*

When the system starts, users are presented with a splash screen. At this stage, all graphical assets are preloaded to ensure a seamless experience without delays before starting the session.

From the splash screen, users are redirected to the main menu, where three tile buttons are displayed, each corresponding to a different demo function. Users can select a tile button by gazing at it.

Selecting the product demo option transports users to the product demo scene, where three product models are available for preview. Gazing at a product model zooms in on the selected product and displays its information panel. The panel contains details such as the product description, price, availability, reviews, and ratings. If users are satisfied with the product, they can add it to their cart by selecting the 'Add to Cart' button.

Selecting the model demo option displays a rotating model, allowing users to visualize the product being worn for a better viewing experience. An information panel is also provided, displaying details about the product and the merchant. If satisfied, users can proceed by adding the product to their cart.

After adding items to the cart, users are redirected to the payment gateway. Since the payment gateway is accessible in VR mode, users do not need to remove their VR viewer to fill out the payment information form. The gateway displays the details of the selected product, enabling users to verify them before proceeding to checkout.

Once verified, users are redirected to PayPal for the checkout process. The purchasing process is considered complete once the payment is successfully made in PayPal and the transaction is processed without issues.

V. Preliminary Usability Testing

For the preliminary testing phase, the focus was placed on gathering qualitative feedback through a survey conducted with a selected group of participants who had experience with online shopping. The primary goal at this stage was to assess the system's usability, interface design, and overall user experience. Quantitative data, such as task completion times or success rates, was not collected during this phase as the objective was to identify areas for improvement rather than measure performance metrics.

From the preliminary testing, most participants agreed that the system features a user-friendly interface. They found that the hints and instructions available in every scene had effectively guided them through the purchasing process. Additionally, the clean and minimalist design, utilizing the selected color scheme, was well-received.

Participants reported minimal motion sickness during the process and found the experience interesting and engaging. Many noted that they had never tried online shopping in VR mode before and expressed interest in using the system again if it were officially launched.

Despite the positive feedback, some participants pointed out some limitations found with this prototype. A notable issue was the inability to control the rotation of 3D models during the preview. Users had to wait for the object to rotate to their desired position instead of freely adjusting it. Another limitation was the incomplete cart system, which allowed only one item to be added at a time. This was due to the lack of native support for such functionality in A-Frame, requiring the use of third-party JavaScript libraries.

Additionally, the system experienced disorientation errors when accessed on smartphones with smaller screens, impacting the overall user experience.

TABLE I
Feedback Summary

Positive Feedback	Negative Feedback
User-friendly interface	No control over 3D models
Motion sick minimized	Incomplete cart system
New and interesting experiences	Poor space management
Products visualized through 3D models	Limited compatibility

Table 1 provides the summary of the feedback from participants during this closed testing session.

According to [16], challenges include designing for various devices, addressing motion sickness and discomfort, and ensuring privacy and security. [17] further highlights issues like latency, power consumption, hardware stability, usability, and portability. While privacy and security are not the primary focus at this stage, this project encountered device compatibility and navigation issues during development. Creating an immersive WebVR environment that matches real-world experiences remains challenging, with latency being a critical factor that reduces user satisfaction and heightens motion sickness.

To address this issue while making the system accessible to everyday users, certain compromises are suggested. High-performance hardware typically required for seamless VR interactions could be substituted with simplified, predefined object viewing configurations, which would mitigate the impact of latency while maintaining usability. Similarly, adopting a minimalist user interface could reduce computational demands, addressing latency concerns and enhancing the user experience. These proposed trade-offs highlight the balance required to develop cost-effective WebVR systems.

VI. Conclusions

VR online shopping offers a unique and engaging experience. However, making it a common shopping experience for everyone requires time, resources, and collaborative effort.

Based on the feedback received, several improvements can be implemented for this prototype:

- Proper database implementation: A robust database is essential efficient data management. Integrating a database with third-party JavaScript libraries can enhance the cart system's functionality. Additionally, with the rise of AI, data collection can facilitate statistical analysis and insights into users' preferences and shopping patterns. This, in turn, can enable personalized recommendations for current and future purchases.
- Improved device compatibility: Display disorientation was reported during testing. For VR online shopping to appeal to a wider audience, compatibility with a broader range of devices, including tablets and smartphones with smaller screens, must be improved.
- Integration with AR: Augmented Reality (AR) can be incorporated to visualize virtual objects in the real world. Displaying objects in real-world dimensions could provide users with a better understanding of spatial usage, aiding in more informed purchasing decisions.

Although this prototype was initially developed in 2017, it remains relevant for continued research and development. Moving forward, recent technological advancements, particularly in privacy and security, will be incorporated to further extend and refine the original work presented here.

Acknowledgment

I would like to express my heartfelt gratitude to Thomas Liem for generously allowing me to use his work as the

foundation for this paper. His contributions provided a strong basis for extending the concept and adapting it to align with current technological advancements.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] E. Tkacz, A. Kapczynski, and Springerlink (Online Service), *Internet - Technical Development and Applications*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[2] O. H. Fares, J. Aversa, S. H. Lee, and J. Jacobson, "Virtual reality: A review and a new framework for integrated adoption," *International Journal of Consumer Studies*, vol. 48, no. 2, pp. xx–xx, 2024. doi: 10.1111/ijcs.13040.

[3] H. Estifaei, M. Riza and H. F. Manesh, "The implications of Virtual Reality technology in e-commerce," *2010 IEEE International Conference on Industrial Engineering and Engineering Management*, Macao, China, 2010, pp. 723-727, doi: 10.1109/IEEM.2010.5674615.

[4] R. Grande, J. Albusac, J. J. Castro-Schez, D. Vallejo and S. Sánchez-Sobrino, "A Virtual Reality Shopping platform for enhancing e-commerce activities of small businesses and local economies," *2023 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, Sydney, Australia, 2023, pp. 793-796, doi: 10.1109/ISMAR-Adjunct60411.2023.00175.

[5] M. E. Rana, K. Shanmugam and K. Y. Chong, "An Evaluation of Leveraging AR and VR for Enhanced Customer Engagement and Operational Efficiency in e-Commerce," *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Manama, Bahrain, 2024, pp. 917-923, doi: 10.1109/ICETSIS61505.2024.10459576.

[6] Anurag, R. Singh, P. Sharma, and V. Dutt, "E-commerce: The enhancement with the integration of AR and VR," in *Proceedings of the 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, Mohali, India, 2023, doi: 10.1109/icaiccit60255.2023.10465861.

[7] N. T. Singh, S. Singh, S. Singh, A. Arora, A. Dhaundiyal and A. Narang, "Transforming E-Commerce: Augmented Reality (AR) and Virtual Reality (VR) Integration for Interactive and Immersive Shopping Experiences," *2023 7th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*, Kolkata, India, 2023, pp. 1-5, doi: 10.1109/IEMENTech60402.2023.10423551.

[8] M. Sawiros, R. Lou, and Maged Rawash, "NEXT-GEN E-COMMERCE in the METAVERS," *2022 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, Oct. 2022, doi: https://doi.org/10.1109/ismar-adjunct57072.2022.00017.

[9] R. Y. Kim, "Retail After COVID-19: Use Virtual Reality to Enhance Ecommerce," *2022 IEEE Technology and Engineering Management Conference (TEMSCON EUROPE)*, Izmir, Turkey, 2022, pp. 118-123, doi: 10.1109/TEMSCONEUROPE54743.2022.9801972

[10] A. Chandak, A. Singh, S. Mishra, and S. Gupta, "Virtual Bazar—An interactive virtual reality store to support healthier food choices," in *Proceedings of the 2022 1st International Conference on Informatics (ICI)*, Noida, India, Apr. 2022, pp. 137–142. doi: 10.1109/ICI53355.2022.9786879.

[11] D. Shravani, P. Y. R, P. V. Atreyas and S. G, "VR Supermarket: a Virtual Reality Online Shopping Platform with a Dynamic Recommendation System," *2021 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*, Taichung, Taiwan, 2021, pp. 119-123, doi: 10.1109/AIVR52153.2021.00028.

[12] A-Frame Team, "Introduction to A-Frame," A-Frame Documentation, version 0.5.0. [Online]. Available: https://aframe.io/docs/0.5.0/introduction/. [Accessed: Jan. 6, 2025]

[13] Google, "It's your turn to make it," Google Cardboard Manufacturer's Kit, Aug. 6, 2024. [Online]. Available: https://developers.google.com/cardboard/manufacturers. [Accessed: Jan. 6, 2025].

[14] Topaz Labs, "Example of equirectangular image," 2013. [Online]. Available: https://www.topazlabs.com. [Accessed: Jan. 6, 2025]

[15] Hostinger, "Website color schemes: 50 design ideas for inspiration," Hostinger Tutorials, [Online]. Available: https://www.hostinger.my/tutorials/website-color-schemes. [Accessed: Jan. 7, 2025].

[16] S. Nocilla, "The Significance of Web VR/AR and AI: Challenges for UX/UI Designers," *ResearchGate*, Jan. 2024. [Online]. Available: https://www.researchgate.net/publication/377762085_The_Significance_of_Web_VRAR_and_AI_Challenges_for_UXUI_Designers. [Accessed: 11-Jan-2025].

[17] S. Lysenko and A. Kachur, "Challenges Towards VR Technology: VR Architecture Optimization," in *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2023, pp. 1-9. doi: 10.1109/DESSERT61349.2023.10416538.

https://doi.org/10.31436/ijpcc.v11i1.530

Digital Twin-Based Evaluation of Vehicular Controller Area Network Intrusion Detection Systems

Shaila Sharmin, Hafizah Mansor, Andi Fitriah Abdul Kadir, Amelia Ritahani Ismail

Department of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia

*Corresponding author shailasharmin@protonmail.com

(Received: 26th December, 2024; Accepted: 15th January, 2025; Published on-line: 30th January, 2025)

Abstract— The functions and operations of a modern automobile are becoming increasingly computerised, with this transformation made possible by Electronic Control Units (ECUs) that communicate and coordinate with each other on the in-vehicle network. Controller Area Network (CAN) is one of the most popular protocols for the in-vehicle network, supporting low latency and reliable communications. However, the CAN protocol does not have provisions for security, such as encryption, authentication, and authorisation, which makes it vulnerable to cyberattacks, particularly in today's automotive landscape characterised by extensive connectivity with external devices, vehicles, and infrastructure. While intrusion detection systems (IDS) for CAN have emerged as a key security measure, assessing their performance against realistic attacks remains a challenge since testing with real vehicles poses significant costs and safety risks and testbeds suffer from a lack of fidelity in terms of the CAN frame transmission timings and generated payloads. This work proposes a digital twin (DT)-based framework for CAN IDS evaluation that replicates the functionality of real-world ECUs and CAN bus of a vehicle with real-time flow of data from the physical bus to its virtual representation. The main contribution of this work is a CAN DT that can not only enable the generation of realistic attack traffic for simple and sophisticated attack scenarios but also the generation of diverse combinations of attack and real driving scenarios. This DT can facilitate the evaluation of both the detection capability and performance of CAN IDS. This work presents the methodology for generating the proposed DT and discusses current findings as well as future work.

Keywords— In-vehicle network, Controller Area Network, Intrusion detection, Digital twin

I. Introduction

The modern vehicle is capable of more than just moving passengers and cargo from one point to another – it has a myriad of features and functionalities that facilitate driving, enable safety and comfort, and support navigation, communication, and entertainment. These systems, which are increasingly computerised in modern vehicles, are enabled by as many as 150 microcontrollers called Electronic Control Units (ECUs) [1]. ECUs coordinate with each other by communicating the current state of the vehicle on internal vehicular networks or in-vehicle networks. Numerous protocols are implemented for in-vehicle networks with the most common being Controller Area Network (CAN).

The CAN protocol enables low-latency, reliable communications but does not provide mechanisms for encryption, authentication, or authorisation. This makes vehicular CAN bus vulnerable to a variety of cyberattacks that can allow car theft or cause dangerous accidents. This is especially true in today's automotive landscape where vehicles are equipped with a wide range of communication interfaces to enable vehicle-to-everything (V2X) connectivity. These interfaces, which include Wi-Fi, Bluetooth, and radio, enable external entities access to the in-vehicle network and become potential attack vectors. While Koscher et al. [2] established the vulnerability of vehicular CAN bus to injected CAN frames, Checkoway et al. [3] demonstrated the possibility of remotely attacking a vehicle's CAN bus. More recent work on CAN bus hacking underscores the continued need to secure the vehicular CAN bus [4], [5].

The development of intrusion detection systems (IDS) has emerged as a key effort towards securing the vehicular CAN bus. CAN IDS vary in the technique used as well as the feature of CAN bus traffic used for detection. Unlike conventional computer networks, a vehicular network represents a safety-critical system where a CAN IDS would need to detect attacks accurately and as quickly as possible to minimise harm to occupants and surroundings. As such, all CAN IDS need to be evaluated against realistic CAN bus traffic and attack scenarios to ensure their performance in a real in-vehicle network.

However, generating realistic attack scenarios remains a challenge since using real vehicles for security testing is a costly option and poses a safety risk to personnel and the environment. While testbeds and simulations do not have these issues and are an attractive alternative for security testing [6], [7], current proposals have limitations in fidelity, specifically in the behaviour and interactions of ECUs. This impacts the realism of the generated CAN frame payloads, particularly in attack scenarios and undermines the evaluation of payload-based CAN IDS carried out on such solutions.

The main contribution of this work is to propose a digital twin (DT)-based framework for generating a virtual representation of a real-world CAN bus, capable of accurately emulating the behaviour and interactions of real ECUs. This DT can, thus, be used to simulate both simple and sophisticated attacks and generate CAN attack traffic that is realistic in terms of frame transmission timings and payloads. Establishing the flow of data from the physical CAN bus to the virtual CAN bus can further enable the generation of countless combinations of attack and driving scenarios, resulting in robust security and performance assessment of CAN IDS.

The rest of the work is organised in the following manner: Section II provides an overview of the CAN protocol as well as the concept of Digital Twins. Section III discusses current proposals for CAN testbeds, simulations, and DT. Section IV outlines the proposed framework while Section V presents current results. Finally, Section VI concludes this work and discusses future work.

II. Background

A. *Controller Area Network (CAN)*

The Controller Area Network (CAN) protocol was introduced in the 1980s with the aim of enabling efficient, reliable communication for in-vehicle networks. It uses a bus architecture to connect Electronic Control Units (ECUs) within a vehicle that control and coordinate the various operations of the vehicle. This bus architecture significantly reduces the weight and complexity of the in-vehicle network compared to older point-to-point connections [8], [9]. CAN finds usage in critical vehicular subsystems such as powertrain and chassis that enable functions like power steering, braking and transmission [10].

CAN is a multi-master, message-based communication protocol, which means that any node on a CAN bus can transmit frames, and all frames are received by all nodes on the bus. A CAN data frame consists mainly of an arbitration identifier (AID), a data length code (DLC), and a data field [11]. The AID identifies a data frame and the information contained in the data field. While an ECU may broadcast multiple AIDs, a particular AID is typically broadcast by only one ECU [12]. Every ECU also subscribes to a list of AIDs and only reads the data frames of received frames that match these AIDs. The DLC specifies the number of bytes in the subsequent data field of the frame. The data field, which can be up to 64 bits, encodes the information being conveyed by the frame and represents the frame's payload.

An ECU encodes values of a particular set of signals in the data field of each AID and transmits the latest signal values to update all other nodes of the bus and coordinate the operations of the vehicle. While most AIDs are broadcast at fixed frequencies, some AIDs may be event-triggered and broadcast occasionally. The signals associated with each AID and the way they are encoded in the data field are specified in the form of rules in a CAN database (DBC). Unlike the format of a CAN frame which is specified by the CAN protocol, the CAN DBC may vary among different vehicle makes and models and is often kept proprietary and confidential.

Since any node on the CAN bus can transmit frames, CAN implements an arbitration mechanism when two nodes attempt to broadcast frames at the same time. In the event of bus contention, a frame with a lower-valued AID has higher priority and is broadcast first, while the higher-valued AID has lower priority and is retransmitted later. CAN has an error-handling mechanism implemented through cyclic redundancy checks and acknowledgement bits in the frame. It also has a method for error confinement to prevent errors from propagating in the bus whereby each node implements an error counter and is removed from the bus when the value of the error counter becomes too high (bus-off) [13], [14].

B. *CAN Attack Model*

CAN was designed for in-vehicle networks at a time when they were isolated systems. The security of the in-vehicle network was less of a concern while low latency and reliability were prioritised for the protocol. As a result, CAN lacks key security features like encryption, authentication, authorisation and integrity [8]. The modern vehicle also has many communication interfaces that allow external access to the in-vehicle network and thus act as attack vectors. These two factors combine to make the vehicular CAN bus vulnerable to a range of cyberattacks.

Cho & Shin [15] as well as Verma et al. [13] propose an attack model for the CAN bus which begins with the distinction between a weakly compromised node and a strongly compromised node. A weakly compromised node is one that an adversary has stopped from transmitting frames, while a strongly compromised node is one that the adversary has complete control over and can use to transmit malicious frames on the bus. This attack model categorises CAN bus attacks in the following manner:

1) *Fabrication attacks*: Fabrication attacks represent the most common type of CAN bus attacks, whereby an attacker uses a strongly compromised node to inject malicious frames. These include the following attacks:

- Denial of Service (DoS): A DoS attack is carried out by injecting frames with AID 0x000 and an arbitrary data field at a high frequency. This attack takes advantage of the CAN arbitration mechanism and prevents the broadcast of other legitimate frames. To evade security mechanisms in newer vehicles that prevent the transmission of frames with invalid AIDs, a DoS can be carried out by injecting the lowest-valued valid AID that appears in normal CAN traffic [8].

https://doi.org/10.31436/ijpcc.v11i1.530

- Fuzzing: A fuzzing attack involves the injection of frames with random AIDs and payloads at a high frequency. While the injection of random AIDs generally disrupts the transmission of legitimate frames, the random AIDs can include valid AIDs which can confuse ECUs about the real values of signals.
- Targeted ID or Spoofing: In a targeted ID attack, the adversary injects frames with a specific valid AID and manipulated payloads to cause ECUs that subscribe to the AID to malfunction. The fabricated frames may be injected at a high frequency in what is called a *flooding* delivery, or immediately following the appearance of legitimate frames of the same AID in a *flam* delivery. Both flooding and flam delivery achieve the same effect, but the latter does so with fewer fabricated frames.
- Replay: A replay attack is carried out by capturing a sequence of frames from the CAN bus and injecting them again at a later point in time when the vehicle is in a different state.

2) Suspension: A suspension attack involves weakly compromising a node on the CAN bus so that the node stops broadcasting CAN frames. This results in frames of the associated AIDs being missing from the bus traffic. A node can be prevented from broadcasting frames using any technique, such as by forcing it into the bus-off state [16].

3) Masquerade: A masquerade attack can be thought of as combining a suspension and a spoofing attack: legitimate transmissions of an AID are first suspended and then a malicious node injects spoofed frames of the same AID with manipulated payloads. This scenario is different from a spoofing attack where the fabricated frames appear alongside legitimate frames of the same AID, making it a more subtle, difficult-to-detect attack.

C. *Digital Twin*

The concept of digital twin (DT) was introduced by Grieves in 2003 who described it as “rich representations of products that are virtually indistinguishable from their physical counterparts” [17]. The DT concept model was described as including three components: physical objects, their virtual representations, and the data and information that connect these counterparts. From this early definition, the idea of what constitutes a digital twin has evolved [18], [19] but Guo et al. [20] find no consistent definition of DT in their survey. In the current literature, there are three levels of understanding of what a digital twin is that vary on the kind of interaction between the physical and virtual counterparts [18], [19]. The first may be described as a *digital model* where the virtual representation is built of a specific physical object, but there is no persistent flow of data between the two counterparts. The second may be described as a *digital shadow*, where there is a unidirectional flow of data from the physical twin to the virtual twin, with changes in the physical twin resulting in changes to the virtual twin. Finally, there is the *fully integrated digital twin*, represented in Fig. 1, where there is a bidirectional flow of data between the physical and virtual twin such that the virtual twin adapts to changes in the physical twin and provides feedback to the physical twin.

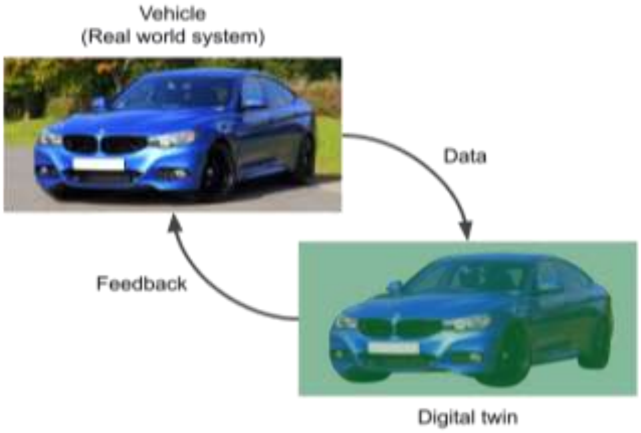


Fig. 1 Interactions in a fully-integrated DT

While some works [18], [19] emphasise the real-time, bidirectional flow of data between the virtual and physical counterparts as a key component of digital twins, such stipulations are considered restrictive in [21]. VanDerHorn and Mahadevan [21] consider two factors that distinguish a DT from a digital model or a simulation: a DT represents a particular instance of a physical object (e.g. a specific vehicle) instead of the entire class of the physical object, and the flow of data from the physical object to the virtual object over time. Other requirements on the digital twin may be considered with respect to the use case for which a particular implementation is aimed.

Digital twin technology is envisioned as an enabler of smart manufacturing and Industry 4.0. In the review of digital twin applications in the industry, [18] finds extensive applications of digital twins for product design, production, and product health management. Apart from these, DT can also be used for security applications such as in [22]. In this ‘virtual testing’ application of DT, DT is akin to a “more realistic and accurate” simulation and is used to simulate and explore different attack scenarios that would cause damage to real systems [19].

III. Literature Review

Intrusion detection systems (IDS) have emerged as a key mechanism for securing the vehicular CAN bus alongside encryption and authentication schemes. Current CAN IDS show a wide variety in the technique used for attack detection, ranging from relatively simpler statistical methods to advanced methods based on traditional

https://doi.org/10.31436/ijpcc.v11i1.530

machine learning (ML) as well as deep learning (DL) [23], [24]. CAN IDS also vary in terms of the features utilised for intrusion detection – an IDS may use the timing of CAN frames, sequences of AIDs, the payload of CAN frames, or any combination of these features for analysis and attack detection [10]. The in-vehicle network where a CAN IDS operates is distinct from conventional computer networks due to the limited computing capability of ECUs. The safety-critical nature of the in-vehicle network also necessitates low false-positive and false-negative rates, as well as fast attack detection. Therefore, in addition to meeting detection capability requirements measured using security metrics such as accuracy and F1-score, a CAN IDS should also meet non-functional requirements characterised by performance metrics such as detection latency [23].

Many CAN IDS proposals are evaluated in offline experiments using publicly available CAN intrusion datasets whereby the proposed methods are used to analyse the dataset. Using such datasets allows reproducibility of results and comparison of different methods under similar experimental settings [23]. However, evaluation using datasets are restricted to the attack scenarios contained in these datasets, which do not contain realistic samples of advanced attacks such as suspension and masquerade [13], [23]. Furthermore, evaluations with these datasets do not allow robust assessment of non-functional properties like detection latency and resource consumption in a realistic environment. As such, it is necessary to move towards online methods of evaluations which can allow the assessment of both detection capability and performance in varied attack scenarios and in experimental settings closely resembling real in-vehicle networks.

The best option for online testing is real vehicular CAN buses which are closest to real operating environments. Stachowski et al. [25] present an assessment methodology where CAN IDS products under test are integrated into a real vehicle for real-time performance evaluation. Three undisclosed anomaly-based CAN IDS products were evaluated in a vehicle on which various targeted ID attacks were performed while the vehicle was both stationary and in motion in a private test track. Their methodology encompasses both qualitative and quantitative metrics: while the quantitative metrics measure detection capability, the qualitative metrics include the effort required to integrate the IDS solution in a vehicle, flexibility of the solution, forensic capabilities, etc. However, only quantitative security metrics were reported, and performance metrics were not measured. There are further challenges associated with using real test vehicles. Conducting attacks on real vehicles runs the risk of permanently damaging the internal electronics. There is also a safety risk towards drivers, passengers, bystanders and surroundings [13], [26]. Furthermore, safely conducting security tests with a real vehicle also incurs significant costs, an example of which is a dynamometer used by Verma et al. [13] during CAN traffic collection. On the other hand, testbeds and simulations can mitigate these challenges by minimising the safety risks associated with running attack scenarios as well as minimising financial costs [26].

A. CAN Security Testbeds and Simulations

Numerous CAN testbeds and simulations have been developed for cybersecurity applications, such as for testing encryption schemes, reverse engineering, and penetration testing. Cros et al. [27] present a simulation platform called Cacao, aimed towards the evaluation of encryption and signature solution for CAN communications. Raspberry Pi devices are used to simulate nodes on a CAN network that has been used for monitoring bandwidth usage as a means of detecting brute-force attacks. Mundhenk et al. [28] also propose a discrete event simulator for assessing encryption schemes for CAN. Unlike Cacao, this platform was used to analyse real-time performance aspects like computation time and memory usage for authentication protocols.

Zheng et al. [29] propose a testbed architecture for security analysis of a vehicular CAN network, which can be used to capture CAN bus traffic for analysis and to simulate attacks. It consists of a real-time CAN bus simulation along with an emulated infotainment system that was used to simulate a DoS attack. Fowler et al. [30] also propose a CAN testbed based on a commercial Hardware-in-the-loop (HIL) solution, which they use to perform a penetration test in a case study, where vehicle network vulnerabilities are exploited using a dongle connected to the On-Board Diagnostic (OBD-II) port. Instead of simulating complete vehicle functionality, Granata et al. [31] aim to simplify security testing by emulating the minimum set of components to effectively reproduce security vulnerabilities. Their hybrid CAN bus simulation system, called HybridgeCAN, is proposed as a low-cost testbed alternative to expensive hardware-in-the-loop (HIL) testing systems and real vehicles.

Everett & McCoy [32] provide a software package and hardware framework as part of the Open Car Testbed and Network Experiments (OCTANE) testbed geared towards reverse engineering and testing of automotive networks. The software has a layered architecture, making it flexible and adaptable, while the hardware framework does not require specific hardware components. Portable Automotive Security Testbed with Adaptability (PASTA) [33] is another CAN testbed that focuses on white box ECUs which can be reprogrammed to set up the development environment as well as implement and test security solutions. It either disposes of or uses scaled-down versions of actuators and does not use expensive sensors to reduce cost and enhance safety and portability. A limitation of this testbed is that the software vehicle simulator does not reflect actual vehicle behaviour accurately.

While these testbeds are suitable for reverse-engineering, penetrating testing, and evaluating encryption methods, they do not focus on emulating realistic interaction among ECU nodes, hindering direct application for IDS evaluations.

B. Testbeds and Simulations for CAN IDS Evaluation

Compared to other cybersecurity applications, fewer testbeds and simulations are geared towards testing and evaluation of CAN IDS. A platform for evaluating CAN IDS employing various detection techniques and CAN bus traffic features would entail accurate simulation of CAN bus communications, not only in terms of the timing of messages but also the generation of realistic message payload data.

A real-time vehicular CAN bus testbed is provided by Jadidbonab et al. (2021) which can be used for training and testing CAN IDS. A virtual car in the CARLA autonomous vehicle simulator serves as the source of physical data input to simulated ECUs in a virtual CAN bus implemented in Vector CANoe that generates CAN bus traffic. While the virtual car enables the generation of realistic driving scenarios, the virtual CAN bus can be connected to a physical CAN bus consisting of an attack and IDS nodes. A clustering-based intrusion detection algorithm was tested against a targeted ID attack in two ways: offline, against a previously collected CAN bus log; and online, as a plug-and-play addition to the testbed. The classifier yielded lower accuracy and precision in the latter evaluation, which the authors discuss could be due to an overfitted model, inadequately representative training data, or issues with data parsing. However, the differences in the results underline the importance of performing online tests with CAN IDS. A limitation of this testbed is that it does not include bidirectional communication with the virtual car, i.e. the driving behaviour is not influenced by attacks on the virtual CAN bus.

Jichici et al. [7] also use Vector CANoe in their framework that integrates adversary model and intrusion detection nodes in a simulated CAN bus. CAN bus logs collected from a real vehicle are replayed in the virtual CAN bus, while an application interface is developed that allows configuration and launching of fuzzing and targeted ID attacks. MATLAB is used in this framework to enable implementation of CAN IDS, with a k-Nearest Neighbor (kNN) classifier used to demonstrate CAN IDS evaluation. Both message interval and data fields of the CAN bus traffic were used as features for the classifier, which generally yielded very good detection results in terms of sensitivity, specificity, false negative rate (FNR) and false positive rate (FPR). While the usage of real-world data in an industry-standard simulator makes for a realistic testbed, this testbed does not emulate ECUs. Furthermore, performance metrics like detection latency are not measured.

Another CAN bus security testbed is provided by Shi et al. [34] which focuses on maintaining similarity in timing between real-world CAN messages and those generated in the testbed. A real CAN bus log is fed into an ECU Operation Centre which in turn feeds corresponding time series data to each emulated ECU on the testbed CAN bus. A collector module is also implemented which reads messages broadcast by the emulated ECUs to a testbed database. The simulation is evaluated for stability and effectiveness, with the testbed messages demonstrating a relative delay of 0.8% and a negligible packet loss. Using a dynamic time warping (DTW) algorithm, it is also found that the similarity between the real CAN log and the CAN log collected from the testbed is very high. While all the fabrication attacks as well as suspension and masquerade attacks are described and implemented in this testbed, they have not been analysed or used for any form of security testing in this work.

An important limitation of these works is that they do not emulate the behaviour of ECUs. In other words, the simulations do not involve emulated ECUs that read data from the CAN bus. Therefore, attacks like fuzzing, targeted ID, and masquerade attacks that manipulate payloads of certain AIDs would not affect the payloads of other related AIDs. Analysis conducted in [35] using data from a CAN digital twin indicates that even during attacks, there is a correlation between messages containing related signals. In their example, an attack on messages containing vehicle speed is correlated with the change in engine speed. This implies that attacks targeting a particular AID affects messages of related AIDs as well, which would have a bearing on the performance of CAN IDS that analyse payloads. As such, a platform for simulating attacks on a CAN bus should be able to emulate the interactions between related ECUs for effective assessment of CAN IDS.

C. Digital Twin for Automotive CAN

Digital twin already finds diverse applications within the automotive field. Bhatti et al. [36] identify seven areas of application of digital twin technology in the automotive industry in their survey: (a) intelligent driver assistance, (b) autonomous navigation, (c) converters and inverters, (d) consumer centered development, (e) digital design and manufacturing, (f) health monitoring, and (g) battery management systems. In these application areas, DT is utilised to model all or some aspects of a vehicle's functions and operations in a virtual representation, which can be used to predict and analyse the behaviour and state of the replicated functions in various scenarios.

In the domain of automotive cybersecurity, digital twin-based approaches have been presented for privacy assessment and enhancement [37] as well as automated software security testing [38]. However, while the concept of a digital twin has already been applied for intrusion and anomaly detection in industrial cyber-physical systems [39],

[40], it has not been sufficiently explored in the literature with regard to utility for intrusion detection for automotive systems.

A DT-based approach to enable the design, implementation, and maintenance of vehicular wiring harnesses has been proposed in [41]. However, the use of DT for the simulation of in-vehicle networks remains a relatively nascent area of study. To enable use cases such as analysing effects of cyberattacks on in-vehicle networks and the development of security countermeasures, a digital twin of a real-world vehicular CAN bus called CarTwin is proposed by Popa et al. [35]. While previous work in this area focuses on replicating vehicle dynamics, this work replicates a real CAN bus in details like wire lengths, stub lengths, number of nodes, as well as data transmitted on the network. Seven different ECUs of the real CAN bus, related to power steering, instrument panel cluster, powertrain, etc., are emulated using MATLAB Simulink models implemented on development boards. These emulated ECUs not only broadcast CAN messages but also read CAN messages from the bus, thus simulating interactions of related subsystems on the CAN network. A software application with a user interface is used to provide input signals required by the ECU models. Experiments using signals from real CAN logs as input reveal a high correlation between output computed by the digital twin ECUs and the data in the real CAN log. The utility of this digital twin for security analysis is further demonstrated by an analysis of a targeted ID attack on the vehicle speed, where the authors find that messages communicating engine speed are also influenced. This is in contrast to a generic attack-free CAN log manipulated to simulate an attack, where there is no correlation between the targeted vehicle speed and the engine speed. However, this work does not focus on attack implementation or using the proposed DT for IDS evaluation. While CarTwin replicates a real-world CAN bus, it does not use the corresponding DBC for the CAN bus communications. Furthermore, an automatic flow of data from the physical CAN bus to the virtual representation is absent in this proposal, which makes it the ‘digital model’ level of DT.

D. Research Gap

An important limitation of prior CAN testbeds for IDS evaluation is that they lack ECU behaviour emulation. Since ECUs read and use data transmitted by other ECUs on the CAN bus, changes in a signal (e.g. braking signal) may result in changes in related signals (e.g. vehicle speed). As such, a spoofing or masquerading attack that targets a particular AID does not impact only signals of the targeted AID but also related signals in other AIDs. Therefore, if this interaction among ECUs is not replicated in the CAN testbed, the generated CAN data payloads would not reflect real-world data and would not be appropriate for evaluating CAN IDS. The fidelity of generated payloads is especially significant for the evaluation of CAN IDS that utilise frame payloads and leverage correlation among signals for anomaly detection.

While some works like [29], [35] implement ECU models to simulate ECU interactions, they are not geared towards IDS evaluations and do not implement diverse attack scenarios such as fuzzing or spoofing attacks. Simulations of driving scenarios in prior testbeds are also limited to replaying previously captured CAN traffic or generating CAN traffic with unrealistic signal values.

The present work aims to address these gaps by not only emulating the functionality and interactions of a real-world vehicular CAN bus but also implementing unidirectional, real-time data flow from the physical CAN bus to its virtual representation. By emulating ECU behaviours, we can generate realistic CAN bus data in both normal and attack scenarios. Furthermore, the data flow from the physical to the virtual twin would allow us to examine the impact of different attacks in any driving scenario the physical vehicle is in. The present work is thus a step closer to a true digital twin which can be used for robust evaluation of CAN IDS that is reflective of their performance in a real car.

IV. Proposed Evaluation Framework

The DT-based evaluation framework proposed in this work seeks to address the need for high fidelity, low risk, and low-cost alternatives for evaluating CAN IDS against diverse attack scenarios. The scope of the proposed CAN DT is to simulate the behaviour of ECUs on the real-world CAN bus to enable the generation of CAN bus traffic that is realistic in terms of timing and frame payloads, in both normal and attacks scenarios. Towards achieving this, data and specifications from a real-world vehicular CAN bus are collected and used to understand architecture of the target CAN bus as well as the bus traffic that is to be simulated. This information is used to implement a virtual CAN bus with virtual ECUs that simulate the behaviour and interactions of their physical counterparts. This would enable the generation of realistic CAN bus traffic, particularly under attack scenarios that are too risky to be conducted on a real vehicle. The generated CAN traffic can thus be used to perform detection capability and performance assessments of CAN IDS. The proposed DT framework allows not just repeatable experiments for IDS evaluation, but also has the potential to generate attack traffic for different driving scenarios using unidirectional flow of data from the physical CAN bus to its virtual twin. The proposed CAN DT-based framework is described in further detail in the following subsections.

A. Data Collection

To implement a realistic DT simulation of a selected vehicular CAN bus, we identify the following information and data that should be collected:

1) *Sample CAN bus traffic:* A sample of bus traffic collected from the target vehicular CAN bus is required to obtain the set of valid AIDs that are observed during normal operation as well as their normal observed transmission frequencies. In combination with the vehicle's DBC, this sample also serves as the source of bus traffic for running repeatable simulations of normal and attack scenarios. For vehicles that allow it, this sample may be collected from a vehicle's CAN bus via the OBD-II port. For other CAN buses not accessible via the OBD-II port, it is possible to tap the CAN bus and collect this data. We collected data from a Hyundai Sonata 2018, which provides direct access to a CAN bus via its OBD-II port. A sample of CAN bus traffic was collected with the aid of a Korlan USB2CAN adapter *[42]* which was used to connect a Linux laptop to the vehicle's CAN bus via the OBD-II port. The SocketCAN package in Linux provides the can-utils library which includes the functionality to log traffic from a CAN bus with not just the AID, DLC, and data field but also the timestamp.

2) *DBC:* The DBC for a vehicle specifies the rules for how signal data are encoded in frames of each AID. As such, it provides information such as the signals that are encoded by each AID, along with the ECUs that transmit each AID and the expected receivers. Although the best case would be to obtain the DBC for the vehicle from the Original Equipment Manufacturer (OEM), DBCs are often proprietary and commonly confidential to hinder CAN bus hacking. In such a situation, open source DBCs contributed to repositories like *opendbc [43]* may be leveraged. For the Hyundai Sonata 2018, we find a corresponding DBC in *opendbc*, *hyundai_2015_ccan.dbc*, that is applicable to the vehicle's CAN data.

3) *Wiring diagram:* The wiring diagram for the vehicle model, often part of auto mechanic manuals and available online, supplements the information that can be obtained from the DBC with respect to the wiring harness – the CAN bus segments that are present along with the number and functionality of ECUs on each segment. These details inform the architecture of the virtual CAN bus as well as the computational model that needs to be implemented for each virtual ECU.

B. *Data Analysis*

In this stage, the CAN bus traffic is analysed to examine (1) transmission frequencies of each AID, and (2) the relationships among signals transmitted by each AID.

Frames of each AID are typically broadcast by only one ECU and at regular intervals [13]. The time interval for each AID, which is not specified in the DBC, should be obtained from the collected CAN bus sample by analysing each stream of AIDs so that the virtual representations of the respective ECUs can be modelled to perform transmissions at similar intervals.

The DBC for the vehicle may be used to decode the signals transmitted in the captured CAN traffic. A pairwise correlation test performed among all the decoded signals from the dataset should reveal groups of signals showing high correlation among each other. Attacks targeting a particular AID, such as in a spoofing or masquerade attack, should result in changes not just to the signals of that AID, but also other AIDs with highly-correlated signals. These groups of correlated signals and AIDs can allow us to select a subset of ECUs if we are interested in a smaller scale simulation that can produce realistic changes under attack scenarios.

The data analysis may be performed with any statistical packages, such as the *pandas* and *numpy* Python packages in our case. For the deserialising signals from CAN frames using the DBC, we use the *cantools* Python library that provides utilities for parsing DBC files, encoding and decoding signals, monitoring and plotting CAN signals [44].

C. *ECU Modelling*

After identifying the signals and AIDs of interest and the corresponding ECUs, the behaviour of these ECUs needs to be emulated with respect to their functionalities and data transmission. For each ECU, given the set of input and output signals, we need to implement the computation model that can generate output signals from input. The virtual counterpart of each ECU, thus, uses the DBC to decode input signals from received CAN frames, compute output signals, and then encode the output signals in frames for transmission. The virtual ECUs transmit their respective AIDs at the time intervals determined in the data analysis stage. The virtual ECUs are connected on a virtual CAN bus which serves as the digital twin of the real-world CAN bus. The virtual CAN bus is interfaced with the physical counterpart so that signals generated on the real CAN bus can be sent to the virtual CAN bus as input.

We implement the virtual ECUs and CAN bus using the Vehicle Network Toolbox from MathWorks [45], which provides functions and blocks for CAN communication simulations. This virtual CAN bus is bridged to the real-world CAN bus, which could be via the vehicle's OBD-II port or, in the case of attack simulations repeated with a single driving scenario, a CAN bus prototype with an appropriate connector. If we consider a smaller scale DT whereby only a subset of ECUs are emulated, then frames transmitted by the other ECUs are replayed from the real CAN bus in the manner of a restbus simulation [35], [46].

https://doi.org/10.31436/ijpcc.v11i1.530

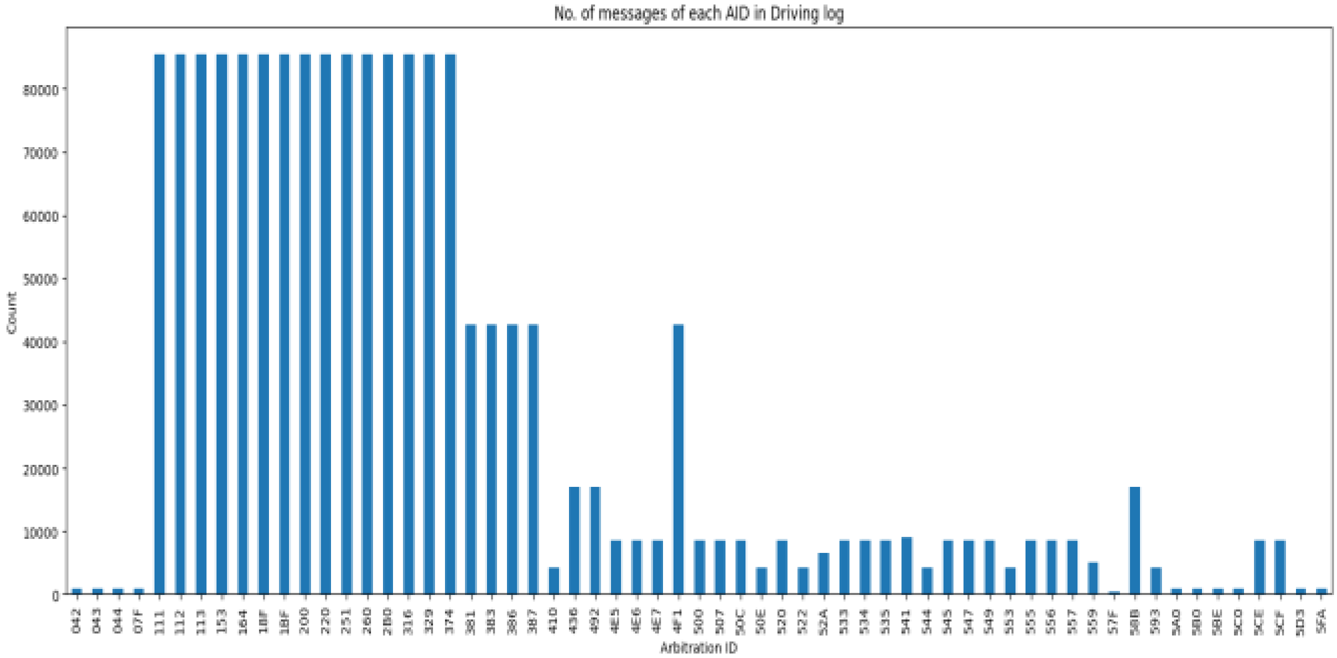


Fig. 2 Number of CAN frames by AID

D. *Attack Implementation*

Once the virtual CAN bus twin is operational, the attack scenarios required for IDS evaluation may be implemented. In the attack model that we consider, most attacks require a strongly compromised node that is capable of injecting frames on the CAN bus. As such, an attack node is added to the virtual CAN bus which can be programmed to inject frames at appropriate frequencies and suspend transmissions for fabrication, suspension, and masquerade attacks. Given that the virtual CAN bus represents a white box system where the AIDs and signals associated with all functionalities are known, the attack node can be set to execute spoofing, suspension, and masquerade attacks that target specific functionalities and inject malicious frames with the targeted AID. Executing DoS and fuzzing attacks are relatively simpler, and so is a replay attack, which entails capturing and replaying bus traffic from the real or virtual CAN bus.

E. *IDS Evaluation*

At this stage, the CAN DT may be used for IDS evaluation against different attack scenarios and in different driving scenarios. A node running the IDS as well as measuring evaluation metrics is added to the virtual DT for testing against the generated CAN traffic. The DT simulation can be run using either recorded sample of CAN bus traffic or real-time CAN traffic from the physical CAN bus. The former case allows data collected during a particular driving scenario to be used to drive a simulation multiple times with different attack scenarios. With this, one or more IDS can be evaluated against multiple attacks to obtain statistically significant results. In the case of using real-time CAN traffic from the physical CAN bus, attacks can be run against the vehicular CAN bus while the vehicle is in different driving situations, e.g. stationary, driving at high speeds. This can allow the evaluation of any CAN IDS against a wide variety of attack and driving scenario combinations.

While the DT can be used for real-time assessment of CAN IDS to measure both security and performance metrics, it can also be used to generate realistic attack datasets. Generated datasets used to evaluate a particular CAN IDS can also be made available along with the IDS so that future IDS proposals can be directly compared or benchmarked using the same datasets.

V. Findings and Discussion

As mentioned previously, we begin with collecting a sample of data from a Hyundai Sonata 2018. Approximately 14 minutes of driving data was collected while it was driven on urban roads. The collected data consisted of a total of 1,754,253 CAN frames, averaging 2054.82 frames transmitted per second. A total of 61 unique AIDs were found in this log. In Fig. 2 which shows the number of frames of each AID, we can see that, with some exceptions, frames with lower-valued AIDs appear the most on the CAN bus. This can be a result of the arbitration mechanism whereby lower-valued AIDs have higher priority for transmission and higher-valued AIDs have to wait for retransmission in the event of bus contention. Lower-valued AIDs are therefore always able to broadcast, while high-valued AIDs are transmitted fewer times due to lost arbitration in some situations.

A. *Timing Analysis*

We divided the collected CAN bus log into streams of frames of each AID and calculated the time interval for each frame. The time interval for a frame can be described as the period of time between the transmission of the frame and the transmission of the previous frame of the same AID. From these, we calculated the average time interval as well as the maximum percentage of deviation from the mean for each AID.

Apart from a few AIDs that appear at intervals of 1-2 seconds, a majority of the AIDs (50) in the CAN bus log were broadcast at time intervals under 0.2 seconds. In Fig. 3 which provides a distribution of these AIDs by average time interval, we can see that the time intervals even among these AIDs vary in magnitude and scale, ranging from 0.01 to 0.2 second.

The maximum percentage error from the mean time interval was calculated for each AID stream to understand the regularity of the CAN bus transmissions. As can be observed in Fig. 4, the largest number of AIDs show under 40% deviation from the average time interval, indicating that these are transmitted at reliably regular intervals. A smaller number of AIDs show greater variation, which is indicative of irregular or event-triggered transmissions. Variations in time intervals also arise from ECUs losing arbitration to higher-priority frame and having to wait to attempt retransmission of lower-priority frames.

It is important for any CAN bus modelling effort to take into consideration these timing features in CAN traffic. While lower-valued AIDs may always be transmitted at regular intervals without losing arbitration and without having frames delayed, higher-valued AIDs may lose arbitration and show delayed transmissions more often. These differences in timing characteristics are relevant considerations for timing- and frequency-based CAN IDS, which detect deviations from normal patterns in time intervals or frequencies. In the event of DoS or fuzzing attacks, it is expected for time intervals of legitimate frames to increase as the injected frames hinder normal transmissions, while a spoofing attack would cause time intervals of the targeted AID to decrease. Overall, a faithful CAN bus model should not only incorporate the dynamics of frame timing under normal operation, but also during different attack scenarios, for more accurate CAN IDS evaluations.

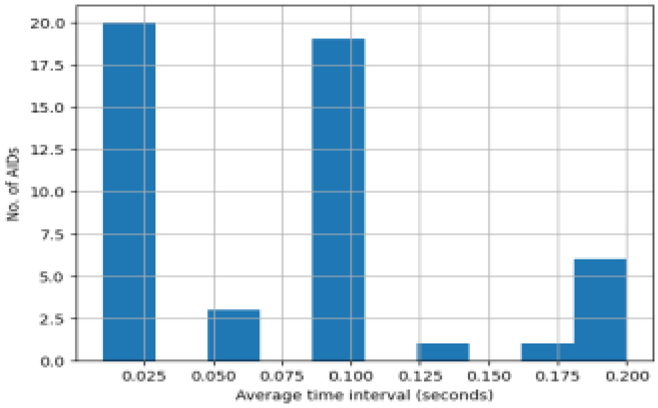


Fig. 3 Distribution of AIDs by average time interval, excluding AIDs with average time intervals greater than 0.25 second

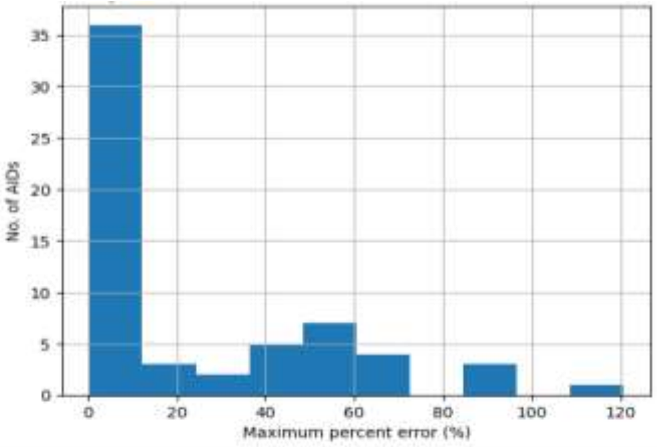


Fig. 4 Distribution of AIDs by maximum percent error from average time interval

TABLE 1
SENDER ECUS FOUND IN COLLECTED CAN LOG

Acronym in DBC	**Full name**
DATC	Dual Automatic Temperature Control
BCM	Body Control Module
TCU	Transmission Control Unit
ESC	Electronic Stability Control
EMS	Engine Management System
MDPS	Motor Driven Power Steering
ABS	Anti-lock Brake System
CLU	Cluster Module
ACU	Airbag Control Unit
FPCM	Fuel injection Pump Control Module
LCA	Lane Centering/Change Assist
ODS	Occupant Detection System

B. *Signal Analysis*

The data collected from the Hyundai Sonata 2018 consisted of CAN data frames with payloads in raw bytes. To deserialise the signals encoded in these data frames, we use the *hyundai_2015_ccan*.db file from *opendbc*, using which we are able to deserialise signals for 48 AIDs. These 48 AIDs are transmitted by 12 ECUs responsible for different subsystems, which are listed in Table 1.

The *cantools* library was used to deserialise signals from the CAN log using the aforementioned DBC file to yield a total of 627 signals. Of these signals, 493 signals remain constant throughout the CAN bus log, leaving 134 signals for analysis. We visualise the steering angle signal from AID 0x2B0, transmitted by the MDPS ECU in **Error! Reference source not found.** as well as the individual wheel speeds from AID 0x386, transmitted by the ABS ECU in Fig. 6.

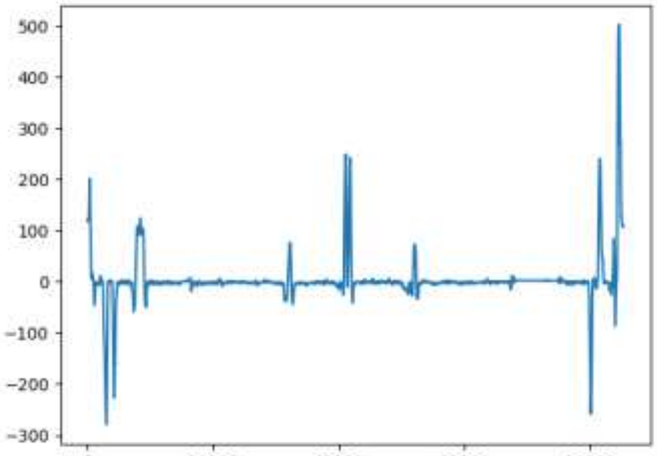


Fig. 5 Steering angle signal from AID 0x2B0

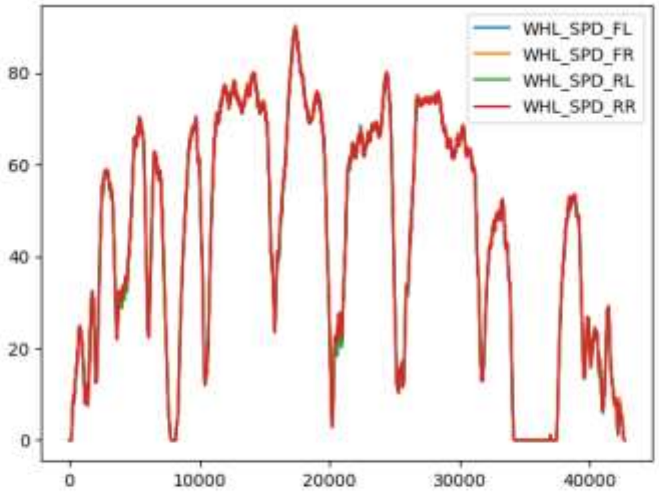


Fig. 6 Individual wheel speed signals from AID 0x386

To understand how different signals are related to each other and identify groups of correlated signals, we perform a pairwise Pearson correlation test on the non-constant 134 signals and generate a correlation heatmap, which is available at [47]. Signals showing a magnitude of correlation coefficient higher than 0.5 are listed in Table 2. The signals in the heatmap are reorganised by applying hierarchical agglomerative clustering with complete linkage, to facilitate the identification of signal clusters showing high correlations. While it may be expected to find correlations among signals originating from the same ECUs, we see in this heatmap significant correlations among signals originating from *different* AIDs and ECUs. An example is wheel speed signals from ABS AIDs showing a high positive correlation with signals from TCU and EMS ECUs. These correlations indicate that it is possible for changes in a signal to result in changes in other related signals. This is due to the fact that each ECU uses data transmitted by other ECUs as input for its respective functions and in turn, transmits signals that are used by other ECUs.

The correlation among related signals should also be maintained in attack scenarios like spoofing and masquerade where fabricated frames with manipulated payloads are injected to provide false information to ECUs. In this situation, when ECUs read and use the spoofed values of signals in the malicious frames, the anomaly cascades into the data transmitted by these ECUs. Such effects of attacks on CAN bus traffic are not captured in other methods of generating CAN bus data such as augmentation of benign CAN bus logs or testbeds that do not emulate ECU behaviour [35]. In such methods, the injected frames do not produce any changes in related frames, which is different from what would be observed in a real CAN bus and is thus not useful for evaluating CAN IDS particularly based on analysing frame payloads.

VI. Conclusions and Future Work

Using real vehicles for attack simulation and security testing can be restrictive in terms of the associated costs, safety risks, and attack scenarios that can be conducted. While testbeds and simulations do not have these challenges, they do not provide sufficient fidelity for the assessment of CAN IDS that use different features of CAN bus traffic. An important limitation of current testbeds and simulations is that they do not emulate the interaction of ECUs or generate realistic CAN traffic. This work aims to address these gaps by proposing a DT-based evaluation framework for CAN IDS which can be used to generate diverse attack scenarios and perform detection capability and performance evaluations of CAN IDS. This CAN DT models a real-world CAN bus at the ECU level and interfaces with the real-world bus for data to drive the DT simulation. Not only can it allow repeatable simulations of attack

https://doi.org/10.31436/ijpcc.v11i1.530

TABLE 2
SIGNALS WITH ABSOLUTE CORRELATION COEFFICIENT GREATER THAN 0.5

No.	Signal	AID	Sender	Highly correlated signals
1	CR_Datc_OutTempF	044	DATC	59, 83
2	CF_Tcu_Alive1	111	TCU	10, 15
3	N_TC	111	TCU	8, 7, 12, 21, 23, 45, 42, 51, 50, 65, 64, 63, 62, 69, 71, 80, 84, 85, 86, 89
4	SWI_CC	111	TCU	9, 7, 12, 36, 47, 42, 65, 64, 63, 62, 69, 71, 85
5	SWI_GS	111	TCU	16
6	TEMP_AT	111	TCU	53, 68, 74, 75, 77, 90
7	VS_TCU	112	TCU	3, 4, 9, 8, 12, 21, 23, 36, 45, 42, 65, 64, 63, 62, 69, 71, 80, 84, 85
8	N_TC_RAW	112	TCU	3, 7, 12, 21, 23, 45, 42, 51, 50, 65, 64, 63, 62, 69, 71, 80, 84, 85, 86, 89
9	CUR_GR	112	TCU	4, 7, 12, 36, 42, 65, 64, 63, 62, 69, 71, 85
10	CF_Tcu_Alive	112	TCU	2, 15
11	N_INC_TCU	112	TCU	13
12	CF_Tcu_TarGr	113	TCU	3, 4, 9, 8, 7, 21, 36, 42, 65, 64, 63, 62, 69, 71, 85
13	N_TGT_LUP	113	TCU	11
14	CF_Tcu_ShfPatt	113	TCU	38, 54
15	CF_Tcu_Alive3	113	TCU	2, 10
16	CF_Tcu_ITPhase	113	TCU	5
17	AliveCounter_TCS1	153	ESC	18
18	CheckSum_TCS1	153	ESC	17
19	CF_Esc_AliveCnt	164	ESC	20, 29
20	CF_Esc_Chksum	164	ESC	19, 29
21	R_NEngIdlTgC	18F	EMS	3, 8, 7, 12, 23, 45, 42, 51, 50, 65, 64, 63, 62, 69, 71, 80, 84, 85, 86, 89
22	R_PAcnC	18F	EMS	60, 61, 73, 76
23	CF_Ems_PumpTPres	200	EMS	3, 8, 7, 21, 40, 45, 42, 51, 50, 65, 64, 63, 62, 69, 71, 80, 84, 85, 86, 89
24	FCO	200	EMS	35, 33, 45, 44, 43, 51, 50, 82, 84, 86, 88, 89
25	LONG_ACCEL	220	ESC	40, 35, 37, 33, 45, 44, 43, 51, 50, 82, 84, 86, 88, 89
26	YAW_RATE	220	ESC	27, 30, 31, 32, 41, 56
27	LAT_ACCEL	220	ESC	26, 30, 31, 32, 41, 56
28	CYL_PRES	220	ESC	52, 72, 87
29	ESP12_Checksum	220	ESC	19, 20
30	CR_Mdps_OutTq	251	MDPS	27, 26, 31, 32, 41, 56
31	CR_Mdps_StrColTq	251	MDPS	27, 26, 30, 32, 41, 56
32	CR_Mdps_StrTq	251	MDPS	27, 26, 30, 31, 41, 56
33	TQI_TARGET	260	EMS	24, 25, 40, 35, 37, 45, 44, 43, 51, 50, 82, 84, 86, 88, 89
34	TQI_MAX	260	EMS	46, 48, 87
35	TQI	260	EMS	24, 25, 40, 37, 33, 45, 44, 43, 51, 50, 82, 84, 86, 88, 89
36	SPK_TIME_CUR	260	EMS	4, 9, 7, 12, 47, 42, 65, 64, 63, 62, 69, 71, 81, 85
37	TQI_MIN	260	EMS	25, 35, 33, 44, 43, 51, 50, 82, 86, 88, 89
38	CRUISE_LAMP_S	260	EMS	14, 54
39	CRUISE_LAMP_M	260	EMS	75, 77, 90
40	CF_Ems_AclAct	260	EMS	23, 25, 35, 33, 45, 44, 43, 51, 50, 82, 84, 86, 88, 89
41	SAS_Angle	2B0	MDPS	27, 26, 30, 31, 32, 56
42	VS	316	EMS	3, 4, 9, 8, 7, 12, 21, 23, 36, 45, 65, 64, 63, 62, 69, 71, 80, 84, 85
43	TQI_ACOR	316	EMS	24, 25, 40, 35, 37, 33, 45, 44, 51, 50, 82, 84, 86, 88, 89
44	TQI	316	EMS	24, 25, 40, 35, 37, 33, 45, 43, 51, 50, 82, 84, 86, 88, 89
45	N	316	EMS	3, 8, 7, 21, 23, 24, 25, 40, 35, 33, 44, 43, 42, 51, 50, 65, 64, 63, 62, 69, 80, 82, 84, 85, 86, 89

scenarios for statistically significant IDS evaluations, but, with the flow of data from the real to the virtual CAN bus, it can be used to generate any combination of attack and driving scenarios for a thorough assessment of CAN IDS that is reflective of performance in the real-world. Towards building the DT of a real CAN bus, we collected data from a Hyundai Sonata 2018 and analysed timing and signal data to understand patterns that are relevant to intrusion detection and ECU modelling.

There are several challenges with the proposed CAN DT for CAN IDS evaluation. Firstly, it relies on the vehicle DBC, which is not always available for all vehicle models. While we

https://doi.org/10.31436/ijpcc.v11i1.530

TABLE 2 (CONTD.)
SIGNALS WITH ABSOLUTE CORRELATION COEFFICIENT GREATER THAN 0.5

No.	Signal	AID	Sender	Highly correlated signals
46	RATIO_TQI_BAS_MAX_STND	316	EMS	34
47	PUC_STAT	316	EMS	4, 36, 81
48	TQFR	316	EMS	34
49	TEMP_ENG	329	EMS	59, 83
50	TPS	329	EMS	3, 8, 21, 23, 24, 25, 40, 35, 37, 33, 45, 44, 43, 51, 82, 84, 86, 88, 89
51	PV_AV_CAN	329	EMS	3, 8, 21, 23, 24, 25, 40, 35, 37, 33, 45, 44, 43, 50, 82, 84, 86, 88, 89
52	BRAKE_ACT	329	EMS	28, 72, 87
53	MAF_FAC_ALTI_MMV	329	EMS	6, 68, 74, 75, 77, 90
54	ACC_ACT	329	EMS	14, 38
55	MUL_CODE	329	EMS	66
56	CR_Mdps_DrvTq	381	MDPS	27, 26, 30, 31, 32, 41
57	CF_Fatc_ChkSum	383	DATC	58
58	CF_Fatc_MsgCnt	383	DATC	57
59	CR_Fatc_OutTemp	383	DATC	1, 49, 83
60	CR_Fatc_OutTempSns	383	DATC	22, 61, 73, 76
61	CR_Fatc_TqAcnOut	383	DATC	22, 60, 73
62	WHL_SPD_RR	386	ABS	3, 4, 9, 8, 7, 12, 21, 23, 36, 45, 42, 65, 64, 63, 69, 71, 80, 84, 85
63	WHL_SPD_RL	386	ABS	3, 4, 9, 8, 7, 12, 21, 23, 36, 45, 42, 65, 64, 62, 69, 71, 80, 84, 85
64	WHL_SPD_FR	386	ABS	3, 4, 9, 8, 7, 12, 21, 23, 36, 45, 42, 65, 63, 62, 69, 71, 80, 84, 85
65	WHL_SPD_FL	386	ABS	3, 4, 9, 8, 7, 12, 21, 23, 36, 45, 42, 64, 63, 62, 69, 71, 80, 84, 85
66	WHL_SPD_AliveCounter_MSB	386	ABS	55
67	CF_Ems_ModeledAmbTemp	492	EMS	70, 76
68	CR_Ems_EngOilTemp	492	EMS	6, 53, 74, 77, 90
69	CF_Clu_Vanz	4F1	CLU	3, 4, 9, 8, 7, 12, 21, 23, 36, 45, 42, 65, 64, 63, 62, 71, 80, 84, 85
70	CF_Clu_DTE	50C	CLU	67, 73, 76
71	CF_Clu_VehicleSpeed	52A	CLU	3, 4, 9, 8, 7, 12, 21, 23, 36, 42, 65, 64, 63, 62, 69, 80, 84, 85
72	BAT_Alt_FR_Duty	545	EMS	28, 52, 87
73	TEMP_FUEL	545	EMS	22, 60, 61, 70, 76
74	AMP_CAN	545	EMS	6, 53, 68, 75, 77, 90
75	CTR_CDN_OBD	547	EMS	6, 39, 53, 74, 77, 90
76	IntAirTemp	547	EMS	22, 60, 67, 70, 73
77	STATE_DC_OBD	547	EMS	6, 39, 53, 68, 74, 75, 90
78	BAT_SOH	549	EMS	79
79	BAT_SOC	549	EMS	78
80	CR_Fpcm_LPActPre	555	FPCM	3, 8, 7, 21, 23, 45, 42, 65, 64, 63, 62, 69, 71, 84, 85
81	PID_03h	556	EMS	36, 47
82	PID_04h	556	EMS	24, 25, 40, 35, 37, 33, 45, 44, 43, 51, 50, 84, 86, 88, 89
83	PID_05h	556	EMS	1, 49, 59
84	PID_0Ch	556	EMS	3, 8, 7, 21, 23, 24, 25, 40, 35, 33, 45, 44, 43, 42, 51, 50, 65, 64, 63, 62, 69, 71, 80, 82, 85, 86, 89
85	PID_0Dh	556	EMS	3, 4, 9, 8, 7, 12, 21, 23, 36, 45, 42, 65, 64, 63, 62, 69, 71, 80, 84
86	PID_11h	556	EMS	3, 8, 21, 23, 24, 25, 40, 35, 37, 33, 45, 44, 43, 51, 50, 82, 84, 88, 89
87	PID_07h	557	EMS	28, 34, 52, 72
88	PID_0Bh	557	EMS	24, 25, 40, 35, 37, 33, 44, 43, 51, 50, 82, 86, 89
89	PID_23h	557	EMS	3, 8, 21, 23, 24, 25, 40, 35, 37, 33, 45, 44, 43, 51, 50, 82, 84, 86, 88
90	CF_Clu_Odometer	5B0	CLU	6, 39, 53, 68, 74, 75, 77

use an open-source DBC for our vehicle, such DBC is not available for all car models, which restricts the number of vehicles to which this methodology can be applied.

Moreover, the implementation of data flow between the physical CAN bus and the device hosting its virtual twin may introduce a new attack vector and raise security and privacy concerns. This attack vector could potentially be exploited to sniff the physical CAN bus and steal data revealing information such as driving behaviour or conduct attacks on the physical CAN bus that interfere with normal operation. It is necessary to implement security measures while establishing communication between the physical and digital twin to ensure that these threats do not become a reality. Finally, it is also pertinent to explore resource utilisation of the virtual twin, especially if we are interested in scaling up the virtual representation by increasing the number of ECUs that are emulated in the virtual CAN bus.

Implementation of the CAN DT using insights gathered from data analysis and validating the accuracy of generated CAN bus traffic remain as future work.

ACKNOWLEDGMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] R. N. Charette, “How Software Is Eating the Car,” IEEE Spectrum. Accessed: Sep. 08, 2022. [Online]. Available https://spectrum.ieee.org/software-eating-car

[2] K. Koscher, A. Czeskis, F. Roesner, S. Patel, and T. Kohno, “Experimental Security Analysis of a Modern Automobile,” *2010 IEEE Symp. Secur. Priv.*, pp. 1–16, 2010.

[3] S. Checkoway *et al.*, “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” *Proc. 20th USENIX Secur. Symp.*, pp. 77–92, 2011.

[4] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” in *Black Hat USA*, Las Vegas, 2015.

[5] “Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars,” Keen Security Lab Blog. Accessed: Jun. 14, 2022. [Online]. Available: http://keenlab.tencent.com/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/index.html

[6] H. Jadidbonab, A. Tomlinson, H. N. Nguyen, T. Doan, and S. A. Shaikh, “A Real-Time In-Vehicle Network Testbed for Machine Learning-Based IDS Training and Validation,” 2021, p. 16.

[7] C. Jichici, B. Groza, and P.-S. Murvay, “Integrating Adversary Models and Intrusion Detection Systems for In-vehicle Networks in CANoe,” in *Innovative Security Solutions for Information Technology and Communications*, vol. 12001, E. Simion and R. Géraud-Stewart, Eds., in Lecture Notes in Computer Science, vol. 12001. , Cham: Springer International Publishing, 2020, pp. 241–256. doi: 10.1007/978-3-030-41025-4_16.

[8] B. Lampe and W. Meng, “can-train-and-test: A curated CAN dataset for automotive intrusion detection,” *Comput. Secur.*, vol. 140, p. 103777, May 2024, doi: 10.1016/j.cose.2024.103777.

[9] F. Pollicino, D. Stabili, and M. Marchetti, “Performance Comparison of Timing-Based Anomaly Detectors for Controller Area Network: A Reproducible Study,” *ACM Trans. Cyber-Phys. Syst.*, vol. 8, no. 2, pp. 1–24, Apr. 2024, doi: 10.1145/3604913.

[10] E. Aliwa, O. Rana, C. Perera, and P. Burnap, “Cyberattacks and Countermeasures for In-Vehicle Networks,” *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–37, Apr. 2021, doi: 10.1145/3431233.

[11] K. Tindell, “The canframe.py tool,” Ken Tindell’s blog. Accessed: Jan. 27, 2023. [Online]. Available: https://kentindell.github.io/2020/01/03/canframe_py_tool/

[12] D. Stabili, F. Pollicino, and A. Rota, “A benchmark framework for CAN IDS,” presented at the Italian Conference on Cyber Security, Apr. 2021.

[13] M. E. Verma *et al.*, “A comprehensive guide to CAN IDS data and introduction of the ROAD dataset,” *PLOS ONE*, vol. 19, no. 1, p. e0296879, Jan. 2024, doi: 10.1371/journal.pone.0296879.

[14] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, “Evaluation of CAN Bus Security Challenges,” *Sens. Switz.*, vol. 20, no. 8, 2020, doi: 10.3390/s20082364.

[15] K.-T. Cho and K. G. Shin, “Fingerprinting Electronic Control Units for Vehicle Intrusion Detection,” in *25th USENIX Security Symposium (USENIX Security 16)*, Austin, Texas: USENIX Association, 2016, pp. 911--927. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cho

[16] K.-T. Cho and K. G. Shin, “Error Handling of In-vehicle Networks Makes Them Vulnerable,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna Austria: ACM, Oct. 2016, pp. 1044–1055. doi: 10.1145/2976749.2978302.

[17] M. Grieves, “Digital Twin: Manufacturing Excellence through Virtual Factory Replication,” 2014.

[18] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, “Digital Twin in Industry: State-of-the-Art,” *IEEE Trans. Ind. Inform.*, vol. 15, no. 4, pp. 2405–2415, 2019, doi: 10.1109/TII.2018.2873186.

[19] M. Liu, S. Fang, H. Dong, and C. Xu, “Review of digital twin about concepts, technologies, and industrial applications,” *J. Manuf. Syst.*, vol. 58, no. October 2019, pp. 346–361, 2021, doi: 10.1016/j.jmsy.2020.06.017.

[20] J. Guo, M. Bilal, Y. Qiu, C. Qian, X. Xu, and K.-K. Raymond Choo, “Survey on digital twins for Internet of Vehicles: Fundamentals, challenges, and opportunities,” *Digit. Commun. Netw.*, vol. 10, no. 2, pp. 237–247, Apr. 2024, doi: 10.1016/j.dcan.2022.05.023.

[21] E. VanDerHorn and S. Mahadevan, “Digital Twin: Generalization, characterization and implementation,” *Decis. Support Syst.*, vol. 145, p. 113524, Jun. 2021, doi: 10.1016/j.dss.2021.113524.

[22] M. Eckhart and A. Ekelhart, “Towards security-aware virtual environments for digital twins,” *CPSS 2018 - Proc. 4th ACM Workshop Cyber-Phys. Syst. Secur. Co-Located ASIA CCS 2018*, pp. 61–72, 2018, doi: 10.1145/3198458.3198464.

[23] S. Sharmin, H. Mansor, A. F. Abdul Kadir, and N. A. Aziz, “Benchmarking frameworks and comparative studies of Controller Area Network (CAN) intrusion detection systems: A review,” *J. Comput. Secur.*, vol. 32, no. 5, pp. 477–507, Nov. 2024, doi: 10.3233/JCS-230027.

[24] G. Karopoulos, G. Kambourakis, E. Chatzoglou, J. L. Hernández-Ramos, and V. Kouliaridis, “Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and a Meta-Taxonomy,” *Electronics*, vol. 11, no. 7, p. 1072, Mar. 2022, doi: 10.3390/electronics11071072.

[25] S. Stachowski, R. Gaynier, and D. J. LeBlanc, “An Assessment Method for Automotive Intrusion Detection System Performance,” National Highway Traffic Safety Administration, Washington, D.C., DOT HS 812 708, Apr. 2019.

[26] S. Mahmood, H. N. Nguyen, and S. A. Shaikh, “Automotive Cybersecurity Testing: Survey of Testbeds and Methods,” in *Digital Transformation, Cyber Security and Resilience of Modern Societies*, vol. 84, T. Tagarev, K. T. Atanassov, V. Kharchenko, and J. Kacprzyk, Eds., in Studies in Big Data, vol. 84. , Cham: Springer International Publishing, 2021, pp. 219–243. doi: 10.1007/978-3-030-65722-2_14.

[27] O. Cros, A. Thiroux, and G. Chênevert, “Cacao, a CAN-Bus Simulation Platform for Secured Vehicular Communication,” in *Ad Hoc Networks*, vol. 345, L. Foschini and M. El Kamili, Eds., in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 345. , Cham: Springer International Publishing, 2021, pp. 213–224. doi: 10.1007/978-3-030-67369-7_16.

[28] P. Mundhenk, A. Mrowca, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty, “Open source model and simulator for real-time performance analysis of automotive network security,” *ACM SIGBED Rev.*, vol. 13, no. 3, pp. 8–13, Aug. 2016, doi: 10.1145/2983185.2983186.

[29] X. Zheng, L. Pan, H. Chen, R. Di Pietro, and L. Batten, “A Testbed for Security Analysis of Modern Vehicle Systems,” in *2017 IEEE*

Trustcom/BigDataSE/ICESS, Sydney, NSW: IEEE, Aug. 2017, pp. 1090–1095. doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.357.

[30] D. S. Fowler, M. Cheah, S. A. Shaikh, and J. Bryans, "Towards a Testbed for Automotive Cybersecurity," in *2017 IEEE International Conference on Software Testing, Verification and Validation (ICST)*, Tokyo, Japan: IEEE, Mar. 2017, pp. 540–541. doi: 10.1109/ICST.2017.62.

[31] D. Granata, M. Rak, and G. Salzillo, "Towards HybridgeCAN, a hybrid bridged CAN platform for automotive security testing," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece: IEEE, Jul. 2021, pp. 249–254. doi: 10.1109/CSR51186.2021.9527969.

[32] C. E. Everett and D. McCoy, "OCTANE: Open Car Testbed And Network Experiments Bringing Cyber-Physical Security Research to Researchers and Students," in *6th Workshop on Cyber Security Experimentation and Test*, 2013, p. 8.

[33] T. Toyama, T. Yoshida, H. Oguma, and T. Matsumoto, "PASTA: Portable Automotive Security Testbed with Adaptability," presented at the Black Hat Europe, London, 2018.

[34] D. Shi, L. Kou, C. Huo, and T. Wu, "A CAN Bus Security Testbed Framework for Automotive Cyber-Physical Systems," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–11, Aug. 2022, doi: 10.1155/2022/7176194.

[35] L. Popa, A. Berdich, and B. Groza, "CarTwin—Development of a Digital Twin for a Real-World In-Vehicle CAN Network," *Appl. Sci.*, vol. 13, no. 1, p. 445, Dec. 2022, doi: 10.3390/app13010445.

[36] G. Bhatti, H. Mohan, and R. Raja Singh, "Towards the future of smart electric vehicles: Digital twin technology," *Renew. Sustain. Energy Rev.*, vol. 141, no. January, p. 110801, 2021, doi: 10.1016/j.rser.2021.110801.

[37] V. Damjanovic-Behrendt, "A Digital Twin-based Privacy Enhancement Mechanism for the Automotive Industry," 2018, pp. 272–279.

[38] S. Marksteiner, S. Bronfman, M. Wolf, and E. Lazebnik, "Using Cyber Digital Twins for Automated Automotive Cybersecurity Testing," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria: IEEE, Sep. 2021, pp. 123–128. doi: 10.1109/EuroSPW54576.2021.00020.

[39] F. Akbarian, E. Fitzgerald, and M. Kihl, "Intrusion Detection in Digital Twins for Industrial Control Systems," *2020 28th Int. Conf. Softw. Telecommun. Comput. Netw. SoftCOM 2020*, 2020, doi: 10.23919/SoftCOM50211.2020.9238162.

[40] A. Pokhrel, V. Katta, and R. Colomo-Palacios, "Digital Twin for Cybersecurity Incident Prediction: A Multivocal Literature Review," *Proc. - 2020 IEEEACM 42nd Int. Conf. Softw. Eng. Workshop ICSEW 2020*, pp. 671–678, 2020, doi: 10.1145/3387940.3392199.

[41] R. Tharma, R. Winter, and M. Eigner, "An Approach for the Implementation of the Digital Twin in the Automotive Wiring Harness Field," presented at the 15th International Design Conference, 2018, pp. 3023–3032. doi: 10.21278/idc.2018.0188.

[42] "Korlan USB2CAN - 8devices." Accessed: Jun. 21, 2024. [Online]. Available: https://www.8devices.com/products/usb2can_korlan

[43] "commaai/opendbc: democratize access to car decoder rings." Accessed: Jan. 20, 2024. [Online]. Available: https://github.com/commaai/opendbc

[44] "CAN BUS tools — cantools 39.4.3.dev10+gcc02988 documentation." Accessed: Dec. 26, 2024. [Online]. Available: https://cantools.readthedocs.io/en/latest/

[45] "Vehicle Network Toolbox." Accessed: Dec. 26, 2024. [Online]. Available: https://www.mathworks.com/help/vnt/index.html

[46] "Accelerating Testing with Advanced ECU Restbus Simulation." Accessed: Dec. 24, 2024. [Online]. Available: https://www.ni.com/en/solutions/transportation/hardware-in-the-loop/vehicle-communication-software-suite.html

[47] S. Sharmin, "Pairwise Pearson correlation heatmap for non- constant signals extracted from a Hyundai Sonata 2018." Zenodo, Jan. 2025. doi: 10.5281/zenodo.14627705.

https://doi.org/10.31436/ijpcc.v11i1.561

Examining Mortality Risk Prediction Using Machine Learning in Heart Failure Patients

Mohammad Khalid Hussain, Sharyar Wani, Adamu Abubakar

Department of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia

*Corresponding author mohammad.khalid.hussain@gmail.com

(Received: 26th December, 2024; Accepted: 15th January, 2025; Published on-line: 30th January, 2025)

Abstract— Heart failure is fatal. Signs and symptoms of heart failure often overlap with those of other medical conditions. These symptoms could kill the patient. Predicting heart failure mortality helps healthcare workers spend resources to reduce or prevent deaths. Demographics, laboratory tests, and vital signs were used to create and test prediction models. This study compares random forests, and support vector machine to determine the best mortality risk prediction approach. This study analyses heart failure symptoms to identify risk factors for mortality. The study also examines how these findings apply to all heart failure patients. The study collects a subset of MIMIC-III heart failure patients to achieve this goal. Previous research studies used a smaller dataset, which is compared to this one. The experimental examination of blood creatinine, ejection fraction, and binned age shows that machine learning is be able to classify heart failure patients by mortality risk. This information helps clinicians improve treatment, improving patient outcomes and resource allocation. The study shows that machine learning can improve heart failure mortality risk prediction by using large clinical datasets like MIMIC-III. This study advances predictive analytics in healthcare, giving valuable information for clinicians and academics seeking to better heart failure patient care.

Keywords— Blood creatinine, Ejection fraction, Logistic regression, random forests, gradient boosting, heart failure

I. Introduction

Machine learning prediction tasks typically involve datasets that can be organized to distinguish between expected and unexpected outcomes, enabling effective model training and evaluation [1-2]. There exist studies suggesting that the assessment of a cardiac patient's mortality can be accomplished by evaluating the heart's ejection fraction and blood creatinine levels [3]. Nevertheless, it should be noted that the datasets employed in those studies are constrained in their scope. The dataset exhibits a significant likelihood that the model generated is not applicable to various types of patient data. The act of selecting and organizing a dataset from a publicly accessible database, such as the Medical Information Mart for Intensive Care (MIMIC-III) and subsequently implementing a comparable procedure on this dataset facilitates the development of a more comprehensive model. The dataset possesses a substantial amount of information and offers the opportunity to even incorporate race as a variable while constructing the model if need be.

Heart failure (HF) with preserved ejection fraction is common and is associated with substantial morbidity and mortality [4]. Clinical trials do not provide sufficient evidence to help guide renal dysfunction. This is despite the fact that renal dysfunction is extremely common in patients with chronic heart failure (CHF) and related to worse outcomes a lot of the treatments for CHF are the cause of worsening renal function [3]. Serum creatinine levels are an indicator of proper renal function. Serum creatinine is a waste product caused by muscle wear and tear and the kidneys are responsible for removing it from the blood. The European Society of Cardiology raises the breakoff point to greater than 50% or if its level reaches a limit of 266 μmol/L [6]. At the same time, it should be noted that the initial rise of serum creatinine may not necessarily corelate to intrinsic kidney injury but to a change in haemodynamics. This is because HF patients usually have reduced renal function at baseline and thus even a small decrease in renal function will increase serum creatinine to an extent that may even require stopping necessary medication for recovery.

The past couple of decades has seen a shift from manual record systems to electronic record systems in many fields. Information systems refer to all elements required to transfer information and respective processing procedures within an organization. Such information is collected, transformed, and disseminated by a combination of people, hardware and software, communication networks, and data resources [7].

Information systems are used in many fields such as business, economics, law, education, government administration, and medicine. Specific examples include enterprise planning, customer relationship management, and supply chain management [7]. Information systems are extremely beneficial in areas where data is of great importance. One such area is the medical field. Application of information systems in the medical field include patient monitoring and Electronic Health Record (EHR) systems. Patient records are required for medical and legal reasons. The use of computerized patient records has been around for about four decades [8]. Computerized patient records ease documentation and administrative procedures [9]. Examples include prevention of redundant tests and patient history inquiry at point of care. The former will not only save time but also costs. In addition, they can be used for analysis to help reduce medical errors and thus improve overall healthcare [10].

An EHR is a computerized information record composed of a person's health data. It accumulates longitudinal, cross-institutional, and multi-modal health data. It also has to be based on a standard so that interoperability is possible Interoperability is important for cross-institutional usage as well as enabling a life-long patient history [11]. In summary, EHRs contain all medical information of a patient, both past and present.

The use of EHR systems assumes that users who need access are equipped with necessary equipment and software [11]. If the requirements are fulfilled, EHR systems offer several advantages: availability and ease of retrieval, access, and transfer of information. However, they are not without their disadvantages. EHR systems require substantial startup costs with regard to hardware and software. Users will also require training in order to use them. Furthermore, dedicated IT staff is required for system maintenance [11]. Examples of EHR systems include OpenMRS, HOSxP, WorldVistA, GNU Health, and OpenEMR.

Given the increasing need to derive actionable insights and solutions from existing electronic healthcare system data, significant knowledge can be extracted, particularly in areas such as heart attack and mortality risk prediction for heart failure patients. Machine learning offers powerful tools to address these challenges effectively. Consequently, the objective of this study is to examine mortality risk prediction in heart failure patients using machine learning techniques.

The structure of the paper is as follows: Section 1 provides an introduction and an overview of the research. Section 2 presents a review of relevant literature. Section 3 outlines the models and performance evaluation metrics employed in the study. Section 4 focuses on the analysis and presentation of the results, followed by Section 5, which provides a discussion of the findings. Finally, Section 6 concludes the research with key takeaways and implications.

II. RELATED WORK

The selected literature covers machine learning, healthcare systems, and chronic disease management. These studies span a wide spectrum of issues, from data preprocessing approaches in machine learning to specific clinical applications like heart failure and chronic renal disease. This review group papers by approach and examines methodology, performance indicators, and findings.

Data preprocessing and efficient machine learning methodologies are explained in Shen et al. [1] and Kumar et al. [2]. Shen et al. [1] reviewed large data preparation strategies and stressed their importance in machine learning model quality and reliability. Their investigation emphasized approaches such as feature selection, dimensionality reduction, and handling missing data, which are crucial for scalable big data applications. Accuracy, precision, and recall were used to assess preprocessing impacts across datasets. Kumar et al. [2] examined healthcare dataset machine learning predictive analytics issues. They discussed methods such as ensemble learning and neural networks, emphasizing the importance of balancing bias and variance. The authors used F1 score, MSE, and AUC-ROC to compare models, showing that hybrid models can provide reliable predictions.

Murphy et al. [3] and Redfield [4] examined heart failure with reduced and preserved ejection fractions as clinical entities. Murphy et al. [3] studied heart failure with reduced ejection fraction (HFrEF) etiology and treatment choices, stressing predictive analytics' mortality risk management potential. While their study did not expressly analyze machine learning models, the implications for applying advanced predictive tools in optimizing therapy were evident.

In his study on heart failure with preserved ejection fraction (HFpEF), Redfield [4] detailed clinical and diagnostic problems. Predictive models using biomarkers like ejection fraction and comorbidities improved clinical decision-making. Forbes and Gallagher [5] and Ponikowski et al. [6] studied chronic kidney disease (CKD) and cardiac failure. Forbes and Gallagher [5] gave CKD assessment and management a framework that stressed early detection and personalized management. Although not explicitly linked to machine learning, their findings align with predictive analytics in early disease detection.

Acute and chronic heart failure clinical recommendations were developed by Ponikowski et al. [6]. These guidelines provide structured data for machine learning models to predict patient outcomes and optimize therapy routes. Model performance could include survival rates, predicted accuracy, and rehospitalization reduction. Several researches examined healthcare infrastructure and EHRs.

Xu and Quaddus [7] focused on information systems infrastructure management and the need for robust data storage and processing for predictive analytics.

Kirch [11] offered a succinct summary of the importance of EHRs in public health, noting their potential to enable large-scale machine learning applications. Haux et al. [10] expected healthcare information system improvements to enhance clinical decision-making and research. Giere [8], Hollerbach et al. [9], and Kirch [11] examined electronic patient information and document security. They stress the importance of secure, interoperable, and accessible data for advanced analytics and machine learning.

These researches agree that machine learning and electronic healthcare systems can transform predictive analytics, especially chronic illness management. Clinical studies give organized data and practical applications, while data preparation and infrastructure studies demonstrate the technical foundations of effective analytics. These studies measure accuracy, precision, recall, AUC-ROC, and clinical outcomes like survival and hospitalization reduction. These metrics underline the effectiveness of machine learning models in addressing healthcare challenges.

Chicco and Jurman [12] also carried out research in the same domain as Ahmad et al. [13] using the latter's dataset. However, their research differs in that they apply machine learning classifiers in contrast to purely statistical methods. They also rank the features that are significant in determining mortality risk among heart failure patients corresponding to the most important risk factors. In order to evaluate the ranking, they also perform biostatistics tests and compare them. Both methods used for feature ranking showed ejection fraction and serum creatinine as the most relevant features that affected mortality and thus, they built their mortality risk machine learning models based on these two factors alone. They learned that not only are ejection fraction and serum creatinine enough for predicting mortality risk, using just these two features for mortality risk prediction classifiers resulted in more accurate models. Their approach effectively showed that machine learning can be used for binary classification (presence of death event or not) of electronic health records of patients with heart failure.

The evaluated papers show that powerful machine learning, robust data preparation, and healthcare applications work together. They show that predictive analytics can improve clinical decision-making in heart failure and CKD care. In line with these methods, this study uses machine learning to predict heart failure mortality risk.

III. RESEARCH METHODOLOGY

The research uses the design science research methodology. Design science is used to study the "creation of artifacts and their embedding in our physical, psychological, economic, social and virtual environments." Good design improves life through the creation of "innovative, sustainable products and services," by creating value, and by mitigating any unintentional negative results of technology use. Design science combines both analysis and synthesis in product and system design by drawing from several scientific disciplines [14].

A. Data Acquisition and Preparation

The dataset, called the Medical Information Mart for Intensive Care v3 (MIMIC-III) by Johnson et al. [15] was obtained for this research [15]. The data set is a collection of 40 tables with a total of 534 columns and 728,556,685 rows organized as a relational database. In order to prepare data sets for use in the experiments, the required data had to be curated from the database and converted into a compatible format such as CSV before it could be used in the experiment. All the required features could be directly extracted from the database with the exception of the ejection fraction. This had to be specifically extracted from the clinical notes. The interim CSV files created with the previous step were passed through a filter written in the R language to extract the required ejection fraction values from the patients' echodiagram notes.

The raw dataset was generated as a result of first: it comes from patients that were diagnosed with heart failure. Patients are older than 16, i.e. patients that are not neonates. Serum creatinine and ejection fraction categories were obtained from different tables linked with the admissions table. First, the subset of patients with heart failure diagnosis was obtained by limiting the International Classification of Diseases (ICD-9) codes on the pattern 428%. This pattern helps include congestive heart failure (428.0), left heart failure (428.1), systolic heart failure (428.2), diastolic heart failure (428.3), combined systolic and diastolic heart failure (428.4), as well as general heart failure (428.9). Patients' ages and whether they died during their admission was obtained from the admission data. The former was extracted from dates of birth. Patients who were not admitted were omitted since we are focusing on inpatients.

The ejection fraction data and serum creatinine were held in different tables. Serum creatinine was obtained from the 'labevents' table. This value is regularly obtained from patients. Since we are dealing with a prediction problem, we need to take the first reading of serum creatinine when the patient is admitted.

The ejection fraction data is stored as plain text in the echodiagram data. These notes are stored in the 'noteevents' table under the category 'Echo'. Similar to serum creatinine, only the very first reading of the ejection fraction is required. But unlike serum creatinine, ejection fraction values need to be extracted from the echodiagram notes.

B. *The Trained Models*

1) Random Forest

Random forest, similar to bagging and boosting, is a binary tree-based ensemble method classifier. Ensemble methods create models with a lower variance by combining the output of multiple simpler models (often called "learners"). In order to understand the random forest ensemble method, it is imperative that decision trees are discussed. The main parts of a decision tree are nodes and branches. To make understanding easier, tree-based terminology will be discussed briefly:

- Nodes: these are of three types: (1) root/decision/parent nodes: these represents a data sample and a decision rule (e.g. patients above the age of 45?), (2) internal/chance nodes: these present the possible choices at a juncture in a decision tree that is not the root or leaf nodes of the decision tree (e.g. patients age below or equal to 45), and (3) leaf/end nodes: these are terminal nodes of a decision tree. which represent the final result of a decision tree after going through all the possible decisions at a subset of root nodes.
- Branches: these represent all possible outcomes from a decision tree, binary or otherwise. They are presented by the pathway from root nodes to leaf nodes going through internal nodes.
- Splitting: data samples at parent nodes need to be split into purer internal until they reach leaf nodes of for the respective target variable. Both continuous and discrete input variables can be used. The parent node is split into two at subsequent internal nodes into two (in the case of binary trees) "bins" depending on their value. The split is determined based on the degree of "purity" of resultant child nodes from the parent node where the split is made. This "purity" may be determined using entropy, Gini index, classification error, information gain, gain ratio, or twoing criteria. Splitting continues under the required homogeneity in the initial data sample is reached [16].

Since random forests are "binary" tree-based, the decision trees are always split into two at the nodes. At each node, the decision rule is determined by choosing a conditional rule that ensures the highest information gain. This means that the rule should provide the best separation between the available values at that level.

A random forest is a classifier consisting of a collection of tree-structured classifiers $h(x,\omega_k),k=1,\ldots$ where the ω_k are independent identically distributed random vectors and each tree casts a unit vote for the most popular class at input x.

Of course, all the trees used in a random forest cannot be giving the same classification results, since that would defeat the purpose of having the classifier in the first place. This is because if the average of the same classification results would be equal to each single classification result individually. Thus, one extra regulatory step is added at each split of every tree: only a random chosen subset of the predictors is considered. Essentially, the trees are actively prohibited from taking into consideration some of the predictors in each split. At first glance, this may seem counterintuitive, but it makes sense once we realize that we are aiming for a classification model that be used on a generalized data set, thus this will provide the model a greater perception of the training data. This is what results in a more robust classification model.

2) Support vector machine (SVM)

Support vector machine (SVM) is a supervised learning classifier used in classification problems. SVM can be explained simply if we consider a plot of two groups of multiple points on a 2D coordinate plane. SVM will try to determine the best line to create a split between the two groups to help classify any new points. A basic classification model would attempt to place a straight line between the points where the differentiation is clear, i.e. it is easily determined which groups a certain coordinate point is from. The same would apply in a 3D plane but the only difference is that in this case, SVMs will try to determine the best plane instead of line to classify the training points. At the heart of SVMs is an optimization problem. This problem takes a function, e.g. the equation of a line in a clear 2D plane situation and determines the best values that ensure the maximum distance between points of the two groups that are closest to the split; these points are known as support vectors. The functions that are optimized can be changed depending on the situation of points on a plane.

C. *Experimental Analysis Tools*

The MIMIC-III database was originally created using PostgreSQL and was thus uploaded to a local schema instance of PostgreSQL; there is no choice of choosing a different RDBMS. Jupyter notebook was used to extract the required data. Python was used as the programming language. It was used in a Google Colaboratory (Colab) environment. SQL queries were written within strings in a Python context and then executed to generate results. The ejection fraction of patients in the MIMIC-III database were not always available as values in a column. Instead, some records of ejection fraction were stored in the patients' clinical notes. In order to extract them from the clinical records, an R language filter created by Major [17] was used.

The filter extracts the ejection fraction values from the clinical notes using regular expressions (Regex).

In order to provide comma-separated values (CSV) files for the Jupyter notebooks, the patient data was first extracted from the PostgreSQL database and saved as CSV files. These CSV files were then processed using the aforementioned R filter by Major [17]. Once the ejection fraction values were extracted, the required sub-datasets for the different experiments were created using Jupyter notebook and processed. The sets of features used to predict mortality are {serum creatinine (SC), ejection fraction (EF)}, {serum creatinine (SC), ejection fraction (EF), age}, and {serum creatinine (SC), ejection fraction (EF), age, sex}.

IV. PRESENTATION OF THE RESULTS

The research paper examining mortality risk prediction using machine learning in heart failure patients presents an investigation of a number of different machine learning models that were applied to the MIMIC-III dataset. Some of the most important variables, including serum creatinine (SC), ejection fraction (EF), and age, are included in the dataset. These variables are analyzed according to several demographic categories, including overall, men, and females. The results of the evaluations of models with SC and EF are presented in Table I. A poor area under the curve (AUC) of 0.4931 indicates that the Random Forest Classifier (RFC) has limited predictive capacity. However, it attained a moderate level of accuracy (72.14%). The fact that the model had low recall and F1 scores demonstrates that it is unable to accurately identify situations that are actual affirmative responses. With an accuracy of 76.50% but an area under the curve (AUC) of 0.0, the SVM with Linear Kernel performed incredibly badly, indicating that there was no distinction between the classes. There was a lack of satisfaction with both the recall (10.89%) and the F1 scores (4.14%).

TABLE I
. RESULTS OF MIMIC-III DATASET WITH SC AND EF

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
Random Forest Classifier	0.7214	0.4931	0.1631	0.1504	0.1558	-0.0100	-0.0101	0.821
SVM - Linear Kernel	0.7650	0.0000	0.1089	0.0558	0.0414	-0.0049	-0.0107	0.061

Results using SC, EF, and Age are included in Table II, which demonstrates some small improvements. RFC demonstrated an increase in accuracy (77.45%) and area under the curve (0.5404), indicating a somewhat enhanced capacity to differentiate between outcomes. There was a noticeable improvement in the predicted reliability, as evidenced by the fact that the precision reached 20.53%. A higher recall of 43.27 percent was demonstrated using SVM, but it lacked precision and F1 score consistency, which indicated that the predictions were not balanced. The incorporation of age results in a marginal improvement in prediction power, particularly for RFC. Nevertheless, the models, on the whole, have difficulty delivering reliable forecasts, which indicates that there is a requirement for either additional features or other techniques.

TABLE II
RESULTS OF MIMIC-III DATASET WITH SC, EF, AND AGE

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
Random Forest Classifier	0.7745	0.5404	0.1597	0.2053	0.1790	0.0510	0.0517	0.865
SVM - Linear Kernel	0.5453	0.0000	0.4327	0.0984	0.1336	-0.0052	0.0011	0.068

As compared to SVM, RFC produced a higher accuracy (73.32%) and area under the curve (AUC) (0.5741) when SC and EF were used (see Table III) but only for male patients. However, its inadequate capacity to detect good outcomes is highlighted by its recall rate of 19.84% and its F1 score of 18.28%. However, SVM had a worse F1 score (18.86%) and a lower precision (11.42%), despite having a better recall (64.47%).

TABLE III
RESULTS OF MIMIC-III DATASET WITH SC AND EF FOR MALES ONLY

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
SVM - Linear Kernel	0.4165	0.0000	0.6447	0.1142	0.1886	0.0111	0.0159	0.1610
Random Forest Classifier	0.7332	0.5741	0.1984	0.1730	0.1828	0.0261	0.0264	0.7460

RFC attained a high level of accuracy (81.29%) with SC and EF (Table IV) when limited to female patients, however its area under the curve (AUC) was 52.97%. Poor true positive predictions are indicated by the recall rate (10.03%) and the F1 rate (14.47%). With a recall of 0.37% and a precision of 3.33%, SVM performed worse.

TABLE IV
RESULTS OF MIMIC-III DATASET WITH SC AND EF FOR FEMALES ONLY

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
SVM - Linear Kernel	0.8388	0.0000	0.0037	0.0333	0.0067	-0.0016	-0.0012	0.038
Random Forest Classifier	0.8129	0.5297	0.1003	0.2675	0.1447	0.0626	0.0733	0.642

There was a decrease in performance for both models when Age (Table V) was included for the males-only dataset (previously, only SC and EF were used). The RFC scored higher in accuracy (82.75%), but it had a significantly lower recall rate (3.57%). Each and every metric revealed that SVM performed poorly.

TABLE V
RESULTS OF MIMIC-III DATASET WITH SC, EF, AND AGE FOR MALES ONLY

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
Random Forest Classifier	0.8275	0.5445	0.0357	0.1925	0.0589	0.0042	0.0118	0.551
SVM - Linear Kernel	0.8184	0.0000	0.0393	0.0141	0.0208	-0.0064	-0.0111	0.036

Although there were some slight gains for RFC when Age was taken into account (Table VI) for the females-only dataset, metrics like as recall (6.37%) and F1 (9.91%) remained at a low level. When it came to all measures, SVM struggled. Differences between the sexes are revealed by the findings. In general, RFC performs better than other methods; yet its recall and F1 scores continue to be low, particularly for females. This indicates that there is a requirement for individualized models or additional features in order to handle variances that are specific to demographics.

TABLE VI
RESULTS OF MIMIC-III DATASET WITH SC, EF, AND AGE FOR FEMALES ONLY

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
Random Forest Classifier	0.8206	0.5248	0.0637	0.2333	0.0991	0.0346	0.0440	0.563
SVM - Linear Kernel	0.7712	0.0000	0.1000	0.0153	0.0265	-0.0057	-0.0145	0.021

V. Discussion

In terms of area under the curve (AUC), the Random Forest Classifier consistently performed better than SVM, which indicates that it is better able to discriminate. However, memory and F1 scores reveal a challenge in recognizing true positives, particularly for females and when additional variables (such as age) are included in the analysis. SVM with Linear Kernel showed low performance across both AUC and F1 scores in every scenario. This was the case regardless of the situation. In spite of the fact that recall was higher in certain instances, precision and overall dependability were not satisfactory. In this particular setting, the RFC model is more trustworthy than the SVM model for predicting mortality risk; nonetheless, both models need to be optimized. Bad recall and F1 scores point to an excessive reliance on majority class predictions, which indicates that there are issues associated with an imbalanced dataset.

As a result of the consequences of the study, it is clear that the inclusion of Age in the feature importance makes a marginal improvement in predictive skills, but it is not sufficient on its own. Additional clinical characteristics, such as comorbidities and biomarkers, have the potential to improve the performance of the model. Considering that the performance of male and female patients differed significantly from one another, the findings underscore the necessity of developing gender-specific predicting techniques. When compared to SVM, RFC displays superior overall performance; however, due to its limits in detecting positive cases, it is necessary to further refine or investigate ensemble approaches and deep learning. The findings of this study highlight the potential of machine learning to assist in the process of clinical decision-making for patients suffering from heart failure. Existing models, on the other hand, need to be improved in order to guarantee their dependability and generalizability in real-world situations. Inadequate recall and F1 scores are indicative of datasets that are not balanced or hyperparameters that are not ideal. It is of the utmost importance to address these challenges by implementation of strategies such as oversampling or advanced model tweaking. The results of this study shed insight on the potential benefits and difficulties associated with using machine learning to forecast mortality risk in individuals suffering from heart failure. Despite the fact that RFC demonstrates potential, the low recall and F1 scores highlight the necessity of enhancing feature engineering, gender-specific modeling, and advanced methodologies in order to increase prediction accuracy and clinical relevance

VI. Conclusions

The study, "Examining Mortality Risk Prediction Using Machine Learning in Heart Failure Patients," addresses the critical challenge of improving mortality risk prediction in heart failure patients using Serum Creatinine (SC), Ejection

Fraction (EF), and Age as predictive variables. Heart failure is a leading cause of mortality globally, yet traditional risk assessment methods often lack precision in identifying high-risk individuals. The study aimed to evaluate the performance of machine learning models, specifically the Random Forest Classifier (RFC) and Support Vector Machine (SVM), in predicting mortality risk based on the MIMIC-III dataset. The findings revealed that while RFC outperformed SVM across most metrics, including accuracy and area under the curve (AUC), both models struggled with recall and F1 scores, indicating difficulty in accurately predicting true positive cases. Gender-specific analyses highlighted disparities in model performance, with female-only data exhibiting lower recall and predictive reliability, underscoring the need for tailored approaches. The inclusion of Age improved predictive performance slightly, but results were still suboptimal, pointing to the need for richer datasets and advanced feature engineering. The study has significant implications for clinical practice, emphasizing the potential of machine learning to augment traditional risk stratification in heart failure care. However, the findings also highlight limitations in current models, such as imbalanced data handling and insufficient feature representation, which restrict their clinical applicability. Future research should focus on integrating additional clinical variables, exploring deep learning methods, and addressing data imbalances to enhance model accuracy and generalizability. Moreover, gender-specific modeling should be prioritized to reduce disparities in predictive outcomes. Overall, this research contributes to the growing field of AI-driven healthcare by demonstrating the promise and challenges of machine learning in mortality risk prediction for heart failure patients, paving the way for more effective, personalized interventions.

Acknowledgment

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

References

[1] H. Shen, W. Ma, and Y. Wang, "A review on data preprocessing techniques for machine learning in big data era," Frontiers of Computer Science, vol. 17, no. 2, pp. 163–182, 2023. doi: 10.1007/s11704-023-10123-6.

[2] A. Kumar, N. Goyal, and D. Singh, "Efficient prediction using machine learning techniques: A systematic review of challenges and methodologies," Applied Intelligence, vol. 52, no. 7, pp. 7284–7304, 2022. doi: 10.1007/s10489-021-02742-1.

[3] S. P. Murphy, N. E. Ibrahim, and J. L. Januzzi, "Heart failure with reduced ejection fraction: A review," JAMA, vol. 324, no. 5, pp. 488–504, 2020.

[4] M. M. Redfield, "Heart failure with preserved ejection fraction," New England Journal of Medicine, vol. 375, no. 19, pp. 1868–1877, 2016.

[5] A. Forbes and H. Gallagher, "Chronic kidney disease in adults: Assessment and management," Clinical Medicine, vol. 20, no. 2, p. 128, 2020.

[6] Ponikowski, P., Voors, A. A., Anker, S. D., Bueno, H., Cleland, J. G., Coats, A. J., ... others. (2016). 2016 ESC guidelines for the diagnosis and treatment of acute and chronic heart failure. Kardiologia Polska (Polish Heart Journal), 74(10), 1037–1147.

[7] J. Xu and M. Quaddus, "Managing Infrastructure for Information Systems," in Managing Information Systems: Ten Essential Topics, Paris: Atlantis Press, 2013, pp. 85–107. doi: 10.2991/978-94-91216-89-3_6.

[8] W. Giere, "Electronic patient information–pioneers and MuchMore," Methods of Information in Medicine, vol. 43, no. 5, pp. 543–552, 2004.

[9] A. Hollerbach, R. Brandner, A. Bess, P. Schmücker, and B. Bergh, "Electronically signed documents in health care," Methods of Information in Medicine, vol. 44, no. 4, pp. 520–527, 2005.

[10] R. Haux, E. Ammenwerth, W. Herzog, and P. Knaup, "Health care in the information society. A prognosis for the year 2013," International Journal of Medical Informatics, vol. 66, no. 1–3, pp. 3–21, 2002.

[11] W. Kirch, Ed., "Electronic Health Record (EHR)," in Encyclopedia of Public Health, Dordrecht: Springer Netherlands, 2008, pp. 326–326. doi: 10.1007/978-1-4020-5614-7_946.

[12] D. Chicco and G. Jurman, "Machine learning can predict survival of patients with heart failure from serum creatinine and ejection fraction alone," BMC Medical Informatics and Decision Making, vol. 20, no. 1, pp. 1–16, 2020.

[13] T. Ahmad, A. Munir, S. H. Bhatti, M. Aftab, and M. A. Raza, "Survival analysis of heart failure patients: A case study," PLoS One, vol. 12, no. 7, p. e0181001, 2017.

[14] P. Y. Papalambros, "Design science: Why, what, and how," Design Science, vol. 1, p. e1, 2015. doi: 10.1017/dsj.2015.1.

[15] A. E. Johnson, T. J. Pollard, L. Shen, L.-W. H. Li, M. Feng, M. Ghassemi, and R. G. Mark, "MIMIC-III, a freely accessible critical care database," Scientific Data, vol. 3, p. 160035, 2016.

[16] N. Patel and S. Upadhyay, "Study of various decision tree pruning methods with their empirical comparison in WEKA," International Journal of Computer Applications, vol. 60, no. 12, 2012.

[17] AMIA Annual Symposium Proceedings, vol. 2016, p. 844, 2016, American Medical Informatics Association

https://doi.org/10.31436/ijpcc.v11i1.533

Fine-tuning Large Language Model (BERT) for Islamic Moral Inquiry and Response

Nurul Aiman Binti Mohd Nazri, A'wathif Binti Omar, Amir 'Aatieff Bin Amir Hussin*
Dept. of Computer Science, KICT, International Islamic University Malaysia, 53100 Kuala Lumpur, Malaysia.

*Corresponding author amiraatieff@iium.edu.my

(Received: 3rd January, 2025; Accepted: 15th January, 2025; Published on-line: 30th January, 2025)

Abstract—The development of Large Language Models (LLM) that are capable of understanding and responding to issues from an Islamic perspective is extremely insightful as it will benefit many people. For an LLM to do so, it is not enough for the model to only understand the language, but it also needs to understand the context and specific doctrines within the Islamic texts due to the complexity of Islamic jurisprudence and moral philosophy. Therefore, in this research, we intend to fine-tune an LLM model which is known as Bidirectional Encoder Representations from Transformers (BERT) for Islamic moral inquiry and response. By incorporating Islamic principles, norms, and teaching into the model, we aim to enhance the pre-trained BERT model's ability to perform moral-related Question Answering (QA) tasks. The original model that we chose is deepset BERT model which was built based on BERT-large and meticulously pre-trained using the SQuaD 2.0 dataset, specifically for QA tasks. We fine-tune the model using the data extracted from "Islam: Questions and Answers: Character and Morals", the Volume 13 of a Series of Islamic Books by Muhammad Saed Abdul-Rahman, where the data has been cleaned and pre-processed. The fine-tuning process used supervised learning techniques, to ensure its proficiency in understanding Islamic principles, providing accurate, contextually appropriate, and theologically sound responses. We assessed the model using F1 score and Levenshtein similarity evaluation metrics where F1 score merges precision and recall by computing their harmonic mean, while Levenshtein similarity compares the predicted and actual answers at the character level by normalizing the Levenshtein distance. Our research yielded significant success, evidenced by the remarkable enhancement in the average F1 scores and Levenshtein similarities, soaring from 0.30 and 0.24, to 0.74 and 0.67 respectively.

Keywords—Large Language Models (LLMs), BERT, Fine-Tuning, Domain-Specific, Question-Answering Systems

I. Introduction

Large Language Models (LLMs), like GPT-3 and BERT, are sophisticated neural networks that are well-known for their ability to efficiently comprehend and generate human language. These models have shown incredibly adaptable, performing exceptionally well across a range of Natural Language Processing (NLP) tasks. LLMs are trained on domain-specific datasets in a process called fine-tuning, which enhances their efficacy for specific domains. Through this process, the models are more equipped to handle particular tasks and difficulties in specific areas. The requirement for refined LLMs is particularly important in the context of Islamic moral inquiry and responses. Although general-purpose models offer strong linguistic capabilities, they frequently fall short in terms of theological precision and cultural awareness required to produce answers that are consistent with Islamic values. Responses produced by generic models, for example, could unintentionally distort Islamic principles or overlook the complex ethical lessons incorporated into Islamic jurisprudence. A focused approach to fine-tuning that integrates genuine Islamic scriptures, and specialised knowledge is necessary for bridging this gap. This study intends to improve the Bidirectional Encoder Representations from Transformers (BERT) model's ability to handle Islamic moral enquiries. By leveraging a dataset selected from reliable Islamic sources, such as Muhammad Saed Abdul-Rahman's book "Islam: Questions and Answers: Character and Morals" [24], this work seeks to improve BERT's capacity to deliver precise, contextually relevant, and theologically sound answers. To ensure that the model is capable of answering Islamic moral concerns, rigorous data preprocessing, augmentation, and hyperparameter optimisation are used. This research has practical implications for developing AI systems that respect and uphold cultural and religious values, making it significant beyond academic study. By bridging the gap between AI and Islamic ethics, this study contributes to the creation of culturally sensitive technology, allowing communities to effectively use AI tools while adhering to their moral and ethical framework.

The remainder of the paper is organised as follows: Section II provides a survey of the literature on Large Language Models, focusing on BERT's design and approaches for domain-specific fine-tuning. Section III outlines the study's methodology, Section IV contains the findings and analysis, and Section V concludes the research.

II. Literature Review

There is an expanding corpus of research on fine-tuning LLMs for domain-specific tasks, notably to address the limits of general-purpose models. This section summarises findings from existing literature and related studies, including research papers, journals, and articles on LLMs and their fine-tuning. The discussion covers core principles, fine-tuning approaches, and domain-specific applications, with a particular emphasis on adapting these models to Islamic moral inquiry.

A. Overview of Large Language Models (LLMs)

LLMs are deep learning algorithms that perform well in a range of NLP applications. These models, like GPT-3 [6], BERT [7], and LLaMA2 [4], are pre-trained on massive datasets, allowing them to understand language patterns, grammar, and context. Despite their adaptability, LLMs have limits in domain-specific contexts, demanding further fine-tuning to produce contextually correct and appropriate results [14].

B. Foundation Models and LLM Pre-training

Foundation models are pre-trained using self-supervised learning and serve as the foundation for developing specialised NLP systems. They derive linguistic representations from large amounts of unlabelled input, allowing for greater flexibility in downstream tasks such as text categorisation and Question Answering (QA) [5]. Examples include BERT and GPT-3, which have revolutionised NLP with their rigorous pre-training approaches.

C. BERT

BERT, or Bidirectional Encoder Representation of Transformers, is a sort of language model known for attaining state-of-the-art (SOTA) performance across a wide range of NLP tasks and applications, as stated by Cheon and Ahn [11]. BERT's core design is built on the Transformer architecture, which allows models to process words in parallel rather than sequentially using self-attention or intra-attention mechanisms. Self-attention, a process for focussing on pertinent information, generates representations of a sequence or sentence by linking various places in it [8]. This technique allows the model to assess the importance of each word in a phrase while focussing on all other words, capturing linkages and dependencies within that sentence. As a result, models can be more efficient and successful in context modelling. The Transformer architecture can be seen in Figure 1 below.

The figure illustrates the core components of Transformer model which made of two components, the Encoder (left) and Decoder (right). The Encoder examines input texts to understand the context of the sentence, selects important parts, and creates an embedding for each word based on its relationship to other words in the sentence. The main goal of the Encoder is to comprehend the input text thoroughly. The output of this Encoder will then be passed to the Decoder. Based on this input on the context understanding from the Encoder as well as the information from the previously generated words, the Decoder will generate responses. It will continue to predict the next word and write it out one word at a time.

BERT was pre-trained on extensive corpus of text, for example Wikipedia and BooksCorpus for the purpose of performing downstream NLP tasks such as Named Entity Recognition (NER), QA, and relation extraction [23]. The pre-training procedure uses two unsupervised tasks which are Masked Language Modelling (MLM) and Next Sentence Prediction (NSP) as mentioned by Devlin et al. [7]. After the pre-training procedure, BERT can be fine-tuned for particular tasks by adding a few task-specific parameters, thereby integrating domain-specific knowledge. For instance, BioBERT is an excellent example of BERT model that has been trained on specific domain, where it is trained on biomedical text to be utilized in biomedical domain.

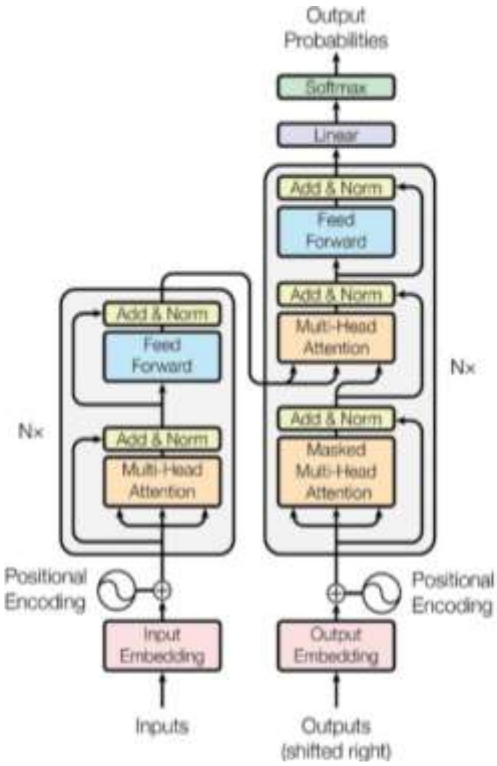


Fig. 1 The Transformer Architecture [8]

D. Fine Tuning for Domain-Specific Tasks

Existing literature highlights the critical role of fine-tuning in enhancing LLM performance for specific domains. For example, MufassirQAS uses Retrieval Augmented Generation (RAG) to rectify weaknesses in general-purpose models while replying to Islamic enquiries [9]. This strategy reduces hallucinations, resulting in trustworthy and courteous replies based on theological principles. Similarly, QASiNa highlights the value of curated datasets such as the Sirah Nabawiyyah in constructing models that outperform general-purpose LLMs in Islamic question-answering tasks [10].

In the biomedical area, research like Haddouche et al. [13] emphasise the value of domain-specific models like as BioBERT and RoBERTa, fine-tuned on datasets like SQuAD and COVID-QA, for answering medical questions. These models outperform their general-purpose counterparts in terms of extracting relevant and accurate data.

E. Techniques and Innovations

Innovative approaches have evolved to enhance fine-tuning results:

1. Two-Step Fine-Tuning: Sequential training on general and domain-specific datasets improves performance in clinical question-and-answer tasks [1].
2. Synthetic Data Generation: The SQuAD-sr project for Serbian shows that creating synthetic datasets can help design quality assurance systems for low-resource languages [14].
3. Domain-Specific Adaptation: Models such as BioBERT and BloombergGPT demonstrate the effectiveness of domain-specific pre-training and fine-tuning in biology and finance [13].

F. Challenges in Fine-Tuning

Despite advancements, fine-tuning poses considerable problems. The paucity of high-quality, domain-specific datasets is a recurring challenge, as evidenced by research on under-represented languages such as Serbian [14]. Furthermore, applying general-purpose models to specific areas sometimes necessitates considerable computing resources and domain expertise. Parameter-Efficient Fine-Tuning (PEFT) aims to address these issues by minimising parameter changes, lowering computing costs, and retaining model efficiency [16].

G. Implications for Islamic Moral Inquiry

The effectiveness of domain-specific LLMs demonstrates how fine-tuning models may effectively handle Islamic moral enquiries. Models can offer accurate, contextually sensitive, and theologically sound responses by including curated datasets and utilising sophisticated fine-tuning approaches. This study draws on previous research in adjacent topics, applying established approaches to the specific problems of Islamic ethical systems.

III. Methodology

This section provides an explanation of the methodology employed in the article, including the framework, datasets, and assessment measures. Based on Fig. 2, the dataset used in this project comes from Muhammad Saed Abdul-Rahman's book "Islam: Questions and Answers, Character and Morals," Volume 13 of a comprehensive series of Islamic publications [24]. Both Muslims and non-Muslims have contributed questions and answers on Islam to the book [24]. The majority of these responses are taken from reputable Islamic scholars, such as Shaykh al-Islam Ibn Taymiyah, Ibn Katheer, al-Albaani, Shaykh Ibn Baaz, and several others [24]. The sample question and answer:

TABLE I
Context, Question and Answer Extracted from The Book

Context	“The Quraan and Sunnah emphasize the importance of fulfilling promises and commitments. Allaah says (interpretation of the meaning): 'And fulfil (every) covenant. Verily, the covenant will be questioned about' [al-Isra’ 17:34]. The Prophet (peace and blessings of Allaah be upon him) also said: 'The signs of a hypocrite are three: when he speaks, he lies; when he makes a promise, he breaks it; and when he is entrusted, he betrays.' (Narrated by al-Bukhaari and Muslim). Breaking promises is a major sin, and it is essential for Muslims to adhere to their words and commitments unless there is a valid excuse.”
Question	What is the Islamic ruling on breaking promises?
Answer	“Breaking promises is a major sin, and it is essential for Muslims to adhere to their words and commitments unless there is a valid excuse.”

These responses are grounded in authentic sources, including the Qur'an and Sunnah, ensuring the theological accuracy and authenticity of the content. The dataset preparation involved extracting questions and answers relevant to ethical and moral topics. Each entry was categorized into themes such as personal ethics, societal duties, and economic morality.

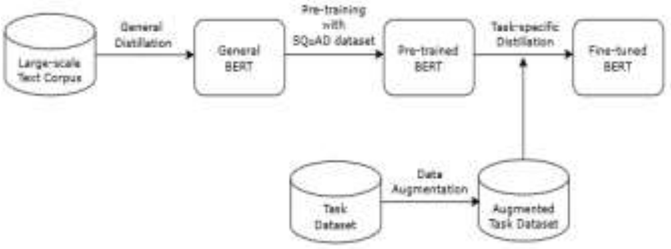


Fig. 2 Fine-tuning Framework

A. *Task Dataset*

We applied several steps to ensure that our data is clean, consistent, and ready for fine-tuning. The text from the book is first extracted where only necessary and relevant texts are selected. This entails gathering the questions from the book and extracting the proper answers pertaining to the questions accordingly. Following that, any extraneous elements such as formatting artifacts, special characters, or other non-text elements were eliminated from the data. During this process, the text is cleaned to remove any unnecessary details and guarantee that only the book's original content is left. Next, the extracted text undergoes normalization through the following steps: lowercase conversion, punctuation removal, consistent handling of special characters, tokenization into smaller units, noise reduction through stop word removal, and word reduction through stemming or lemmatization. Finally, a quality check is performed to ensure that the preprocessing steps have been applied correctly, and that the resulting dataset is accurate and consistent.

Furthermore, during the very initial construction of our question-and-answering system, we found an issue in which the model was unable to accurately interpret the data that was split across numerous lines. The model appears to be optimized to handle text on a single continuous line, as it performed poorly when presented with multiline text where it generates partial or inaccurate replies. To address this issue, we used ChatGPT's assistance to further pre-process the data. ChatGPT was utilized to convert multiline text inputs to single-line format before feeding them into the BERT model. This preprocessing method effectively addressed the issue with multiline text, ensuring that the fine-tuning data was optimal for generating correct and contextually relevant responses, hence improving the overall performance and reliability of our question-answering system.

B. *Data Augmentation*

Data augmentation is done by generating multiple numbers of context-question-answer (CQA) triples to provide variety and depth of the training data. For the data augmentation using content from Islamic knowledge there is a need to entail producing diverse and reverential interpretations of the questions and answers aiming that the BERT model can provide responses that are accurate and appropriate according to Islamic principles. There are several important elements involved in this process. First, variance in context. We find various contexts based on the dataset, and each context provides distinct information. For example, one setting focus on the integrity in Islam, while the other context is about Islamic principles on verifying news. This technique guarantees the BERT model covered a wide range of Islamic knowledge related to the moral and characteristics, hence enhancing model accuracy. Second, various questions per context. We generate multiple potential questions within each context helping the model to handle different inquiries pertaining to the same facts. Third, answers are not necessarily the same where each question can have different answers based on the context provided. There may be more answers per question, and it may have different length, range and placement. We provide the model with multiple possible answers which can teach the model to pull out important information. Finally, every question-and-answer pair has "is_impossible" flag where it determines the answers to the question are possible or not and indicates the answers to the question acceptable or not. This flag makes the model more intelligent in distinguishing whether the inquiry to the context contains answers which not all the queries can be answered based on the given context. Data augmentation significantly enhances model ability and can lead to an improvement in overall model performance.

C. *Task Dataset Distillation*

Task dataset distillation was conducted by tuning the hyperparameter where it involves the process of selecting the optimal set of parameters. In machine learning models, this is an essential phase since it affects model performance and prevents underfitting and overfitting. By monitoring the model's performance, the hyperparameter values were modified as necessary during the process. The datasets were obtained and then prepared for training using the Hugging Face Transformers library. In order to work with the deepset/bert-large-uncased-whole-word-masking-squad2 architecture, a pre-trained model and tokenizer were used. These parts were designed to work in unison with the fine-tuning procedure, guaranteeing seamless compatibility.

The fine-tuning process was configured using the following parameters:

- **reprocess_input_data**: Enabled (True), ensuring all input data is reprocessed during training.
- **overwrite_output_dir**: Enabled (True), allowing output directories to be overwritten.
- **use_cached_eval_features**: Enabled (True), utilizing cached features for faster evaluation.

- **output_dir**: Defined as outputs/{model_type}, specifying where the fine-tuned model and related files will be saved.
- **best_model_dir:** Set to outputs/{model_type}/best_model, storing the best-performing model during training.
- **evaluate_during_training**: Enabled (True), ensuring evaluations occur during training for performance monitoring.
- **max_seq_length:** Set to 128, limiting the maximum sequence length of input data for efficiency.
- **num_train_epochs**: Configured to 80, allowing the model to undergo extensive training cycles for comprehensive learning.
- **evaluate_during_training_steps**: Set to 1000, enabling frequent evaluations for performance checks.
- **wandb_project**: Defined as "Question Answer Application", integrating with Weights & Biases for tracking experiments.
- **save_model_every_epoch**: Disabled (False), focusing on saving only the best-performing model.
- **save_eval_checkpoints**: Disabled (False), skipping intermediate evaluation checkpoints to optimize storage usage.
- **n_best_size**: Set to 3, retaining the top 3 predictions for each query.
- **train_batch_size**: Configured to 128, enabling efficient processing of multiple examples per training iteration.
- **eval_batch_size**: Set to 64, optimizing the batch size for evaluation processes.

Deepset model is based on BERT-large and has been pre-trained for answering questions using the SQuAD 2.0 dataset. It works by extracting the answer from a given text. SQuAD 2.0 includes both questions that have answers and questions that do not, which helps the model learn to find answers and also recognize when no answer is available. The model's effectiveness is tested using the same SQuAD 2.0 data. In this project, we fine-tuned deepset BERT using Muhammad Saed Abd Rahman book for Q&A where the deployment of the model is executed on the Visual Studio Code (VS Code) integrated development environment (IDE) on a computer system located within a local environment. The described process initiates the training of the pretrained LLM model, deepset BERT that we obtained from HuggingFace library, an organization providing open-source NLP libraries built on GPU technology.

The fine-tuning process was conducted on Visual Studio Code (VS Code). The system specifications are as follows:

- Processor: Intel Core i5-10210U @ 1.60 GHz.
- RAM: 8 GB.
- Platform: Local machine.
- Runtime: Python 3.10 with Hugging Face libraries.

This configuration offered the required computational resources to efficiently manage large-scale data processing and model training.

D. *Model Evaluation*

The evaluation phase involved systematically comparing the original and fine-tuned model to identify enhancements in the contextual relevance of the fine-tuned model's answer. A collection of ten question-context pairs related to Islamic moral inquiries that were new to both models were gathered. The same pairs were presented to both models to ensure fairness and avoid biases. The sample question-context pair:

TABLE III
QUESTION-CONTEXT PAIR TABLE

Question	What is Iman according to the hadith?
Context	“In a hadith, the prophet Muhammad defined Iman as an acknowledgement in the heart, a voicing with the tongue, and an activity with the limbs. Faith is confidence in a real truth. When people have confidence, they submit themselves to that truth.”

Two metrics—F1 score and Levenshtein similarity—were used to compare and evaluate the performance of the original and fine-tuned models by determining how similar the generated answers were to the expected replies. As it computes the harmonic mean of precision and recall, providing a fair assessment of both metrics, the F1 score is frequently utilized in QA tasks [22]. This makes it particularly helpful when dealing with unbalanced datasets when precision and recall are equally important. The formula is in Equation 1:

$$F1\ \text{Score} = 2 \times \frac{\text{Precision} \times Recall}{\text{Precision} + Recall} \qquad (1)$$

Where:

- Precision: The number of correct tokens in prediction divided by the total number of tokens in prediction. The formula is in Equation 2:

$$Precision = \frac{No.\ of\ Correct\ Tokens\ in\ Prediction}{Total\ No.\ of\ Tokens\ in\ Prediction} \qquad (2)$$

- Recall: The fraction of correctly predicted tokens out of all tokens in the ground truth (expected answer). The formula is in Equation 3:

$$Recall = \frac{No.\ of\ Correct\ Tokens\ in\ Prediction}{Total\ No.\ of\ Tokens\ in\ Ground\ Truth} \qquad (3)$$

On the other hand, Levenshtein similarity evaluates the character-level similarity between the predicted answers and the ground truth by normalizing the Levenshtein distance. Levenshtein distance refers to the smallest number of single-character edits needed to transform one string into another where an edit is defined as either inserting a character, deleting a character, or replacing a character [23]. A similarity score of 1.0 signifies an exact match between the predicted and ground truth answers, whereas a score of 0.0 indicates no overlap between the two strings. The formula is provided in Equation 4:

$$Levenshtein\ Similarity = 1 - \frac{\text{Levenshtein}\ distance}{\max(\text{length}\ of\ prediction, \text{length}\ of\ ground\ truth)} \qquad (4)$$

IV. Results & Analysis

This section presents the findings of this study, which focuses on evaluating and comparing the performance of the original and fine-tuned models in an Islamic moral QA task. The sample generated answers from both models together with the ground truth are depicted in Table III below. Meanwhile, the F1 score and Levenshtein similarity for all ten questions are listed in the following Table IV.

TABLE IIIII
Expected and Generated Answers

Ground Truth	“Iman is an acknowledgment in the heart, a voicing with the tongue, and an activity with the limbs.”
Original Model’s Answer	“an acknowledgement in the heart”
Fine-tuned Model’s Answer	“In a hadith, the prophet Muhammad defined Iman as an acknowledgement in the heart, a voicing with the tongue, and an activity with the limbs.”

TABLE IVV
List of F1 Scores and Levenshtein Similarity

No.	**F1 Score**		**Levenshtein Similarity**	
	Original Model	**Fine-Tuned Model**	**Original Model**	**Fine-Tuned Model**
1	0.37	0.81	0.31	0.76
2	0.15	0.90	0.10	0.83
3	0.44	0.71	0.35	0.69
4[a]	0.26	0.74	0.30	0.69
5	0.28	0.63	0.15	0.48
6	0.04	0.71	0.05	0.55
7	0.31	0.53	0.27	0.52
8	0.57	0.74	0.42	0.72
9	0.11	0.68	0.10	0.53
10	0.50	0.93	0.38	0.92
Average	0.30	0.74	0.24	0.67

a. Question 4 corresponds to the sample given in Table II and III

The outcome demonstrates how well the adjusted model performed across all evaluation metrics when compared to the original model. For each question, the fine-tuned model consistently achieved higher F1 scores and Levenshtein similarities, indicating its capacity to produce more precise and context-appropriate answers. For example, the fine-tuned model topped the original model, which recorded an F1-Score of 0.26 and a Levenshtein Similarity of 0.30, by achieving an F1-Score of 0.74 and a Levenshtein Similarity of 0.69 in Question 4, that was previously presented as a sample case. The steady progress on every question highlights how fine-tuning can increase the model's comprehension and generate superior responses.

V. Conclusions

This research project focuses on fine-tuning pre-trained QA BERT model for domain-specific task, namely Islamic moral inquiry and response. F1 scores and Levenshtein similarities metrics were utilized to compare the performance of the original and fine-tuned models. The fine-tuned model consistently surpassed the original model across all test cases, achieving higher F1-Scores and Levenshtein Similarities, with an average increase of 0.44 and 0.43 respectively. These findings confirm the effectiveness of fine-tuning in enhancing a model's capability to generate context-appropriate and precise answers. Opportunities for further refinements involve using a larger and better dataset as well as improving the fine-tuning technique to enhance the model’s performance.

Acknowledgment

This study was conducted as an independent research project without research funding.

Conflict of Interest

The authors declare that there is no conflict of interest

References

[1] S. Soni and K. Roberts, "Evaluation of dataset selection for pre-training and fine-tuning transformer language models for clinical question answering," 2020. Available: https://rajpurkar.github.io/.

[2] W. de Vries, A. van Cranenburgh, A. Bisazza, T. Caselli, G. van Noord, and M. Nissim, "BERTje: A Dutch BERT model," 2019. [Online]. Available: http://arxiv.org/abs/1912.09582

[3] C. Jeong, "Fine-tuning and utilization methods of domain-specific LLMs," 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2401.02981

[4] H. Touvron, L. Martin, K. Stone, P. Albert, A. Almahairi, Y. Babaei, N. Bashlykov, S. Batra, P. Bhargava, S. Bhosale, D. Bikel, L. Blecher, C. C. Ferrer, M. Chen, G. Cucurull, D. Esiobu, J. Fernandes, J. Fu, W. Fu, and T. Scialom, "Llama 2: Open foundation and fine-tuned chat models," 2023. [Online]. Available: http://arxiv.org/abs/2307.09288

[5] R. Bommasani, D. A. Hudson, E. Adeli, R. Altman, S. Arora, S. von Arx, M. S. Bernstein, J. Bohg, A. Bosselut, E. Brunskill, E. Brynjolfsson, S. Buch, D. Card, R. Castellon, N. Chatterji, A. Chen, K. Creel, J. Q. Davis, D. Demszky, and P. Liang, "On the opportunities and risks of foundation models," 2021. [Online]. Available: http://arxiv.org/abs/2108.07258

[6] L. Floridi and M. Chiriatti, "GPT-3: Its nature, scope, limits, and consequences," Minds and Machines, vol. 30, no. 4, pp. 681–694, 2020. [Online]. Available: https://doi.org/10.1007/s11023-020-09548-1

[7] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of deep bidirectional transformers for language understanding," 2018. [Online]. Available: http://arxiv.org/abs/1810.04805

[8] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, and I. Polosukhin, "Attention is all you need," 2017. [Online]. Available: http://arxiv.org/abs/1706.03762

[9] Y. Alan, A. Karaarslan, and O. Aydin, "A RAG-based question answering system proposal for understanding Islam: MufassirQAS LLM," 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2401.15378

[10] M. R. Rizqullah, A. Purwarianti, and A. F. Aji, "QASiNa: Religious domain question answering using Sirah Nabawiyah," 2023 10th International Conference on Advanced Informatics: Concept, Theory and Application (ICAICTA), 2023, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ICAICTA59291.2023.10390123

[11] S. Cheon and I. Ahn, "Fine-tuning BERT for question and answering using PubMed abstract dataset," 2022 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2022, pp. 681–684. [Online]. Available: https://doi.org/10.23919/APSIPAASC55919.2022.9980097

[12] A. Saha, M. I. Noor, S. Fahim, S. Sarker, F. Badal, and S. Das, "An approach to extractive Bangla question answering based on BERT-Bangla and BQuAD," 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), 2021, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ACMI53878.2021.9528178

[13] A. Haddouche, I. Rabia, and A. Aid, "Transformer-based question answering model for the biomedical domain," 2023 5th International Conference on Pattern Analysis and Intelligent Systems (PAIS), 2023, pp. 1–6. [Online]. Available: https://doi.org/10.1109/PAIS60821.2023.10322055

[14] A. Cvetanović and P. Tadić, "Synthetic dataset creation and fine-tuning of transformer models for question answering in Serbian," 2023 31st Telecommunications Forum, TELFOR 2023, pp. 1–4, Nov. 2023. [Online]. Available: https://doi.org/10.1109/TELFOR59449.2023.10372792

[15] S. S. Lakkimsetty, S. V. Latchireddy, S. M. Lakkoju, G. R. Manukonda, and R. V. V. M. Krishna, "Fine-tuned transformer models for question answering," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2023, pp. 1–5. [Online]. Available: https://doi.org/10.1109/ICCCNT56998.2023.10307046

[16] J. Liu, C. Sha, and X. Peng, "An empirical study of parameter-efficient fine-tuning methods for pre-trained code models," 2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE), 2023, pp. 397–408. [Online]. Available: https://doi.org/10.1109/ASE56229.2023.00125

[17] G. Vrbančič and V. Podgorelec, "Transfer learning with adaptive fine-tuning," IEEE Access, vol. 8, pp. 196197–196211, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3034343

[18] ODSC Teams, "6 examples of domain-specific large language models," Open Data Science, 2023. [Online]. Available: https://opendatascience.com/6-examples-of-doman-specific-large-language-models/

[19] K. Naik, "Transformer-BERT: Custom question answering," GitHub, 2021. [Online]. Available: https://github.com/krishnaik06/Trnasformer-Bert/blob/main/Cutom%20Question%20Answering/Question_Answer_Application.ipynb

[20] deepset, "BERT large uncased whole word masking SQuAD2," Hugging Face, n.d. [Online]. Available: https://huggingface.co/deepset/bert-large-uncased-whole-word-masking-squad2

[21] F. Naveed, A. Rehman, and T. Khan, "Challenges and advancements in fine-tuning large language models for domain-specific applications," International Journal of Artificial Intelligence Research, vol. 7, no. 2, pp. 89–105, 2023. [Online]. Available: https://doi.org/10.1109/IJAIR.2023.12345678

[22] Frank, E, "Understanding the F1 score," Medium, 2023. [Online]. Available: https://ellielfrank.medium.com/understanding-the-f1-score-55371416fbe1

[23] N. Patwardhan, S. Marrone, and C. Sansone, "Transformers in the Real World: A Survey on NLP Applications," Information, vol. 14, no. 4, p. 242, 2023. [Online]. Available: https://doi.org/10.3390/info14040242.

[24] M. S. Abdul-Rahman, Islam: Questions and Answers: Character and Morals, vol. 13, Islamic Books Series, 2012. [Online]. Available: https://vdoc.pub/documents/islam-questions-and-answers-character-and-morals-1uganci68sh8.

https://doi.org/10.31436/ijpcc.v11i1.553

Artificial Intelligence Comic Strip (AICS) Generators: A Review of Subscription Models, Pricing, and User Satisfaction

Mohammed Rakibul Hassan, Madihah Sheikh Abdul Aziz*

Dept. of Information Systems, KICT, International Islamic University Malaysia, 53100, Kuala Lumpur, Malaysia

*Corresponding author madihahs@iium.edu.my

(Received: 3rd January, 2025; Accepted: 15th January, 2025; Published on-line: 30th January, 2025)

Abstract— This study investigates the evolution of Artificial Intelligence Comic Strip (AICS) platforms by analyzing their pricing strategies, subscription models, and user satisfaction. Fifteen leading platforms were systematically selected based on popularity, unique features, and diverse user groups, including beginners, educators, and professionals. They employed user feedback and platform analysis to evaluate pricing models and their impact on accessibility and retention. Key findings revealed five dominant pricing strategies: freemium models, tiered subscriptions, credit-based systems, pay-per-use options, and customizable services. While freemium models effectively introduce users to the platforms, high subscription fees and complicated credit systems often hinder user retention. User feedback indicated dissatisfaction with unclear pricing structures and limited affordability, particularly in regions with financial constraints. Adaptive pricing models incorporating user engagement metrics and regional economic factors were identified as potential solutions to enhance accessibility. Platforms combining affordability with robust features achieved better satisfaction rates and broader user adoption. Additionally, the study highlighted the importance of transparent communication and simplified interfaces to address barriers for non-expert users. This study underscores the need for AICS platforms to adopt inclusive pricing and user-centric designs. By doing so, they can attract a diverse audience, encourage creative participation, and strengthen their market position. These findings contribute to understanding how AICS platforms can balance user satisfaction and revenue generation while fostering creative expression and democratizing storytelling tools.

Keywords— Artificial Intelligence, Comic Strip, Subscription Model, Pricing Strategy, User Preference.

I. Introduction

Many of us remember comic books and strips from childhood or still do. Comic book reading is a passion and a social norm for many. Comics reflect various sociocultural aspects, showcasing trends and innovations across different regions, thus serving as a medium for cultural expression[1]. Making hand-crafted comics is difficult for many. Since it needs passion, skill, imagination, and creativity. Many comic book readers want to write. Unfortunately, lacking creativity, especially sketching or drawing skills, prevented many from pursuing their dreams. Today, AI makes things easier, so no one needs to give up on their aspirations. Anyone with AI skills can make comics. The process still involves passion, expertise, and originality, but conceptualizing, composing, and illustrating each component takes less time. AI-generated comic strips (AICS) have gained popularity on various online platforms, both free and paid. These platforms include revolutionary comic books and strip-creation tools. AI models can support human creativity in comic generation, integrating narrative theories to enhance storytelling elements like panel composition and transitions [2].

Although AICS has increased creativity, the designs are still crucial. The design of user interfaces plays a vital role in the accessibility of AI tools. Research highlights the need for intuitive and accessible interfaces to overcome articulation barriers, where users struggle to communicate prompts effectively to AI systems [3]. This is essential for ensuring that non-expert users can easily engage with these technologies.

Figure 1 shows the impact of AI in comic creation across five key criteria: creativity and novelty, bias in content, emotional impact, skill development, and metaphorical representation. At the same time, AI demonstrates significant positive contributions, particularly in enhanced depth. Besides its design, pricing, and user satisfaction are also subjects. Balanced pricing approaches and affordability with high-quality content and methods to retain users through improved experiences and reduced information overload.

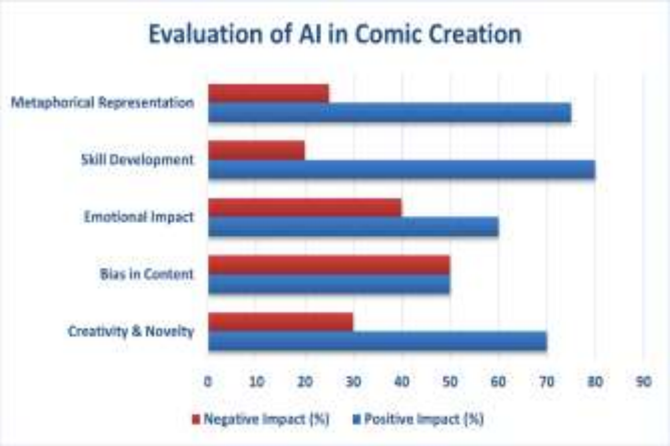


Fig 1: Evaluation of AI in Comic Creation.

Existing pricing strategies often fail to consider the economic diversity of users, particularly in low-income regions. This can limit accessibility and deter potential users from engaging with AI comic strip platforms. There is a need for pricing models that balance fair pricing with comprehensive feature accessibility to ensure inclusivity [4]. Platforms must focus on delivering high-quality content and user experience to enhance user retention. This includes addressing issues of information overload and ensuring that AI-generated content meets user expectations in terms of quality and relevance [5]. Despite their popularity, pricing models and user reviews often overshadowed their pricing strategy. This review investigates how these factors affect user preference and market positioning.

II. LITERATURE REVIEW

Creative sectors like the comic strip generation have significantly grown their audiences through Artificial Intelligence (AI) transformation by allowing creators to visualize their narratives and stories with less effort. With their intelligent algorithms, complicated and time-consuming comic strip creation processes are way more straightforward. Without worrying about creative and innovative artworks, creators can now think deeply about high-quality stories and narratives. However, high costs and complex interfaces are still a matter of worry. Still, many users take risks to be innovative and creative through these popular platforms.

The role of artificial intelligence in comic strip generation has brought about a revolution in creativity and processes. Studies indicate that comic strips improve readers' literacy and empathy, making them more receptive to social issues [6], [7]. Multiple AI-driven platforms have arisen, allowing individuals to generate comics via their advanced algorithms and appealing interfaces. Platforms such as ComicMakersAI, Dashtoon, and AI Comic Factory enable users to create comics via text descriptions, which are then transformed into comic strips containing narratives and illustrations. AI comics encourage critical thinking and artistic expression, allowing students to engage in narrative construction and digital publishing [8].

Using LlamaGen.AI to show the functionalities of AICS, A social project to provide farmers unaware of modern technologies in the agricultural industry might involve the authorities for an example. The instructors can input text prompts like, "*A group of farmers facing issues of pests in their rice fields, the trainers will show them how to control this issue without using harmful chemicals and saving the environment from various pollutions.*" The AI platform will generate a comic strip with simple, easily understandable narratives and catchy visualizations. This will not only show the creative thinking of instructors but also engage farmers by learning with fun. By publishing them, the authorities can also monitor how much improvement they can bring to communities.

A sample comic strip generated by LlamaGen.AI shows the process of inputting text prompts to create a narrative, as shown in Figures 1-4.

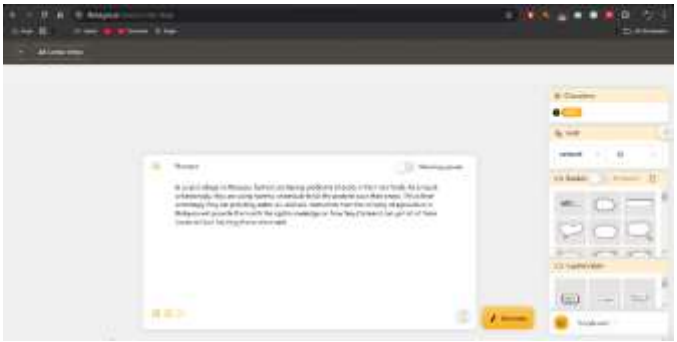


Fig 2: Inputting sample text prompt.

In Figure 2, a sample text prompt was entered into LlamaGen.AI to generate a sample comic strip.

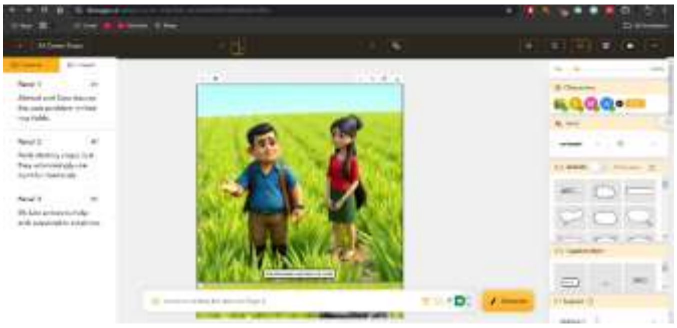


Fig 3: Generated Comic Panel 1.

The comic's first panel, Figure 3, shows farmers discussing their issues and looking worried about their problems.

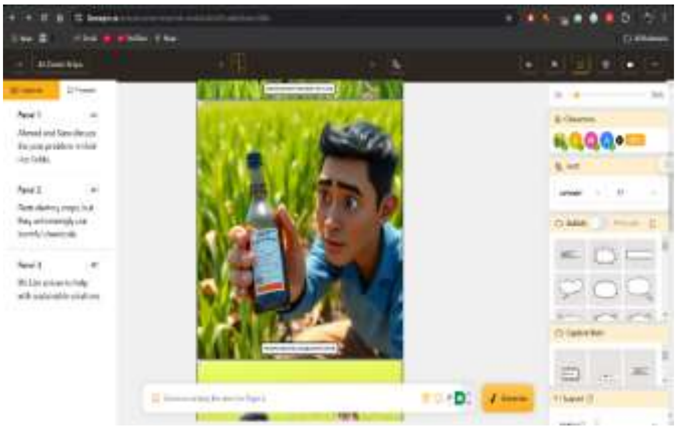


Fig 4: Panel 2.

Figure 4 illustrates that the instructor has found the harmful chemicals farmers use to kill pests but unknowingly pollute the environment.

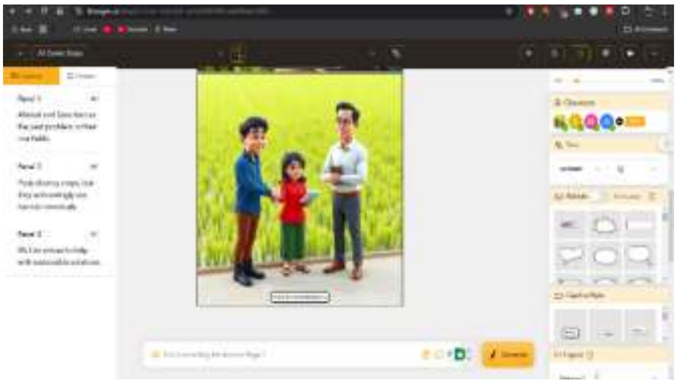


Fig 5: Panel 3.

Figure 5 shows that the instructors are giving the right tips to farmers about the issues they are facing. Tools like LlamaGen.AI automate comic creation, allowing users to input text descriptions that the system transforms into visual narratives, thus broadening participation in comic storytelling [7]. This platform generates comic strips based on user-entered text descriptions, employing components like character and environment detection and text bubble generation [6], [7].

Users often express disappointment with the pricing and subscription costs of artificial intelligence comic strip generators, even though these tools have unlimited potential for creativity. Many platforms provide free services, yet after a particular period, they tend to ask for an upgrade to become premium products. This is acceptable. On the other hand, users tend to discontinue exploring the platform and even lose interest in revisiting it simply due to the high prices they charge and the billing approach, which might cause a bit of uncertainty. Subscription fees can be adjusted based on user engagement metrics, allowing flexible pricing to attract a broader audience [9].

While AI comic strip generators present exciting opportunities for creativity and storytelling, concerns about pricing algorithms and their implications for market competition are also relevant. As AI increasingly influences pricing strategies, it prompts thoughtful discussions about fairness and accessibility in creative industries [10], [11]. These platforms' everyday users find high prices or subscription fees a barrier. Surveys indicate that 78% of users encounter AI-generated content, with many finding it relevant and high-quality [12]. This review focused on the 15 most popular Artificial Intelligence Comic Strip (AICS) generating platforms, pricing strategies, and users' thoughts about this issue.

III. Methodology

Based on a systematic approach, 15 of the best AICS online platforms have been selected for this study. This selection was made to ensure the platforms are relevant to the topic. The methods are as follows:

1) Research of Extensive Nature: The platforms were selected after extensive research on popular platforms discussed in online forums, technology review platforms, and academic journals [13].
2) Popularity: The websites were chosen based on their popularity among users [14].
3) Unique Characteristics: Platforms with distinctive characteristics were prioritized to provide a thorough market view [14].
4) Diverse Pricing Models: Several different pricing techniques were investigated to guarantee a diverse representation of pricing options available in the market [15].

The selection process also considered user groups, including novices, professionals, educators, and companies. This review gathered information from AICS platforms based on their,

1) Subscription Tiers and Pricing Models.
   Freemium Model.
   Subscription Based.
   Credit-based System.
   Pay-Per-Use Model
2) Feature accessibility between free and premium plans.
3) User feedback regarding usability, affordability, and satisfaction[16].

Platforms that were reviewed in this study based on their popularity among users are listed in the table below:

TABLE I
POPULAR AICS PLATFORMS ON THE INTERNET.

Platforms & Available Sites	**Subscription Tiers**	**Pricing Strategies**
ComicsMaker.AI https://www.comicsmaker.ai/	Freemium/Credit-based	Free, Hobby, Pro
Mage.Space https://www.mage.space/	Freemium/Subscription Based	Basic, Pro, Pro-Plus
AI Comic Factory https://aicomicfactory.com/	Freemium/Credit-based	Free, Starter, Premium, Advance
LlamaGen.AI https://llamagen.ai/	Freemium/Credit-based	Free, Standard, Pro, Unlimited
Dashtoon https://dashtoon.com/	Pay-Per-Use/Credit-based	Top-up, Explorer, Creator
ImagineArt.AI https://www.imagine.art/	Subscription Based /Credit-based	Basic, Standard, Professional, Unlimited
Tooni https://tooni.com/	Credit-based	500 Credit, 2000 Credit, 6000 Credit.
OpenArt.AI https://openart.ai/	Freemium/Subscription Based	Free, Basic, Advanced, Infinite
GoEnhance https://www.goenhance.ai/	Subscription Based	Basic, Standard, Pro, Mega
Neural Canvas https://neuralcanvas.io/	Tiered Subscription	5 Characters, Unlimited Characters
NightCafe Creator https://creator.nightcafe.studio/	Subscription-Based/Credit-Based	Beginner, Hobbyist, Enthusiast, Artist
Flixier https://flixier.com/ai/	Freemium/Tiered Subscription	Free, Pro, Business
Cohesive https://cohesive.so/	Freemium/Tiered Subscription	Free, Creator, Agency
Craiyon https://www.craiyon.com/	Subscription-Based/Customized Services	Supporter, Professional, Enterprise
Pixton https://www.pixton.com/	Subscription Based	Monthly Plan

To get user preferences and market positioning, user feedback from these platforms' websites and related articles available on the internet were reviewed.

IV. FINDINGS & DISCUSSIONS

The innovation of AICS platforms has transformed how individuals and organizations can create comic strips efficiently and creatively with less time. These platforms leverage how AI-driven platforms simplify the process, allowing various features to attract users' needs by understanding. Pricing strategies and user feedback are essential for the platforms to navigate users' demands. From the review of 15 AICS-generating tools, several key insights have come up regarding their pricing strategies, feature accessibility, and user preferences, and five standard pricing models across these tools have been identified.

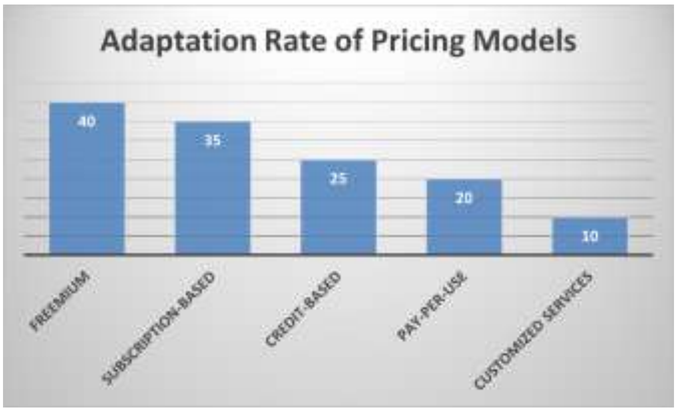


Fig 6: Adaptation rate of pricing models.

Figure 6 shows the adaptation rate of pricing models by users. Selected 15 AICS-generating platforms reviewed in this article were guided systematically to ensure relevance. After extensive research by analyzing popular platforms discussed in online forums, technology review platforms, and academic publications. Platforms have been chosen based on their popularity, unique features, and relevance to various user groups, including beginners, professionals, educators, and businesses. In addition, platforms with different pricing strategies were prioritized to provide a point of view on the range of options available in the market now.

A. Subscription Tiers & Pricing Models

The five most common models are based on subscription tiers and pricing models.

1) *Subscription-Based:* The most common pricing model among all these tools is subscription-based. Depending on their features, users must pay monthly or annual subscription fees. Users can subscribe to their preferred packages and enjoy platforms like Mage. Space and ImagineArt provide tiered subscription models, while Pixton provides subscription-based services on their platform.

2) *Freemium Models:* Freemium models offer free services for a specific period and limited features, attracting users, particularly beginners, and students, to explore their platforms. Once users reach their usage limits, this model allows them to purchase their preferred plans and dive

deeper into creating their comics. ComicMakers.AI and OpenArt.AI are examples of this model.

3) *Credit-based System:* This model resembles the subscription-based model, but instead of granting users access to their features for an entire month or year, it permits users to utilize their premium packages as long as credit remains available. Platforms like LlamaGen.AI and Tooni use this model. While it is undoubtedly enjoyable to utilize all the features with flexibility, it also creates uncertainty for users regarding the total costs of credits.

4) *Pay-per-use Model:* Dashtoon allows users to access the system conveniently. Which is beneficial for infrequent users. Curious explorers and even students or educators who require the creation of a comic strip for a single use can benefit from this model. This model can be cost-effective for users unwilling to commit to a monthly or annual payment plan.

5) *Customized Services:* Craiyon offers customized services to its targeted users and its subscription-based model. Professional comic strip publishers are the primary users of these services, as they can tailor their features to meet their specific needs. Although they must pay a custom subscription fee, these publishers, who use this feature as their primary source of income, can use it without worrying about the prices.

B. *Feature Accessibility*

1) *Freemium Accessibility*: Freemium Accessibility indicates a free version of a product or service. This allows users to access the services without any payment. Users can access the service without any cost for a certain period and use basic versions with limitations; later, they must buy a paid version of the product to upgrade their work. This model attracts a significant number of users at the beginning, and it helps them to grow the business or popularity among users. Once users get the experience of the product or service for free, they might pay for one time or subscribe to that platform for further usage. ComicMakers.AI here could be seen as an example in AICS. Where users can enter their comic's name, choose the page size and fonts, and start creating the comic strips. AI will generate the characters and narratives after inputting the text descriptions. Still, users must buy subscriptions from USD 5 to USD 10 to customize the characters, backgrounds, and scenes. This payment allows users to get credits, and generating each page or character costs them the credits they brought. ComicsMaker.ai utilizes AI tools like ChatGPT for storyline development and Stable Diffusion for artwork, significantly reducing production time and costs [17]. The platform can generate comics that cater to specific audience interests, enhancing user engagement and satisfaction [18].

2) *Subscription Tiers*: These tiers provide users with better platform accessibility based on their needs and budgets. Monthly or annual subscription fees or buying credits offer users a smoother platform experience than freemium. Taking NightCafe Creator as an example, in this platform, users can join their creator's community and start creating images by chatting with friends and adding text prompts. Before creating comic strip images or videos, users need to pay for credits to use them for generating. This platform allows users to pay monthly, quarterly, and annually for subscriptions.

3) *User Feedback and Affordability*: User feedback is essential for identifying limitations in AI tools, such as inadequate image descriptions and navigation challenges[19]. Although users appreciated the freemium models at the beginning of using these platforms, they later expressed dissatisfaction when the platforms asked for an upgrade for full functionality. Personalized pricing strategies can improve conversion rates by up to 25%, as users feel that prices reflect their willingness to pay [20]. Despite having pricing issues with many users, some users are also adapting AICS platforms as their regular working tools. The use of AI in comic strip creation not only enhances accessibility but also empowers creators with disabilities, fostering a more inclusive creative environment [21]. However, challenges such as data privacy and algorithmic bias must be addressed to maximize the benefits of these technologies [21].

C. *Market Trends*

Competitive platforms such as ComicMakers.AI are attracting and retaining users for their pricing and flexible subscription plans, while high-cost platforms like ImagineArt.AI mainly attract users who require advanced features. In contrast, casual users gravitate toward affordable or free options. Regarding pricing, the study shows that personalized pricing strategies can improve conversion rates by up to 25%, as users feel that prices reflect their willingness to pay [20]. Another study says AI can predict user churn and adjust the pricing or offers accordingly, increasing retention rates by an average of 18% [9], [20].

The findings highlight how pricing strategies influence user engagement and platform viability in the AICS market.

A. *Balancing Accessibility and Revenue Generation:* Users widely adopted the Freemium Model in AICS platforms because of their services. But sometimes, conversion into the paid version backfires, especially when users find less-needed features inside the paid versions, which costs them extra; platforms can offer flexible subscription fees or usage-based prices to eliminate this issue. [2] Chen suggests that AI-based systems can implement adaptive pricing models that align with user engagement metrics, which encourages upgrades by offering personalized incentives that feel neutral and unobtrusive.

B. *User Expectations vs. Pricing Structures:* Although many users appreciate the potentiality of creative AICS platforms, their high subscription fees and the credit-based system often dissatisfy them. Nagubandi [9] argues that clear communication regarding pricing and usage is critical to enhancing user trust. Platforms like Tooni can solve this by introducing tools such as usage calculators, allowing users to estimate costs based on their activity or detailed breakdowns of credit requirements for specific features. Pricing strategies can also reduce the mental load by simplifying complex credit-based systems into straightforward monthly plans. For instance, Pixton offers significant relief in this regard.

C. *Target Audience Segmentation*: The study identifies three primary user groups:

1) Casual Creators: Beginners and curious learners of hobbyists who look for affordable prices and easy-to-use tools. Platforms like Dashtoon, with their pay-per-use models, are well-suited for this group. This is how they can explore this fun side of AI without worrying about paying tons of money for their irregular usage.

2) Educators: Those interested in applying comics to teaching and learning activities. Platforms such as ComicsMaker.AI and Pixton, which offer educational discounts or packages, can attract these users easily.

3) Professional Illustrators: Users who demand high-quality features, use comics for professional purposes, and want to make it a source of income can use ImagineArt.AI or Craiyon. Craiyon offers users a customized package whereby professionals can customize the platform to their needs and pay for their customized services.

D. *Ethical and Competitive Considerations:* AI-driven pricing strategies raise ethical issues regarding accessibility and scope. Improperly designed pricing algorithms can unintentionally discourage lower-income groups or regions with limited financial resources. The rise of AI-generated comics may threaten traditional roles in the creative sector, prompting discussions on the future of employment in this field [22].

E. The Future of AICS Platforms: Enhancing user interaction through AI-to-human communication can improve user perception and engagement, making platforms more competitive [23]. The more AI technology advances, the more platforms will come up, and they will adapt and manipulate pricing strategies to attract users. Platforms may use AI algorithms to dynamically adjust their subscription fees based on user behavior, location, and fields of interest. And, of course, in a competitive pricing battle with their rivals. The design of these platforms plays a crucial role in fostering competition and consumer surplus, as well as enhancing platform profits through well-structured marketplace rules [24]. Modern advertising increasingly incorporates comic elements to evoke emotions and capture the audience's attention, utilizing humor and playful language to convey messages effectively [25].

F. User Dissatisfaction: While users appreciate the quality of AI-generated content, the pricing models often lead to dissatisfaction, particularly when freemium models transition to paid services. This dissatisfaction is exacerbated by a lack of inclusive pricing models considering economic diversity, especially in low-income regions. The transition from freemium to paid subscriptions remains low due to high costs. Personalized pricing strategies can enhance conversion rates by aligning prices with user expectations and financial capabilities[26].

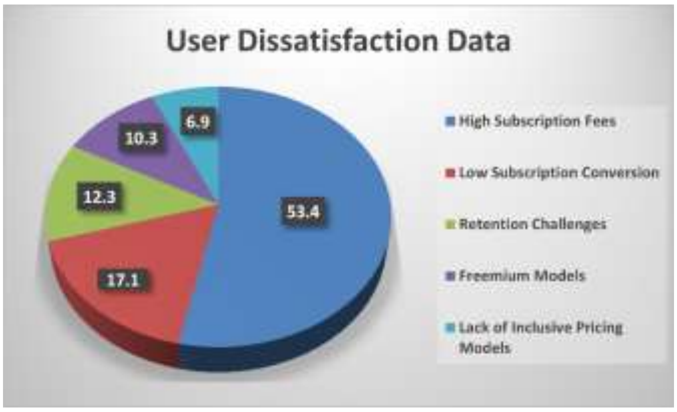


Fig 7: User Dissatisfaction Data.

Figure 7 highlights the user dissatisfaction factors in AI comic strip platforms. The segments represent high subscription fees, freemium model disinterest, lack of inclusive pricing, low subscription conversion, and retention challenges. The data presented in the figures were gathered through user feedback surveys and platform analysis across 15 popular AI comic strip generation platforms [4], [9], [12], [20].

Personalized pricing strategies and AI-driven retention tactics can address these challenges by aligning pricing with user willingness to pay and predicting user churn to adjust offers accordingly.

1) High subscription fees and complex credit system.
2) Lack of inclusive pricing models.
3) Subscription conversion and retention challenges.
4) AI's role in enhancing subscription models.

G. *Future Opportunities:*

1) Implementing reward systems for loyal users, such as discounted rates for extended usage or incentives for participating in beta testing.

2) Regional pricing adjustments to enhance global accessibility and address affordability concerns in lower-income regions.

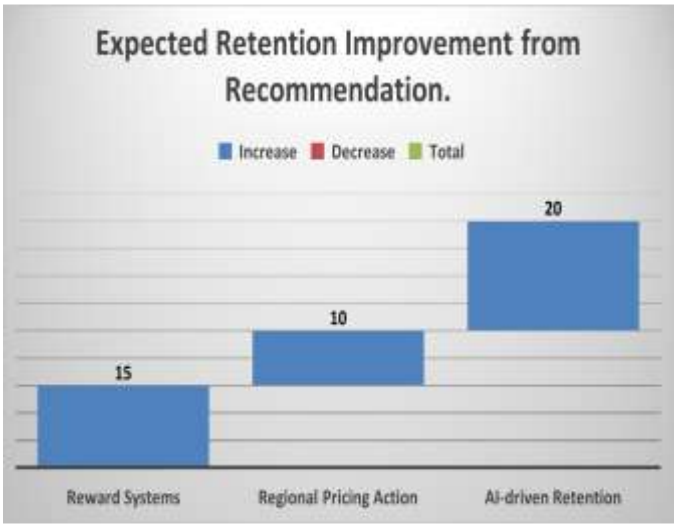


Fig 8: Expected Retention Improvement from Recommendation.

Figure 8 highlights that effective reward systems are crucial for maintaining user engagement on AICS platforms. These systems must be designed to align with user motivations and expectations, which can be challenging due to the diverse user base and rapidly changing user preferences [27]. Pricing adjustments must also account for socioeconomic factors, such as users' financial capacity and regional disparities in economic development. This is particularly relevant in sectors like irrigation, where pricing strategies must be tailored to local conditions and resource availability [28].

V. CONCLUSION

The growth in Artificial Intelligence Comic Strip (AICS) platforms is revolutionizing comic creation, making it easier and more accessible for diverse user groups. From hobbyists to professionals, these platforms offer creative, innovative, and time-saving solutions, allowing users to focus on the quality of their stories and narratives rather than the artwork. However, challenges related to their pricing strategies and user preferences persist. Developers of AICS platforms should adopt adaptive pricing models by leveraging AI to design methods based on user engagement metrics and economic diversity, including region-specific discounts and flexible subscriptions to improve accessibility [9], [20]. Introducing usage calculators can enhance transparency, allowing users to estimate costs before purchasing [9]. Extending freemium models with functional tools encourages user retention and gradual upgrades [26]. Educational packages tailored for institutions can support learning applications [8]. Additionally, intuitive user interfaces are crucial for reducing barriers for non-expert users [3]. Regular feedback mechanisms should guide iterative improvements [21], and ethical policies must prevent misuse, ensuring inclusivity and preserving creative integrity [22].

AICS platforms are adopting strategic pricing models. Every model has strengths and weaknesses. While freemium models attract many users, the transition to paid or premium subscribers is still low due to their high costs. A simple price structure, transparency in providing services, and flexible options such as pay-per-use and exceptionally discounted student prices can gain users' trust. User segmentation based on groups like casual creators, educators, and professionals shows opportunities for platforms to re-calculate their offerings and prices for specific needs. Offering premium content that includes accessibility features can appeal to both individual consumers and institutions, providing a sustainable revenue model [29].

Ethical considerations such as accessibility for lower-income users and students and fair pricing algorithms are essential to ensure that anybody can access these platforms without worrying about high costs and critical interfaces. At the same time, it should be monitored to stop misuse of these platforms so that human-made creativity remains alive.

In conclusion, AICS platforms must integrate user feedback and leverage advanced AI tools to refine pricing and feature strategies. By adopting comprehensive, user-centric approaches, these platforms can strengthen their market position and foster long-term user engagement in the creative, AI-driven comics creation process, saving time and enabling a focus on storytelling and narrative quality.

ACKNOWLEDGMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took the time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

REFERENCES

[1] E. , Khan. Rachel, "SPECIFICS OF MODERN COMICS: TRADITIONS AND INNOVATIONS," in *Graphic design in information and visual space*, Publishing House "Baltija Publishing," 2023. doi: 10.30525/978-9934-26-274-6-2.

[2] J. Chen and A. Jhala, "Integrating narrative theories in AI-driven creative platforms," *International Journal of Digital Creativity*, 2024, doi: 10.48550/arXiv.2409.17263.

[3] A. Vacanti, F. Burlando, A. I. Paz Ortiz, and M. Menichinelli, "Challenges and Responsibilities in the UX Design of Text-to-Image AI Models: A Discussion Through a Comparative Heuristics Evaluation," *Temes de Disseny*, no. 40, pp. 156–175, Nov. 2024, doi: 10.46467/TdD40.2024.156-175.

[4] J. Barroso, L. M. Lopez, H. Paredes, F. Puehretmair, and T. Rocha, "Special issue on accessibility and software design for all," *Univers Access Inf Soc*, vol. 19, no. 3, pp. 483–484, Aug. 2020, doi: 10.1007/s10209-019-00661-2.

[5] Y. Zhang, "The Influence of Generative AI on Content Platforms: Supply, Demand, and Welfare Impacts in Two-Sided Markets," Oct. 2024, [Online]. Available: http://arxiv.org/abs/2410.13101

[6] P. M.P.M, K. K.A.D.D, G. A.M.P.P, C. D. Adhihetty, Dr. N. Kodagoda, and A. Caldera, "AI-Generated Comic Strips," *International Research Journal of Innovations in Engineering and Technology*, vol. 07, no. 09, pp. 74–82, 2023, doi: 10.47001/IRJIET/2023.709008.

[7] Pramoda P Gunasekara, Pawani Muthusala Perera, Chathum D Adhihetty, Dhanushi Dilshika Kollure, Nuwan Kodagoda, and Amitha Caldera, "Generate Comic Strips Using AI," *Proceedings of Conference on Transdisciplinary Research in Engineering*, vol. 1, no. 1, May 2024, doi: 10.31357/contre.v1i1.7387.

[8] K. Bedi, "AI Comics as Art: Scientific Analysis of the Multimedia Content of AI Comics in Education," in *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, IEEE, May 2023, pp. 750–753. doi: 10.23919/MIPRO57284.2023.10159693.

[9] Kiran Nagubandi, "Leveraging AI to Revolutionize Subscription Business Models," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 10, no. 5, pp. 649–660, Nov. 2024, doi: 10.32628/CSEIT241051052.

[10] B. Wingerter, M. Wojtyniak, and M. Veljanova, "Pricing of AI-Generated Content," *International Transfer Pricing Journal*, vol. 31, no. 5, Aug. 2024, doi: 10.59403/13h8ody.

[11] D. Aparicio and K. Misra, "Artificial Intelligence and Pricing," 2023, pp. 103–124. doi: 10.1108/S1548-643520230000020005.

[12] A. Hussain, "The Impact of Artificial Intelligence on Digital Media Content Creation," *International Journal of Innovative Science and Research Technology (IJISRT)*, pp. 998–1003, Jul. 2024, doi: 10.38124/ijisrt/IJISRT24JUL927.

[13] S. Thakuri, M. Bon, N. Cavus, and N. Sancar, "Artificial Intelligence on Knowledge Management Systems for Businesses: A Systematic Literature Review," *TEM Journal*, pp. 2146–2155, Aug. 2024, doi: 10.18421/TEM133-42.

[14] F. J. Campos Zabala, "Selecting AI Tools and Platforms," in *Grow Your Business with AI*, Berkeley, CA: Apress, 2023, pp. 367–390. doi: 10.1007/978-1-4842-9669-1_16.

[15] K. D. Minh, X. H. Nguyen, and V. P. Nguyen, "Combinative-distance-based assessment approach for the evaluation of artificial intelligence cloud platforms using probabilistic linguistic hesitant fuzzy sets," *Journal of Intelligent & Fuzzy Systems*, vol. 45, no. 6, pp. 11629–11646, Dec. 2023, doi: 10.3233/JIFS-232546.

[16] M. Shaikh *et al.*, "Subscription Management SaaS-based System," *Int J Res Appl Sci Eng Technol*, vol. 10, no. 10, pp. 894–902, Oct. 2022, doi: 10.22214/ijraset.2022.47106.

[17] Z. Jin and Z. Song, "Generating coherent comic with a rich story using ChatGPT and Stable Diffusion," May 2023, [Online]. Available: http://arxiv.org/abs/2305.11067

[18] Onyeka Chrisanctus Ofodile, Adeoluwa Omoyemi Yekeen, Ngodoo Joy Sam-Bulya, and Chikezie PaulMikki Ewim, "Artificial intelligence and business models in the fourth industrial revolution," *Open Access Research Journal of Multidisciplinary Studies*, vol. 4, no. 1, pp. 117–130, Sep. 2022, doi: 10.53022/oarjms.2022.4.1.0091.

[19] P. Acosta-Vargas, G. Acosta-Vargas, B. Salvador-Acosta, and J. Jadán-Guerrero, "Addressing Web Accessibility Challenges with Generative Artificial Intelligence Tools for Inclusive Education," in *2024 Tenth International Conference on eDemocracy &amp; eGovernment (ICEDEG)*, IEEE, Jun. 2024, pp. 1–7. doi: 10.1109/ICEDEG61611.2024.10702085.

[20] L. Wang and C. B. Aldave, "Leveraging Emerging Technologies in Pricing Strategies and Consumer Behavior: Case Studies from China's Innovative Markets," *International Journal of Emerging Technologies and Advanced Applications*, vol. 1, no. 6, pp. 6–12, Jul. 2024, doi: 10.62677/IJETAA.2406121.

[21] Nnaemeka Valentine Eziamaka, Theodore Narku Odonkor, and Adetola Adewale Akinsulire, "AI-Driven accessibility: Transformative software solutions for empowering individuals with disabilities," *International Journal of Applied Research in Social Sciences*, vol. 6, no. 8, pp. 1612–1641, Aug. 2024, doi: 10.51594/ijarss.v6i8.1373.

[22] K.-Q. Zhou and H. Nabus, "The Ethical Implications of DALL-E: Opportunities and Challenges," *Mesopotamian Journal of Computer Science*, pp. 17–23, Jan. 2023, doi: 10.58496/MJCSC/2023/003.

[23] Rezwana. , Jeba and L. Maher. Mary, "Identifying Ethical Issues in AI Partners in Human-AI Co-Creation," 2022, doi: 10.48550/arXiv.2204.07644.

[24] J. P. Johnson, A. Rhodes, and M. Wildenbeest, "Platform Design When Sellers Use Pricing Algorithms," *Econometrica*, vol. 91, no. 5, pp. 1841–1879, 2023, doi: 10.3982/ECTA19978.

[25] G. A. Seidullayeva, G. K. Temirkulova, and Zh. L. Kenzhitaeva, "Features of Modern Comic Advertising," *Iasaýı ýnıversıtetiniń habarshysy*, vol. 132, no. 2, pp. 26–39, Jun. 2024, doi: 10.47526/2024-2/2664-0686.41.

[26] J. C. Rodrigues, "Price Management on Global Digital Subscription Services Using Freemium Business Model," 2019, pp. 178–196. doi: 10.4018/978-1-5225-7265-7.ch010.

[27] W. Chen and H. Yang, "Editorial: New challenges and future perspectives in motivation and reward," *Front Behav Neurosci*, vol. 17, Sep. 2023, doi: 10.3389/fnbeh.2023.1293938.

[28] S. Chaudhuri and M. Roy, "Irrigation Water Pricing in India as a Means to Conserve Water Resources: Challenges and Potential Future Opportunities," *Environ Conserv*, vol. 46, no. 1, pp. 99–102, Mar. 2019, doi: 10.1017/S037689291800036X.

[29] Christophe, Jean-Christophe, Burie, P. Samuel, Rigaud, and Petit, "Toward accessible comics for blind and low vision readers. ," 2024, doi: 10.48550/arxiv.2407.08248.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 1 (2025)
https://doi.org/10.31436/ijpcc.v11i1.540

The Future of Food Security: The Role of Blockchain Technology in Global Aquaculture

Zarith Sofea Hazzarul Hisham, Anha Ayamon, Nur Lisa Ashiqeen Mohd Fadzullah, Nurul Aisyah Mohd Rusllim, Majdi Ahmadi Mohd Zohdi, Muhammad Ammar Amsyar Mohd Azhar, Waiz Wajdi Mahamad Yazid, Muhammad Mukhrizq Wafiq Mohd Masri , Ahmad Anwar Zainuddin*

Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Gombak, Malaysia.

*Corresponding author anwarzain@iium.edu.my

(Received: 3rd January, 2025; Accepted: 15th January, 2025; Published on-line: 30th January, 2025)

Abstract— The aquaculture sector faces challenges in maintaining a transparent and traceable supply chain, leading to issues like fraud and compromised food safety for consumers worldwide. Studies reveal that nearly 20% of the global seafood industry engages in mislabelling practices, which significantly undermines consumer trust. From harvesting to sale, blockchain technology offers a safe, immutable database that records each stage of the supply chain. Reliability is ensured by users verifying the data. IoT devices and QR codes gather real-time data on product origin, quality, and handling to improve safety and trust making it available to authorities and consumers. The importance of implementing a robust sustainability and traceability system and becomes evident with the European Commission's decision to temporarily suspend fish imports from Thailand due to the prevalence of illegal fishing practices. This blockchain-based strategy offers an integrated solution to current supply chain problems by enhancing regulatory compliance, minimising fraud, and fostering sustainable behaviours. By documenting each stage in an immutable ledger, this study explores blockchain's potential to transform the aquaculture supply chain, creating a system where product history is fully transparent for consumers and regulators. Most case studies and research, focus primarily on developed regions. This underscores the need for further exploration of blockchain implementation in small-scale and underdeveloped aquaculture settings. Ultimately, this solution fosters a safer, more responsible seafood industry that promotes sustainable practices and benefits society overall.

Keywords— aquaculture, blockchain technology, traceability, food safety, sustainability

I. INTRODUCTION

The agriculture and aquaculture sectors are responsible for food security at a global level, but these sectors are facing major challenges when it comes to transparency, sustainability and operational efficiency. The industry's growing inability to cope with consumer demand for sustainably sourced and safe food is further compounded by issues such as fraud, poor data management, and environmental degradation in conventional supply chains that are already stalling and expanding. The use of valuable digital technologies (e.g. blockchain, IoT, AI) can be the efficiency solution of these problems through the increasing supply chain traceability and guaranteeing food safety, validated by several survey data and case study evidence [1].

This rapidly growing area of food production has its own challenges but has a lot of things in common, including illegal, unreported and unregulated (IUU) fishing, an absence of transparency about how these foods are produced and low levels of consumer confidence. In 2014, more than half of all seafood was grown on farms; and with continued growth and improvement of the industry, aquaculture is destined to play a role in meeting the high turnover of seafood hunter's seafood consumption trends globally. But this boom has also brought issues of sustainability and supply chain waste into sharper focus. Blockchain based security with IoT devices, AI based analytics and big data ecosystems in aquaculture presents a strong underpinning for ensuring data integrity, enhanced monitoring and sustainable practices [2], [3]. In the recent past, there has been a lot of buzz about blockchain as it provides a trustless and distributed ledger system which is immutable. You have that technology, where you can instantly collect and verify data up and down the supply chain. The IoT takes key metrics around fish health, water quality, feeding schedule etc. — and records this information in a way that is immutably secure, on something like a blockchain, so everyone knows what, when where, and why (and can, ideally, trust it as homegrown) and to where it should be going [4]. This leads to improved traceability that guarantees compliance (with regards to environment friendliness), reduces fraud, and increases consumer confidence [5].

Moreover, the results of this research correspond directly to a number of United Nations Sustainable Development Goals (SDGs). Together, by enabling the agriculture and aquaculture sectors to amplify transparency, sustainability and operational efficiency is the way we help drive towards SDG 2: Zero Hunger, SDG 12: Responsible Consumption and Production and SDG 14: Life Below Water. Increasing traceability and preventing fraudulent activity improve food security and reduce environmental impacts such as pollution for example from overfishing. These technological advancements may significantly contribute to the construction of a more equitable and sustainable food system that offered advantages to both producers and consumers by promoting sustainable practices and equipping consumers with reliable information [6].

Figure 1 is an overview of aquaculture blockchain-enabled seafood traceability, which shows all the key steps in the traceability of aquaculture supply chains. It starts with egg laying, and then fish are cultivated in controlled environments. The fish is then checked for quality and packed while ensuring adherence to health and safety guidelines. Conditions, including temperature and handling, are tracked as the seafood is shipped to distribution centers or retailers. Products are stored and then made available for sale to end users. The icons at each stage represent how data is securely recorded and verified on the blockchain, creating a transparent, traceable, and accountable system. Such a system provides consumers and other stakeholders with verified and transparent information about their seafood, from harvesting to plate, engendering trust and helping to support more sustainable businesses.

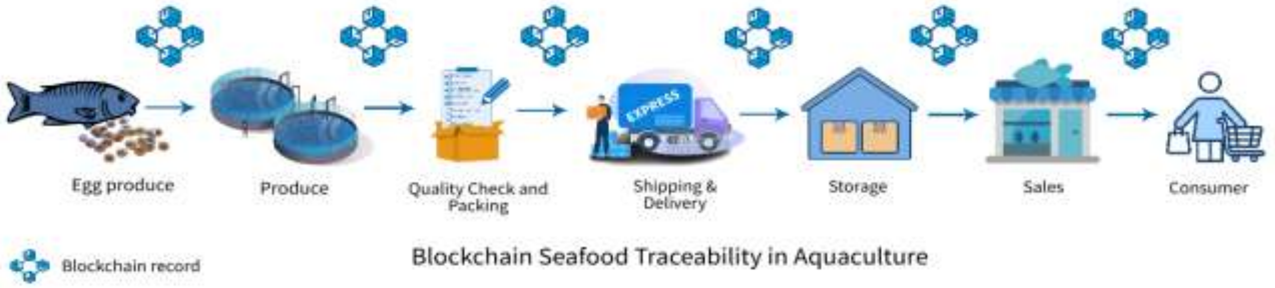


Fig. 1 Blockchain traceability system in the aquaculture supply chain

Since 2003, China has been at the forefront of providing blockchain technology and other digital innovations as the world's largest aquaculture producer [7]. So, in this transition, so many new innovations of IoT and AI Technologies are being used to modernize aquaculture practices as fish farming have many common problems: However, challenges for the industry remain high in terms of implementation costs, the need for standardized protocols, and a need for a more cohesive strategy in how we approach sustainability concerns [8]. Case studies around the world, like blockchain-based shrimp and tuna tracking programs, serve as growing evidence of this transformation — and of the use of the technology with sustainability by design and securing. This paper aims to review the applications of blockchain technology within the aquaculture industry, highlighting its potential with other advanced technologies such as the Internet of Things, Artificial Intelligence, and others. This paper aims to review the applications of blockchain technology within the aquaculture industry, highlighting its potential with other advanced technologies such as the Internet of Things, Artificial Intelligence, and others. It delves into how the potential of blockchain technology can improve traceability, promote sustainability and improve operational efficiencies, across the aquaculture supply chain. A framework is proposed for cannabis adoption in aquaculture, noting challenges and opportunities associated with this pathway and providing case studies that exemplify the impact of cannabis on aquaculture systems.

This paper is organized as follows; Section I gives a brief overview of how blockchain technology, combined with other digital tools like IoT and AI, is transforming aquaculture industry. Section II provides literature reviews for this work. Section III covers the methodology used for this study. Section IV represents the results and discussion of this study which provides a detailed explanation of the benefits and potential applications of blockchain technology in aquaculture industry. Lastly, Section V provides the summarization and conclusion of this study.

II. LITERATURE REVIEWS

Table 1 represents a literature review, summarizing key studies and insights on the role of blockchain technology in enhancing food security within the global aquaculture sector.

TABLE I
LITERATURE REVIEW

Article	Key Findings/Argument	Supporting Evidence/ Sample Characteristics/ Method	Strengths/ Limitations
[9]	This research discusses how blockchain boosts safety, quality, traceability, and transparency in seafood supply chains.	The research explores blockchain in aquaculture, highlighting transparency, sustainability, and tackling IUU fishing practices.	This research explores blockchain in aquaculture, focusing on sustainability, transparency, adoption barriers, and stakeholders resistance.
[10]	This study finds blockchain reduces illegal fishing, improves traceability, and supports sustainable consumer demands globally.	The literature review, using PRISMA, identified 37 blockchain records (2018-2021) with text-mined terminologies detailed in tables.	The study highlights research gaps, blockchain use in fisheries, and aquaculture but notes potential obsolescence.
[11]	The paper highlights advanced technologies in aquaculture, promoting sustainability, while outdated laws hinder innovation adoption.	This paper emphasizes aquaculture, "Industry 4.0" data insights, and innovations boosting fish production efficiency.	This paper highlights aquaculture's current state, tech potential, and strategies, yet lacks global applicability.
[12]	The study highlights Blockchain Technology's potential in improving aquaculture traceability and ensuring supply chain transparency.	The study suggests Blockchain Technology addresses data gaps, ensuring traceability and emphasizing stakeholder collaboration for standards.	This study excels in sustainability and safety insights but faces adoption challenges from costs and distrust.
[13]	The study highlights blockchain's potential for aquaculture traceability, emphasizing transparency and differing company needs.	The authors developed a tailored blockchain solution for L Aquatic Products Co., Ltd. After analysing their processes.	The study highlights blockchain's aquaculture potential but is limited by narrow focus and outdated literature scope.
[14]	Blockchain enhances aquaculture supply chain transparency, automates compliance, boosts efficiency, and fosters consumer trust.	This study highlights a multilayer system for supply chain tracking, improving food safety, and blockchain cost-effectiveness.	The study highlights IoT-driven environmental compliance but faces challenges in underdeveloped nations due to costs and readiness.
[15]	This paper proposes a decentralized blockchain system for fishery traceability, emphasizing precise stakeholder data input.	The researchers use sequence diagrams, smart contracts, and security analysis to enhance fishery traceability and resilience.	The blockchain solution boosts fishery traceability with IoT and engagement but needs accurate data and further testing.
[16]	This study finds blockchain improves fisheries traceability, ensuring transparency, with Ethereum smart contracts enhancing monitoring.	The study demonstrates Ethereum-based blockchain and smart contracts for fish supply chain traceability, ensuring transparency and compliance.	This study proposes a blockchain approach for aquaculture, enhancing transparency and trust but facing scalability and cost challenges.
[17]	The study highlights blockchain's role in improving traceability, security, and trust in marine aquaculture via IoT, AI, and Big Data.	Blockchain applications like FishCoin and ShrimpChain enhance seafood traceability, while IoT and AI optimize quality and operations.	This blockchain-IoT framework enhances aquaculture transparency but faces adoption, cost, and data reliability challenges.
[18]	Blockchain is expected to enhance fishery traceability, simplify processes with smart contracts, and promote sustainable practices.	This research emphasizes IoT sensors for supply chain transparency and YOLOv8's role in environmental monitoring, requiring integrated data collection for model optimization.	This research effectively employs Blockchain, IoT, and YOLOv8 for fisheries management but faces technological and adoption challenges.
[19]	Integrating blockchain, IoT, and machine leaning enhances fish supply chains, addressing challenges with a layered framework for authenticity and data sharing.	The researchers reviewed Blockchain in fish supply chains and developed a framework emphasizing machine learning for quality and safety.	This paper highlights blockchain, IoT, and ML integration for fish supply chains but notes implementation and research gaps.
[20]	This study showcases blockchain's role in aquaculture, enhancing transparency, communication, and sustainability through compliance tracking.	This study examines blockchain adoption in aquaculture, integrating interviews and analytics to compare its efficiency with traditional methods.	This study highlights blockchain's economic and scalable benefits for aquaculture but notes resistance, compatibility, and long-term viability concerns.
[21]	The research shows blockchain enhances product transparency, boosting	Surveyed consumer attitudes show blockchain improves seafood	This research showcases blockchain's role in sustainable seafood initiatives

	customer engagement and informed seafood purchasing decisions.	traceability, origins access, and sustainability awareness.	but notes sample bias and short-term focus.
[22]	The study shows blockchain reduces aquaculture's environmental impact by enhancing compliance, preventing overfishing, and ensuring responsible sourcing.	The case study analyses blockchain's role in aquaculture sustainability using catch reports and compliance records insights.	This study showcases blockchain's role in aquaculture sustainability but highlights challenges like data accuracy and adoption resistance.
[23]	The research suggests blockchain enhances stakeholder collaboration in aquaculture, improving information flow and sustainability practices.	The research uses focus groups to explore blockchain's role in aquaculture collaboration and reviews successful case studies.	The research emphasizes blockchain's role in stakeholder collaboration for sustainability but notes challenges like resistance and data subjectivity.
[24]	The study finds a blockchain platform boosts fish product traceability, transparency, trust, and data integrity across the value chain.	The study emphasizes fish value chain integration, highlights Ethereum smart contracts, and supports blockchain traceability with ISO 22005.	Despite challenges like technology, data management, and interface needs, the study proposes blockchain to enhance fisheries traceability.
[25]	The paper identifies blockchain implementation challenges in fisheries and recommends building trust, infrastructure, and financial incentives.	The paper employs a three-phase framework with expert input: identifying barriers, refining them, and analysing causal links.	This paper excels in enhancing data reliability but has limited generalizability due to context-specific expert biases.
[26]	The study highlights data reliability and challenges in poor regions, advocating blockchain, IoT, and AI for food traceability.	This study reviews food traceability literature, exploring blockchain-IoT benefits, data gaps, and technical needs for implementation.	The study deeply analyses food traceability but lacks real-world examples, focusing on developed areas and requiring further research.

A. Research Gaps

Literature review on blockchain technology aquaculture brings considerable understanding of various benefits associated with this technology, which includes increased traceability, sustainability, and efficiency of operations. However, a number of these gaps are persisting and provide a constraint to a comprehensive understanding of its application and scalability.

One of the gaps found the geographic scope. Most of the research focused on developed regions, and there are only a few studies related to blockchain adoption in developing countries. The small-scale aquaculture practiced throughout these regions poses other set of challenges due to the lack of technological and financial infrastructure. This would give further insight into how blockchain could be fitted to those contexts to have truly inclusive solutions serving the larger aquaculture industry.

Despite the theoretical benefits that blockchain could impart, very few quantitative case studies have measured the real-world impact of the technology. Specific data such as fraud-reduction rates, operational cost savings, or improved sustainability metrics is rarely provided. Without these empirical data, a stakeholder would have a very difficult time justifying the necessary investment to adopt blockchain.

Issues that are always talked about involve a high cost of implementation as well as resistance by stakeholders. In any case, there is no detailed analysis regarding the two issues. For example, the stakeholders in conventional supply chains are either unfamiliar or distrustful of digital technologies. Addressing these challenges effectively through education, incentives, and simplified blockchain solutions are important for wider diffusion, especially in underdeveloped regions.

B. Recommendations for Future Research

Thus, future research should focus on filling these gaps. The emphasis on future research should be based on studies in developing regions and in small-scale aquaculture systems, since many of them have special economic and infrastructural problems which are not well reflected in the literature review. In this respect, research should be done on blockchain solutions tailored to suit them, affordable and feasible, with broader inclusion and equity in aquaculture advancement.

Potential benefits due to blockchain would have to be emphatically determined through empirical research. Future research should hence focus on the collection and analysis of data that would realistically measure indicators of performance related to fraud reduction, cost savings, and improvements in sustainability metrics. These insights would provide stakeholders with the justification needed to adopt blockchain technologies.

Research on looking into overcoming high costs of implementation and stakeholder resistance, especially those that are not familiar with digital technologies needs to be done. The research may look into training the stakeholders or giving them financial motives, while at the same time developing simplified blockchain solutions which will easily be adopted and integrated within supply chains. Building trust among these stakeholders shall be paramount for wide acceptance.

III. METHODOLOGY

The methodology used for this paper focuses on a comprehensive analysis of blockchain technology in addressing food security challenges within the global aquaculture sector. A thorough literature review, supported by a systematic collection of data from reliable academic databases and industry publications, served as the basis for the paper.

The data from these sources are published from 2019 onwards to guarantee that the most updated information is obtained to pinpoint recent developments in blockchain, IoT, and AI applications in aquaculture. The focus is on very recent studies to ensure that the latest developments and case studies are covered. However, foundational works published before 2019 are also referenced when applicable, as they provide theoretical foundation and historical context for the evolution of technology.

The number of papers used as a reference is at least 15 papers. The literature review studied focuses on identifying blockchain’s application in aquaculture, including supply chain transparency and traceability, fraud prevention, and reducing inefficiencies in food distribution. By identifying challenges and chances to formulate a solution in implementing blockchain technology in the aquaculture industry, recommendations are made thoroughly to fulfill this criterion.

There were still some possible biases and limitations to note in the paper themselves, despite the system analysis. Most of these are regionally or contextually based case studies that could inhibit, to some degree, the generalizability of findings across aquaculture contexts worldwide. This study considered the geographical and contextual nature of each paper under review for area trends that could be applied to larger regions. However, it acknowledges that the unique challenges and infrastructural constraints in small-scale settings or underdeveloped regions of aquaculture require further exploration and tailored solutions.

Methodologically, reliance on secondary data brings potential limitations in the accuracy and completeness of the original studies. This analysis, therefore, prioritizes papers with robust methodologies, such as empirical research and systematic reviews, while highlighting gaps in areas where the data is sparse or inconsistent.

The study aims to address these considerations by providing research relevant to a wide range of aquaculture stakeholders, while also identifying areas where further research is needed to enhance regional applications.

IV. RESULTS AND DISCUSSION

A. Key Benefits of Blockchain Technology

As blockchain technology promises efficiency, transparency, and traceability globally, its application in food security has grown recently. This is because consumers will be able to learn where their food comes from thanks to this technology. The use of blockchain has huge potential to improve food security, particularly at a time when aquaculture is expected to remain the primary source of protein. It has the potential to change the way aquaculture meets global food demands by resolving issues with traceability, sustainability, and efficiency.

One of the major benefits of blockchain technology in aquaculture is increased traceability of the products throughout the value chain. Stakeholders can track the origins of fish products from wherever they came to their plates thanks to blockchain's decentralized and unchangeable record. This is very important in ensuring the safety of food since sources of contamination can be identified quickly, thus helping increase consumer confidence in what they consume. [27]. For example, blockchain technology can be used to guarantee that fish and seafood are sourced responsibly and that their origins are transparent in areas where aquaculture plays a major role in local economies [28] will help to ease consumer concerns about overfishing and environmental degradation [29]. In recent years, blockchain technology has picked up tremendous momentum in its application to food security because of the promise it holds for efficiency, transparency, and traceability across the world. This is because, with the technology, consumers would finally be able to trace where their foods come from. According to the study made by T. Asha Vijay and M. S. Raju, research indicates that approximately 20% of the global seafood industry is involved in mislabelling practices [30]. Food security could possibly be greatly enhanced through the integration of blockchain, at least at a time when aquaculture was expected to remain the leading source of protein. It has the potential to change how aquaculture contributes to global food security by trying to solve the problems of efficiency, sustainability, and traceability [31], [32]. This ability lowers financial costs related to food recalls and waste while also boosting consumer confidence [33]. It is evident that apart from lesser-known industries like trade finance and convertible bonds, blockchain technology can also enhance more common activities such as stock trading and international payments. Today, blockchain is gaining significant attention from countries, and the environment is well-suited for its growth and adoption [34]. Aquaculture producers can improve their sustainability practices and lessen their ecological imprint by using blockchain to track ratios of feed conversion and health factors, which will help ensure global food security [35]. For instance, due to the significant scale if illegal, unreported, and unregulated fishing activities, the European Commission issued a yellow card to Thailand a few years ago, temporarily halting all fish imports from the country. Implementing an end-to-end supply chain system for seafood tracking and tracing, enabled by AI and blockchain technology, holds the potential to modernize the industry and boost export opportunities [36].

Apart from improving production, there might also be other beneficial ways where blockchain technology can be used to facilitate financial services and market accessibility. Farmers who document their catching processes well and the good qualities of the seafood grown with excellent service would win consumers' trust for much higher prices [37]. This is particularly true in underdeveloped countries where small-scale aquaculture plays a significant role in local food systems and revenues [38]. Furthermore, blockchain can facilitate aquaculture farmers' access to insurance and financial solutions that meet their demands, improving their ability to adjust to climatic shifts and fluctuations in the market [39], [40].

Furthermore, there is a possibility that blockchain technology will enhance the efficiency of logistics and reduce administrative obstacles in aquaculture. Durach et al. add that blockchain could help in enhancing the processes of delivery by making the process transparent, where all stakeholders will have real-time information on shipments, which would encourage mutual trust and accountability [41]. Through a source of truth that is tamper-proof, blockchain will simplify all documentation processes and improve communication amongst stakeholders from farmers to merchants [42]. Consumer will benefit from premium seafood at competitive pricing as a result of the resulting efficiencies, which will reduce costs and enhance service delivery [43].

Figure 2 summarizes some of the key benefits that can be achieved by using the blockchain technology in aquaculture, including improved global food security, enhanced traceability and food safety, increased sustainability and cost reduction, provided better financial services and market access, and optimised logistics and administration.

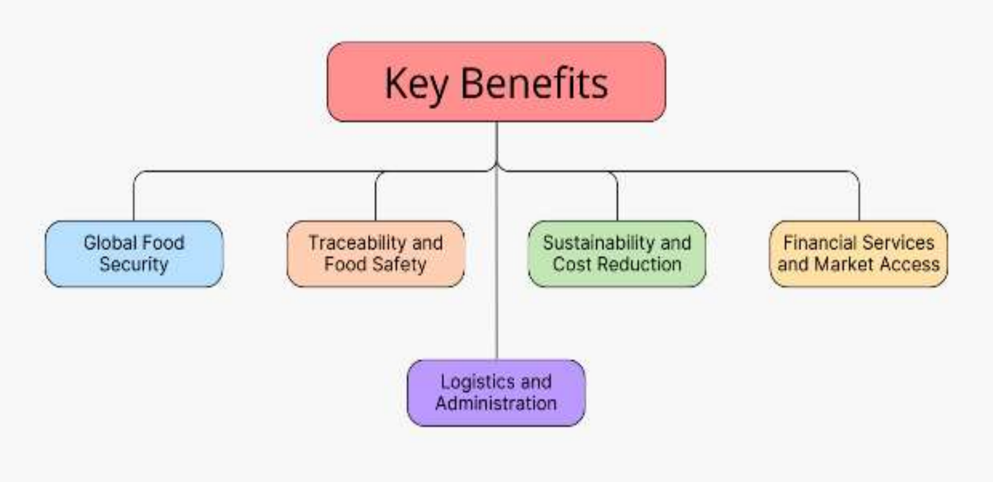

Key Benefits
Global Food Security
Traceability and Food Safety
Sustainability and Cost Reduction
Financial Services and Market Access
Logistics and Administration

Fig. 2 Key Benefits of Blockchain Technology

B. Implementation Challenges and Recommendations

Although blockchain technology has the potential to improve global food security and sustainability in global aquaculture, its application in underdeveloped countries and in traditional supply chains face significant obstacles.

One of major challenges is technological barriers. This is because the complexity of blockchain technology and the lack of understanding among stakeholders are significant hurdles. Many supply chains lack the necessary infrastructure and technical expertise to implement blockchain effectively, which is particularly pronounced in underdeveloped regions [44], [45], [46]. Despite its potential, the technology used is still in its early stages, and there is a need for further research and development to address this barrier [47], [48]. Enhancing data management by investigating methods to improve data asymmetry and management within blockchain systems to ensure seamless integration across the supply chain can help solving this [49], [50]. Future research should prioritize developing standardized data structures to enable blockchain implementation in aquaculture supply chains. This approach will help resolve data asymmetry issues and support real-time interventions aimed at achieving the Sustainable Development Goals (SDGs) [49], [51]. Future implementations could involve using smart contracts to automate and manage transactions within the aquaculture supply chain. This would enhance efficiency, reliability, and security while eliminating the need for intermediaries [52], [53].

Additionally, unfavourable institutional environments and the lack of supportive policies and standards hinder the adoption of blockchain technology. This challenge is particularly significant in developing countries, where regulatory frameworks do not accommodate such technological advancements [45], [46], [48]. Working with policymakers to establish regulations that support the adoption of blockchain in aquaculture, while addressing critical concerns such as data privacy and security, can help resolve this issue [48], [51]. Other suggestion is by working towards creating standardized protocols and guidelines for blockchain implementation to ensure consistency and interoperability across different regions and sectors [54], [55]. To successfully implement blockchain technology in global aquaculture, it is crucial to involve all stakeholders actively. This involves engaging aquaculture companies, retailers, and consumers to ensure they understand the benefits and are motivated to support the implementation of blockchain systems [12], [42].

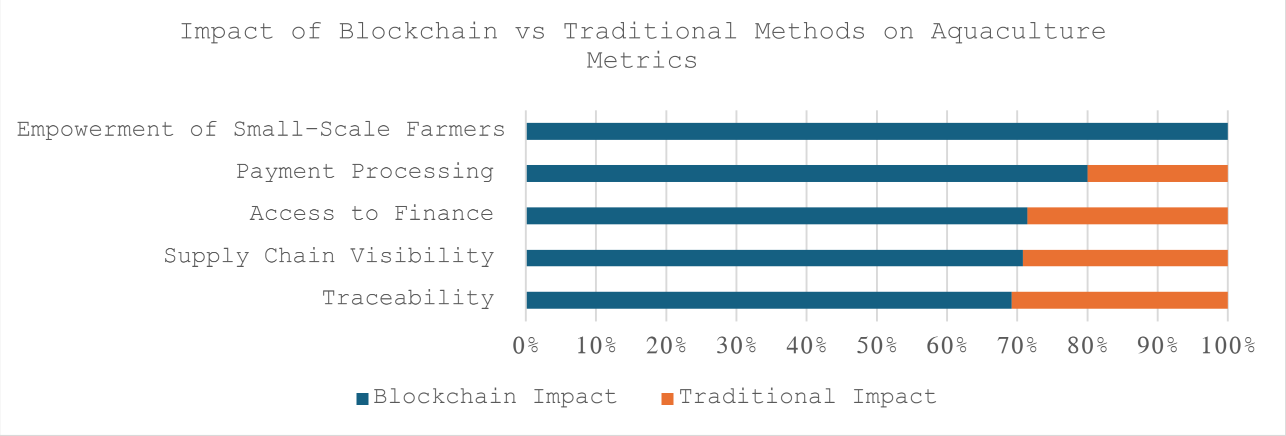


Fig. 3 Impact of Blockchain vs Traditional Methods on Aquaculture Metrics

Furthermore, countries with limited financial resources face challenges due to the high costs and resource demands associated with implementing blockchain technology, including setup and maintenance [45]. The implementation of a sustainable supply chain using blockchain technology is further complicated by the absence of well-defined business models and best practices for adopting this system [56]. To address this, conduct detailed cost-benefit analyses to assess the financial implications of blockchain adoption and uncover potential cost-saving opportunities. Seek and secure funding from governmental and non-governmental organizations to support blockchain projects in aquaculture, emphasizing long-term sustainability and scalability [51], [53]. Explore strategies to optimize resource allocation in blockchain projects, ensuring that investments are focused on areas with the greatest potential to enhance food security and promote sustainability [49], [57].

Blockchain technology can only be effective in aquaculture finance if it is integrated with existing digital systems. Achieving this requires a significant move toward digitalization within the industry, which may become a critical prerequisite for the successful operation of blockchain [58]. According to [20], IUU fishing accounts for 20 percent of the global catch, with this figure reaching up to 50 percent in certain regions. The sector often relies on bonded labour, destructive fishing practices, and fraudulent methods to generate income, all while harming local fisheries, coastal states, and marine ecosystems. Recognized as a major global issue, IUU fishing is estimated to involve one-fifth of all wild-caught fish, translating to economic losses of $10 billion to $23.5 billion annually. Creating a detailed implementation roadmap that encompasses concept development, compliance, and optimization is crucial for addressing this issue effectively [42]. Designing pilot projects and prototypes can help evaluate the feasibility and efficiency of blockchain technology in aquaculture. These initiatives provide valuable insights into the practical challenges and advantages of implementing blockchain, paving the way for further refinements and optimizations [42]. Offer education and training programs to help stakeholders understand the benefits and workings of blockchain technology, promoting a culture of innovation and adaptability [48], [53].

C. Comparison between Blockchain Technology with Alternative Technologies

Blockchain technology is gaining widespread recognition for its ability to enhance transparency, traceability, and trust within supply chains, particularly in the aquaculture and agri-food sectors. Its core features, such as immutability, auditability, and provenance, work together to promote transparency and minimize the risk of fraudulent practices [48], [57], [59]. The decentralized nature of blockchain ensures that no single authority can modify the data, making it a reliable and robust solution for maintaining trustworthy records [55]. In aquaculture, blockchain technology can strengthen the relationship between producers, retailers, and consumers by ensuring transparency, credibility, and fairness in transactions [12].

Several alternative technologies are available for use in aquaculture. One of the most common is traditional databases, which are often employed for record-keeping in supply chains. However, these databases lack the inherent trustworthiness of blockchain, as they are vulnerable to tampering and rely on a central authority for data management and verification [58]. Figure 3 illustrating the impact of blockchain technology with traditional methods on different aquaculture metrics, like the empowerment of small-scale farmers, payment processing, access to finance, supply chain visibility, and traceability. While these alternatives can be effective in digitalized environments, they do not inherently offer the same level of transparency and traceability as blockchain. Additionally, while digitalizing supply chains can significantly enhance efficiency and data management, it does not inherently ensure data integrity or prevent fraud—two critical advantages provided by blockchain technology [58]. IoT devices play a vital role in aquaculture by enhancing data collection and monitoring, offering real-time insights into environmental conditions and fish health. However, IoT alone cannot address data integrity and trust issues. Blockchain complements IoT by securely recording data in an immutable ledger, ensuring reliability and transparency [60]. AI can significantly optimize aquaculture operations by forecasting trends and automating various processes. However, while it enhances efficiency, AI alone does not address the critical issues of data transparency and traceability, which are essential for building consumer trust and ensuring regulatory compliance [60].

Blockchain technology is ideally suited to addressing the challenges of transparency, traceability, and trust within aquaculture and agri-food supply chains. Its design guarantees secure, immutable records of transactions, making it superior to traditional databases and other technologies that lack these built-in features. While digitalization and IoT enhance data collection and operational efficiency, blockchain stands out by uniquely ensuring data integrity and credibility—critical for building consumer trust and achieving sustainability objectives [49], [57], [51].

In conclusion, while other technologies provide certain advantages, blockchain's distinctive features of immutability and decentralized trust make it an excellent choice for improving transparency and traceability in global aquaculture and food supply chains.

V. CONCLUSION

The food security of the world is dependent on the farming and aquaculture industry as two of its main pillars. Yet, they struggle to deliver transparency, sustainability, and operational efficiency. In this paper, we investigated the use of disruptive digital technologies in aquaculture, like blockchains, IoT, and AI, which could pave the way for transformation in aquaculture practice. All of this was possible over mainstream technologies with ease and should be enough to universally improve supply chains crippled with differentiation, piracy, management or environment driven issues.

Blockchain provides a decentralized and tamper-proof ledger system that can greatly enhance traceability and transparency in the aquaculture supply chain [15]. Blockchain offers security in the supply chain through the validation and verification of data when combined with Internet of Things (IoT) devices that monitor conditions like fish health, water quality and feeding schedules [61]. This integrated approach has direct implications for combatting illegal, unreported and unregulated (IUU) fishing, enhancing consumer confidence, and addressing the increasing demand for sustainably produced and safe seafood.

Global case studies, including blockchain-supported shrimp and tuna tracking initiatives, demonstrate how these technologies can help remedy problems of environmental degradation and supply chain opacity [62]. An example can be found in countries such as China — a world leader in the aquaculture sector — which offers you insights into how blockchain and IoT are revolutionizing operations and creating new standards in sustainability and in providing innovative practices. Among China's measures are the establishment of blockchain-based systems for end-to-end traceability in shrimp, tuna, and other seafood [25]. Such systems help verify product information by generating unalterable records at all points in the supply chain. The use of IoT-enabled devices like water quality sensors and a feeding monitor generates real-time data about aquaculture operations and keeping the water environment in check to ensure maximum efficiency and minimal waste [63], [64], [65]. However, most of these systems are still witching optimization, as they have not yet finished several aquaculture cycles to reach full operational maturity. While difficult, China's leadership in the uptake of digital aquaculture technology shows that these innovations can be scaled — a model from which other countries wishing to modernise their aquaculture sector can learn. Great way to phrase it: China's pro-active fisheries supply chain engagement is helping not just with the transparency and efficiency in the aquaculture supply chain, but also the consumers trust in sustainably sourced seafood [66]. But with the world's hunger for seafood ever on the rise, China's ambitions are a blueprint for how to use advanced technologies to help solve systemic problems across an industry. China's holistic approach to the digital transformation of aquaculture, focusing on collaboration and standardized protocols, will ultimately transform the industry for the better.

There are still significant obstacles ahead, though. Another barrier identified is high implementation costs, lack of standardized protocols, and fragmented strategies around food systems that make widespread adoption difficult [67]. Moreover, there are still challenges in both harmonizing interests among stakeholders and adapting technologies to different industrial and regional activities. However, the strides we've made thus far point to a bright future.

To solve these challenges now and in the future we need to take action on multiple fronts. To achieve this, standardized protocols and interoperable systems for data exchange and integration can be developed, promoted, and adopted along the aquaculture value chain. It is essential to invest in research and development to decrease the high prices to implement and make these technologies more simpler to use. Encouraging cooperation and dissemination of information among various stakeholders (governments, industry players, and academia) is key to the successful implementation and scaling of these technologies.

Adoption of these innovations will be critical in bringing the aquaculture industry towards greater sustainability, efficiency, and transparency. This has direct links to several United Nations Sustainable Development Goals (SDGs) — SDG 2: Zero Hunger; SDG 12: Responsible Consumption and Production; and SDG 14: Life Below Water. Digitizing the aquaculture industry will secure the food source for the future and protect the ocean whilst securing sustainable food sources for generations to come [6].

Acknowledgment

Heartfelt appreciation to our esteemed professors and educators for their steadfast dedication and diligent efforts in imparting invaluable knowledge to us. Their commitment has greatly contributed to our advancement in enhancing our skills and comprehension in the field of Computer Networking, IoT security, and Blockchain technology.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] M. M. Queiroz and S. Fosso Wamba, “Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA,” *International Journal of Information Management*, vol. 46, pp. 70–82, Jun. 2019, doi: 10.1016/j.ijinfomgt.2018.11.021.

[2] A. Shamsuzzoha, J. Marttila, and P. Helo, “Blockchain-enabled traceability system for the sustainable seafood industry,” *Technology Analysis & Strategic Management*, vol. 36, no. 11, pp. 3891–3905, Nov. 2024, doi: 10.1080/09537325.2023.2233632.

[3] H.-Y. Lan, N. A. Ubina, S.-C. Cheng, S.-S. Lin, and C.-T. Huang, “Digital Twin Architecture Evaluation for Intelligent Fish Farm Management Using Modified Analytic Hierarchy Process,” *Applied Sciences*, vol. 13, no. 1, p. 141, Dec. 2022, doi: 10.3390/app13010141.

[4] S. Ismail, H. Reza, K. Salameh, H. Kashani Zadeh, and F. Vasefi, “Toward an Intelligent Blockchain IoT-Enabled Fish Supply Chain: A Review and Conceptual Framework,” *Sensors*, vol. 23, no. 11, p. 5136, May 2023, doi: 10.3390/s23115136.

[5] C. D. Duong, T. T. Dao, T. N. Vu, T. V. N. Ngo, and M. H. Nguyen, “Blockchain-enabled food traceability system and consumers' organic food consumption: A moderated mediation model of blockchain knowledge and trust in the organic food chain,” *Sustainable Futures*, vol. 8, p. 100316, Dec. 2024, doi: 10.1016/j.sftr.2024.100316.

[6] “Sustainable Agriculture and Sustainable Development Goals (SDGs),” in *Practice, Progress, and Proficiency in Sustainability*, IGI Global, 2024, pp. 1–27. doi: 10.4018/979-8-3693-4864-2.ch001.

[7] H. Zhang and F. Gui, “The Application and Research of New Digital Technology in Marine Aquaculture,” *JMSE*, vol. 11, no. 2, p. 401, Feb. 2023, doi: 10.3390/jmse11020401.

[8] B. Masoomi, I. G. Sahebi, M. Ghobakhloo, and A. Mosayebi, “Do industry 5.0 advantages address the sustainable development challenges of the renewable energy supply chain?,” *Sustainable Production and Consumption*, vol. 43, pp. 94–112, Dec. 2023, doi: 10.1016/j.spc.2023.10.018.

[9] A. Platonava, T. Tsironi, and M. Cashin, "Blockchain in Aquaculture: Enhancing Sustainability and Transparency," p. 563 KB, 9 pages, 2024, doi: 10.48446/OPUS-15780.

[10] F. Tolentino-Zondervan, P. T. A. Ngoc, and J. L. Roskam, "Use cases and future prospects of blockchain applications in global fishery and aquaculture value chains," *Aquaculture*, vol. 565, p. 739158, Feb. 2023, doi: 10.1016/j.aquaculture.2022.739158.

[11] A. V. Altoukhov, "Industrial product platforms and blockchain in aquaculture," *IOP Conf. Ser.: Earth Environ. Sci.*, vol. 421, no. 4, p. 042021, Jan. 2020, doi: 10.1088/1755-1315/421/4/042021.

[12] A. Mileti, D. Arduini, G. Watson, and A. Giangrande, "Blockchain Traceability in Trading Biomasses Obtained with an Integrated Multi-Trophic Aquaculture," *Sustainability*, vol. 15, no. 1, p. 767, Dec. 2022, doi: 10.3390/su15010767.

[13] Y.-J. Pan and H.-P. Shieh, "APPLICATION OF BLOCKCHAIN TECHNOLOGY IN AQUACULTURE MANAGEMENT," *Journal of Marine Science and Technology*, vol. 31, no. 3, Oct. 2023, doi: 10.51400/2709-6998.2701.

[14] M. Luna, S. Fernandez-Vazquez, E. Tereñes Castelao, and Á. Arias Fernández, "A blockchain-based approach to the challenges of EU's environmental policy compliance in aquaculture: From traceability to fraud prevention," *Marine Policy*, vol. 159, p. 105892, Jan. 2024, doi: 10.1016/j.marpol.2023.105892.

[15] P. K. Patro, R. Jayaraman, K. Salah, and I. Yaqoob, "Blockchain-Based Traceability for the Fishery Supply Chain," *IEEE Access*, vol. 10, pp. 81134–81154, 2022, doi: 10.1109/ACCESS.2022.3196162.

[16] E. Cruz and A. Rosado Da Cruz, "Using Blockchain to Implement Traceability on Fishery Value Chain:," in *Proceedings of the 15th International Conference on Software Technologies*, Lieusaint - Paris, France: SCITEPRESS - Science and Technology Publications, 2020, pp. 501–508. doi: 10.5220/0009889705010508.

[17] H. Zhang and F. Gui, "The Application and Research of New Digital Technology in Marine Aquaculture," *JMSE*, vol. 11, no. 2, p. 401, Feb. 2023, doi: 10.3390/jmse11020401.

[18] N. Alsharabi *et al.*, "Using blockchain and AI technologies for sustainable, biodiverse, and transparent fisheries of the future," *J Cloud Comp*, vol. 13, no. 1, p. 135, Aug. 2024, doi: 10.1186/s13677-024-00696-8.

[19] S. Ismail, H. Reza, K. Salameh, H. Kashani Zadeh, and F. Vasefi, "Toward an Intelligent Blockchain IoT-Enabled Fish Supply Chain: A Review and Conceptual Framework," *Sensors*, vol. 23, no. 11, p. 5136, May 2023, doi: 10.3390/s23115136.

[20] R. A. I. Pratiwi, L. A. Fani, and F. Kusasi, "Blockchain Technology in Fisheries Industry: A Systematic Literature Review," *BIO Web Conf.*, vol. 134, p. 05004, 2024, doi: 10.1051/bioconf/202413405004.

[21] N. Alsharabi *et al.*, "Using blockchain and AI technologies for sustainable, biodiverse, and transparent fisheries of the future," *J Cloud Comp*, vol. 13, no. 1, p. 135, Aug. 2024, doi: 10.1186/s13677-024-00696-8.

[22] S. Cao, H. Xu, and K. P. Bryceson, "Blockchain Traceability for Sustainability Communication in Food Supply Chains: An Architectural Framework, Design Pathway and Considerations," *Sustainability*, vol. 15, no. 18, p. 13486, Sep. 2023, doi: 10.3390/su151813486.

[23] R. M. Ellahi, L. C. Wood, and A. E.-D. A. Bekhit, "Blockchain-Driven Food Supply Chains: A Systematic Review for Unexplored Opportunities," *Applied Sciences*, vol. 14, no. 19, p. 8944, Oct. 2024, doi: 10.3390/app14198944.

[24] E. Cruz and A. Rosado Da Cruz, "Using Blockchain to Implement Traceability on Fishery Value Chain:," in *Proceedings of the 15th International Conference on Software Technologies*, Lieusaint - Paris, France: SCITEPRESS - Science and Technology Publications, 2020, pp. 501–508. doi: 10.5220/0009889705010508.

[25] U. Nisar *et al.*, "Unlocking the potential of blockchain technology in enhancing the fisheries supply chain: an exploration of critical adoption barriers in China," *Sci Rep*, vol. 14, no. 1, p. 10167, May 2024, doi: 10.1038/s41598-024-59167-4.

[26] M. Lei, L. Xu, T. Liu, S. Liu, and C. Sun, "Integration of Privacy Protection and Blockchain-Based Food Safety Traceability: Potential and Challenges," *Foods*, vol. 11, no. 15, p. 2262, Jul. 2022, doi: 10.3390/foods11152262.

[27] D. X. Khor *et al.*, "Food safety impacts of finfish and crustacean aquaculture on food security in Asia: -EN- -FR- Effets de la sécurité sanitaire des poissons et des crustacés issus de l'aquaculture sur la sécurité alimentaire en Asie -ES- Consecuencias para la seguridad alimentaria de Asia de la inocuidad de peces y crustáceos procedentes de la acuicultura," *Rev. Sci. Tech. OIE*, vol. 38, no. 2, pp. 629–639, Sep. 2019, doi: 10.20506/rst.38.2.3009.

[28] S. Rana, "Blockchain-based Traceability and Transparency in Agricultural Supply Chains: Challenges and Opportunities," *TURCOMAT*, vol. 11, no. 3, pp. 1948–1956, Dec. 2020, doi: 10.17762/turcomat.v11i3.13591.

[29] A. K. Farmery, A. White, and E. H. Allison, "Identifying Policy Best-Practices to Support the Contribution of Aquatic Foods to Food and Nutrition Security," *Foods*, vol. 10, no. 7, p. 1589, Jul. 2021, doi: 10.3390/foods10071589.

[30] T. Asha Vijay and M. S. Raju, "Blockchain Applications in Fisheries," *E3S Web Conf.*, vol. 399, p. 07008, 2023, doi: 10.1051/e3sconf/202339907008.

[31] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges," *Journal of Cleaner Production*, vol. 260, p. 121031, Jul. 2020, doi: 10.1016/j.jclepro.2020.121031.

[32] C. E. Boyd, A. A. McNevin, and R. P. Davis, "The contribution of fisheries and aquaculture to the global protein supply," *Food Sec.*, vol. 14, no. 3, pp. 805–827, Jun. 2022, doi: 10.1007/s12571-021-01246-9.

[33] Y. Zhang, Y. Liu, Z. Jiong, X. Zhang, B. Li, and E. Chen, "Development and assessment of blockchain-IoT-based traceability system for frozen aquatic product," *J Food Process Engineering*, vol. 44, no. 5, p. e13669, May 2021, doi: 10.1111/jfpe.13669.

[34] Y.-J. Pan and H.-P. Shieh, "APPLICATION OF BLOCKCHAIN TECHNOLOGY IN AQUACULTURE MANAGEMENT," *Journal of Marine Science and Technology*, vol. 31, no. 3, Oct. 2023, doi: 10.51400/2709-6998.2701.

[35] S. Lal *et al.*, "Robot-assisted Aquaculture and Sustainable Seafood Production for Enhanced Food Security," *IJECC*, vol. 14, no. 2, pp. 215–220, Feb. 2024, doi: 10.9734/ijecc/2024/v14i23938.

[36] N. Tsolakis, R. Schumacher, M. Dora, and M. Kumar, "Artificial intelligence and blockchain implementation in supply chains: a pathway to sustainability and data monetisation?," *Ann Oper Res*, vol. 327, no. 1, pp. 157–210, Aug. 2023, doi: 10.1007/s10479-022-04785-2.

[37] E. B. Dompreh *et al.*, "Impact of adoption of better management practices and nutrition-sensitive training on the productivity, livelihoods and food security of small-scale aquaculture producers in Myanmar," *Food Sec.*, vol. 16, no. 3, pp. 757–780, Jun. 2024, doi: 10.1007/s12571-023-01415-y.

[38] Aba Mustapha, "Improving the quality of aquafeed for an effective food security in small scale African aquaculture," *World J. Adv. Res. Rev.*, vol. 7, no. 3, pp. 274–282, Sep. 2020, doi: 10.30574/wjarr.2020.7.3.0349.

[39] T. E. Carpenter, "Measuring the impacts of aquatic animal diseases: the role of economic analysis: -EN- -FR- Mesurer les impacts des maladies des animaux aquatiques : rôle de l'analyse économique -ES- Función del análisis económico para cuantificar las consecuencias de enfermedades de los animales acuáticos," *Rev. Sci. Tech. OIE*, vol. 38, no. 2, pp. 511–522, Sep. 2019, doi: 10.20506/rst.38.2.300.

[40] B. Leka (Moçka), D. Leka, and A. Malaj, "ENHANCING BANKING SYSTEMS THROUGH BLOCKCHAIN TECHNOLOGY: A CURRENCY SITUATION STUDY," *AIJES*, vol. 17, no. 2, pp. 105–109, Dec. 2023, doi: 10.15837/aijes.v17i2.6447.

[41] C. F. Durach, T. Blesik, M. Von Düring, and M. Bick, "Blockchain Applications in Supply Chain Transactions," *J of Business Logistics*, vol. 42, no. 1, pp. 7–24, Mar. 2021, doi: 10.1111/jbl.12238.

[42] O. Iermakova, I. Sedikova, and A. Dashian, "Prospects of Implementation of Blockchain Technology into Aquaculture Sector of Ukraine," *ees*, vol. 6, no. 2, pp. 29–37, Jun. 2022, doi: 10.31520/2616-7107/2022.6.2-3.

[43] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transportation Research Part E: Logistics and Transportation Review*, vol. 142, p. 102067, Oct. 2020, doi: 10.1016/j.tre.2020.102067.

[44] M. Kouhizadeh, S. Saberi, and J. Sarkis, "Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers," *International Journal of Production Economics*, vol. 231, p. 107831, Jan. 2021, doi: 10.1016/j.ijpe.2020.107831.

[45] N. Kshetri, "Blockchain and sustainable supply chain management in developing countries," *International Journal of Information Management*, vol. 60, p. 102376, Oct. 2021, doi: 10.1016/j.ijinfomgt.2021.102376.

[46] P. Katsikouli, A. S. Wilde, N. Dragoni, and H. Høgh-Jensen, "On the benefits and challenges of blockchains for managing food supply chains," *J Sci Food Agric*, vol. 101, no. 6, pp. 2175–2181, Apr. 2021, doi: 10.1002/jsfa.10883.

[47] F. Antonucci, S. Figorilli, C. Costa, F. Pallottino, L. Raso, and P. Menesatti, "A review on blockchain applications in the agri-food sector," *J Sci Food Agric*, vol. 99, no. 14, pp. 6129–6138, Nov. 2019, doi: 10.1002/jsfa.9912.

[48] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains," *Trends in Food Science & Technology*, vol. 91, pp. 640–652, Sep. 2019, doi: 10.1016/j.tifs.2019.07.034.

[49] N. Tsolakis, D. Niedenzu, M. Simonetto, M. Dora, and M. Kumar, "Supply network design to address United Nations Sustainable Development Goals: A case study of blockchain implementation in Thai fish industry," *Journal of Business Research*, vol. 131, pp. 495–519, Jul. 2021, doi: 10.1016/j.jbusres.2020.08.003.

[50] S. Stranieri, F. Riccardi, M. P. M. Meuwissen, and C. Soregaroli, "Exploring the impact of blockchain on the performance of agri-food supply chains," *Food Control*, vol. 119, p. 107495, Jan. 2021, doi: 10.1016/j.foodcont.2020.107495.

[51] A. Chandan, M. John, and V. Potdar, "Achieving UN SDGs in Food Supply Chain Using Blockchain Technology," *Sustainability*, vol. 15, no. 3, p. 2109, Jan. 2023, doi: 10.3390/su15032109.

[52] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-Based Soybean Traceability in Agricultural Supply Chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019, doi: 10.1109/ACCESS.2019.2918000.

[53] M. Alobid, S. Abujudeh, and I. Szűcs, "The Role of Blockchain in Revolutionizing the Agricultural Sector," *Sustainability*, vol. 14, no. 7, p. 4313, Apr. 2022, doi: 10.3390/su14074313.

[54] S. Fernandez-Vazquez, N. Álvarez, O. Leon, and J. Costas, "Investigating the Potential of Blockchain Technology for Improving Traceability in Agriculture," in *2023 Congress in Computer Science, Computer Engineering, &amp; Applied Computing (CSCE)*, Las Vegas, NV, USA: IEEE, Jul. 2023, pp. 452–457. doi: 10.1109/CSCE60160.2023.00081.

[55] P. Howson, "Building trust and equity in marine conservation and fisheries supply chain management with blockchain," *Marine Policy*, vol. 115, p. 103873, May 2020, doi: 10.1016/j.marpol.2020.103873.

[56] P. Liu, A. Hendalianpour, M. Hamzehlou, M. R. Feylizadeh, and J. Razmi, "Identify And Rank The Challenges Of Implementing Sustainable Supply Chain Blockchain Technology Using The Bayesian Best Worst Method," *Technological and Economic Development of Economy*, vol. 27, no. 3, pp. 656–680, May 2021, doi: 10.3846/tede.2021.14421.

[57] S. Menon and K. Jain, "Blockchain Technology for Transparency in Agri-Food Supply Chain: Use Cases, Limitations, and Future Directions," *IEEE Trans. Eng. Manage.*, vol. 71, pp. 106–120, 2024, doi: 10.1109/TEM.2021.3110903.

[58] R. Garrard and S. Fielke, "Blockchain for trustworthy provenances: A case study in the Australian aquaculture industry," *Technology in Society*, vol. 62, p. 101298, Aug. 2020, doi: 10.1016/j.techsoc.2020.101298.

[59] Y. Xu, X. Li, X. Zeng, J. Cao, and W. Jiang, "Application of blockchain technology in food safety control : current trends and future prospects," *Critical Reviews in Food Science and Nutrition*, vol. 62, no. 10, pp. 2800–2819, Apr. 2022, doi: 10.1080/10408398.2020.1858752.

[60] K. Yue and Y. Shen, "An overview of disruptive technologies for aquaculture," *Aquaculture and Fisheries*, vol. 7, no. 2, pp. 111–120, Mar. 2022, doi: 10.1016/j.aaf.2021.04.009.

[61] G. Lv, C. Song, P. Xu, Z. Qi, H. Song, and Y. Liu, "Blockchain-Based Traceability for Agricultural Products: A Systematic Literature Review," *Agriculture*, vol. 13, no. 9, p. 1757, Sep. 2023, doi: 10.3390/agriculture13091757.

[62] A. Alwi, N. A. Sasongko, Suprapto, Y. Suryana, and H. Subagyo, "Blockchain and big data integration design for traceability and carbon footprint management in the fishery supply chain," *Egyptian Informatics Journal*, vol. 26, p. 100481, Jun. 2024, doi: 10.1016/j.eij.2024.100481.

[63] A. F. Abdullah, H. C. Man, A. Mohammed, M. M. A. Karim, S. U. Yunusa, and N. A. B. M. Jais, "Charting the aquaculture internet of things impact: Key applications, challenges, and future trend," *Aquaculture Reports*, vol. 39, p. 102358, Dec. 2024, doi: 10.1016/j.aqrep.2024.102358.

[64] M. Correia *et al.*, "Integrated Multi-Trophic Aquaculture: A Laboratory and Hands-on Experimental Activity to Promote Environmental Sustainability Awareness and Value of Aquaculture Products," *Front. Mar. Sci.*, vol. 7, p. 156, Mar. 2020, doi: 10.3389/fmars.2020.00156.

[65] W.-T. Sung, I. G. T. Isa, and S.-J. Hsiao, "Integrated Aquaculture Monitoring System Using Combined Wireless Sensor Networks and Deep Reinforcement Learning," *Sensors and Materials*, vol. 36, no. 3, p. 1019, Mar. 2024, doi: 10.18494/SAM4660.

[66] S. Qiao, W. Yin, Y. Liu, and D. Li, "The evolution of food and nutrition supply patterns of marine capture and mariculture in China and its transformation coping strategies," *Front. Mar. Sci.*, vol. 11, p. 1478631, Oct. 2024, doi: 10.3389/fmars.2024.1478631.

[67] M. AlShamsi, M. Al-Emran, and K. Shaalan, "A Systematic Review on Blockchain Adoption," *Applied Sciences*, vol. 12, no. 9, p. 4245, Apr. 2022, doi: 10.3390/app12094245.

https://doi.org/10.31436/ijpcc.v11i1.503

ECG Signal Classification Using Hybrid and Non-Hybrid Learning Technologies

Asma Salim Yahya*, Naktal Moaid Edan

Department of Software, College of Computer Science and Mathematics, University of Mosul, Iraq

*Corresponding author asma_alkhairi@uomosul.edu.iq

(Received: 27th August, 2024; Accepted: 29th December, 2024; Published on-line: 30th January, 2025)

Abstract— Most arrhythmias caused by cardiovascular disorders disrupt the electrical activity of the heart, resulting in changes in the morphology of electrocardiogram (ECG) recordings. By analyzing different ECG patterns and comparing machine learning and deep learning techniques, this research aims to accurately identify twenty-nine different cardiac problems and sinus rhythm. The database contains 48 heart rate recordings at a frequency of 360 Hz for about 25 minutes for five classes, namely "N", "S", "V", "F", and "Q". Support Vector Machine (SVM), k-nearest neighbor (k-nearest neighbor) classifier, and random forest (RF) classifier were among the machine learning (ML) techniques used. Experimental results revealed that the random forest classifier achieved the highest classification accuracy, reaching 96.08%, while the support vector machine (SVM) achieved the lowest accuracy, reaching 88.9%. The study included deep learning approaches, namely convolutional neural networks (CNNs), hybrid deep learning models (CNN-LSTM), and recurrent neural networks of the long short-term memory (LSTM) type. Through a comparative analysis of the results of machine learning and deep learning, the best accuracy was achieved by the hybrid deep learning model LSTM-CNN, which achieved 97.25% with a kernel size of 3. Using the Sigmoid and SoftMax activation functions, the model achieved an accuracy of 95.12% and 97.32%, respectively, with the Adam activation function achieving an accuracy of 98.75%, to achieve the highest accuracy of the proposed model and find a balance between accuracy and speed classification. The main objective of this research is to implement a heart rate classification system from adult electrocardiograms using multiple machine learning and deep learning network architectures.

Keywords— Deep Learning, Machine Learning, ECG signals, Classification.

I. Introduction

Heart and blood vessel disorders, including coronary heart disease (CHD), which is characterized by the constriction of blood arteries supplying the heart muscle, are included in the category of cardiovascular illnesses (CVD). Other examples are congenital heart disease, which describes anatomical defects evident from birth, and rheumatic heart disease, which is caused by rheumatic fever induced by streptococcal bacteria and leads to damage to the heart muscle and valves. Globally, cardiovascular disease (CVD) is the primary cause of death. An electrocardiogram, or ECG, is a diagnostic test that captures the electrical activity of the heart and identifies any irregularities. Small electrical impulses generated by the heart travel through spindles to activate the heart's muscles 66.10% [1]. The ECG shows these impulses as a tracing on paper, allowing medical professionals to understand them. Over 17.9 million deaths annually, or 31% of all deaths worldwide, are attributed to it, making it the leading cause of death. 85% of these deaths are linked to cerebrovascular accidents and myocardial infarctions. People with cardiovascular disease or those who have a high risk of getting it because of several risk factors, such as diabetes or hypertension, should be helped to identify the disease's causes and receive treatment with appropriate medication and counselling.

Since its invention, an electrocardiogram, or ECG, has been the main diagnostic tool for determining a variety of heart issues. Recent developments have increased the ECG's significance. It is a commonly used, non-invasive, and reasonably priced diagnostic tool.

Electrocardiography, or ECG, is a diagnostic tool that is widely used to analyse cardiac function. It captures changes in the electrical activity of the heart over time and yields vital physiological data. ECG signals are periodic because they are made up of a wave sequence that repeats throughout time. This pattern consists of a P wave, which is then followed by Q, R, and S waves (which constitute the QRS complex), and a T wave therapy with appropriate medication and counselling comes last. [2], as illustrated in Figure 1.

ECGs can now be interpreted by computers in addition to people, thanks to recent developments in computing and improved technology. ECGs are frequently very lengthy, requiring the doctor to read them beat by beat. This is a laborious and time-consuming procedure that can be challenging for less experienced medical professionals. Replacing it with systems that can accurately classify ECG data and provide counselling and appropriate medications can help this process [4]. Early detection of cardiac arrhythmias is essential for the diagnosis of heart disease and the prompt administration of treatment to patients. Long ECG recordings are difficult for doctors to analyse quickly because the average human eye is not designed to recognize the morphological changes in the ECG signal. For this reason, computer-aided diagnostics are desperately needed. Given the wide range of medical applications where this problem may occur, automated ECG classification is extremely important [5]. The automatic processing of the ECG signal encounters a significant challenge due to the substantial heterogeneity in the morphological and temporal properties of ECG waveforms among different patients, as well as within the same individuals [6]. The primary disadvantage of these ML methods is that they rely on manually extracted features therefore he was numerous machine learning (ML) solutions available for analysing and classifying ECG data at present. The challenge at hand pertains to the potential inability to identify the most appropriate features that will yield optimal classification accuracy. One of the suggested remedies involves the implementation of deep learning.

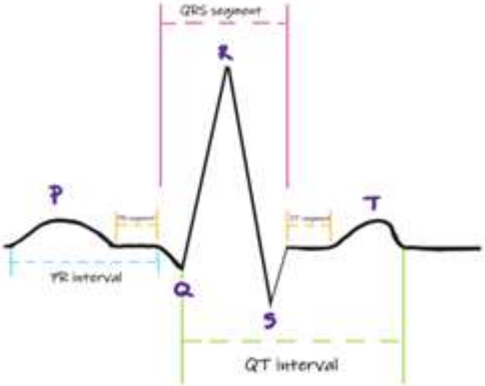


Fig. 1 Normal Electrocardiogram [3]

Architectures, in which the initial layers consist of long-memory LSTM layers designed to identify temporal features inherent in the input signal. Furthermore, the ultimate determination of heartbeat classes is entrusted to fully connected FCN layers to determine the pulse class.

II. Research Review

Recent studies have used deep learning and machine learning approaches to analyze ECG data to detect cardiovascular diseases. Abdullah et al was given [7] A thorough overview of IML approaches' applications in healthcare. Unfortunately, there is just one article that discusses using IML for heart disease categorization based on ECG signals. In a similar vein, Rasheed and colleagues [8] surveyed the research on interpreting ECG signals using IML and found only one study. Nonetheless, they justify their choices with a thorough analysis of IML approaches in their explanation of multi-fusion and multi-modal medical image segmentation, Yang et al. [9] demonstrated the advantages of machine learning (ML) interpretable approaches. Stiglic et al. [10] contrasted this with an emphasis on feature importance-based machine learning (ML) explanations.

A thorough overview of IML approaches' applications in healthcare was given by Abdullah et al. [11] and provided a comprehensive theoretical analysis of the popular IML methods now in use. Unfortunately, there is just one article that discusses using IML for heart disease categorization based on ECG signals. In a similar vein, Rasheed et al. [12] reviewed the literature on IML-based ECG signal interpretation and discovered just one report. However, they provide a comprehensive examination of IML techniques to support their decisions.

The DL-based Electrocardiogram arrhythmia classification pipeline relies heavily on the DL model design. When it comes to deep learning models, the architecture is multi-level or multi-layer, with each layer serving as an extractor of features that can improve its ability to summarize signal properties over time. The selected studies' DL classification models can be broadly classified into four categories: convolutional neural networks (CNNs), recurrent neural networks (RNNs), transformer, "hybrid" (combining different DL models), and "others" (representing less popular models like restricted Boltzmann machines and deep-belief networks), all based on the intrinsic properties of the major feature extractor within the neural networks. Here we present a comprehensive review of such DL algorithms for ECG arrhythmia categorization [13]. Classification of CNNs into 1D and 2D CNNs is based on the number of spatial domain filtering directions of the convolutional filters. To be more precise, 1D CNN filters travel in one way (the feature dimension) while 2D CNN filters go in two directions (the filtering axes) [14]. In their explanation of multi-fusion and multi-modal medical image segmentation, Yang et al. [15] demonstrated the advantages of machine learning (ML) interpretable approaches. Stiglic et al. [16] contrasted this with an emphasis on feature importance-based machine learning (ML) explanations. The CNN can work with any sampling rate for ECG signals. To categorize 2, 5, and 20 different kinds of cardiac illnesses, Stiglic et al. [10] use 1D CNNs and take few-shot learning into account due to the short dataset size. Contrarily, 2DCNN primarily considers inputs that resemble images, like the spectrogram in addition to the scalogram of an electrocardiogram (ECG). Electrocardiogram (ECG) signal classification makes use of a traditional 2D convolutional neural network (CNN), namely, AlexNet [17]. The 2D grey-level pictures with dimensions of 15 x 15 are simply converted from the 1D ECG plot in [18] and used as input in the two-dimensional CNN.

RNN, or Recurrent Neural Network, is a sort of Deep Learning structure that takes into consideration the temporal relationship of feature sequences [19]. It obtains an advantage in extracting hidden statistical information of ECG features by employing the RNN, which makes it more responsive to the temporal properties of the input sequences [20]. In addition, long short-term memory (LSTM), an enhanced version of the recurrent neural network (RNN), has become more popular than the traditional RNN due to its superior capacity to evaluate time series data [13]. A 6-layer Long Short-Term Memory (LSTM) model is created in [21] to autonomously detect Premature Ventricular Contractions (PVC) using Electrocardiogram (ECG) sequences. Moreover, a bidirectional LSTM (BiLSTM) is a specific kind of LSTM that includes two LSTMsFor ECG classification, the BiLSTM model in [20] was used with retrieved ECG wave statistics in the temporal dimension. The amplitudes of the Q- and R-waves, the RR and QR intervals, and the ST segment starting point are among these statistics. Watson [22], a 2D BiLSTM is employed to detect atrial fibrillation (AF) by analyzing the spectrogram of electrocardiogram (ECG) signals. The input characteristics consist of the frequency components at each time instance. He suggests identifying atrial fibrillation (AF) by use of a Bidirectional Long Short-Term Memory (BiLSTM) model that receives an input of a sequence of RR intervals. To sum up, time-varying pulse statistics, time-frequency representation of the ECG, and raw ECG sequences can all be used as input sequences for RNNs. Numerous studies propose integrating several DL models into a single DL network for the categorization of ECG arrhythmias. For example, [23] combines CNN and RNN to create an encoder-decoder framework for heartbeat classification. CNNs are utilized for feature extraction, while RNNs are employed to convert the extracted features into their appropriate categories. More instances of combining CNN and LSTM with BiLSTM can be found in [24], in which CNNs are stacked in front of LSTM/BiLSTM components to extract features.

Recurrent Neural Networks, or RNNs, are a type of Deep Learning structure that considers feature sequence temporal relationships [25]. It gains an advantage in extracting hidden temporal information of ECG features by applying the RNN, which also makes it more responsive to the temporal properties of the input sequences. Furthermore, because of its greater ability to analyze time series data, long short-term memory (LSTM), an improved recurrent neural network (RNN), has gained popularity over the more conventional RNN [26]. In [27], a 6-layer Long Short-Term Memory (LSTM) model is developed to use Electrocardiogram (ECG) sequences to automatically identify Premature Ventricular Contractions (PVC). Furthermore, a particular sort of LSTM that consists of two LSTMs is called a bidirectional LSTM (BiLSTM).

III. Materials and Methods

A. *Applications of Deep Learning in 3D Printing*

The data used comes from the MIT-BIH repository (The Massachusetts Institute of Technology - Beth Israel Hospital). This database contains 48 recordings of heartbeats at a frequency rate of 360 Hz for approximately 30 minutes from 47 different individuals and annotated by a minimum of two cardiologists according to the five classes, namely 'N', 'S', 'V', 'F', and 'Q'.

The MIT-BIH cardiac arrhythmia Dataset contains samples that have been resized, down sampled, and padded at zeroes if needed to a fixed dimension of 188, as stated in the Kaggle dataset note. The classes, namely 'N', 'S', 'V', 'F', and 'Q', each represented by a unique numerical value: 0, 1, 2, 3, and 4, respectively. The description is as follows [28]: N - Regular cardiac contraction, S - Supraventricular preterm or as ectopic pulse (atrial or nodal) V- Ventricular premature contraction (VPC) F- The F represents the fusion of a ventricular beat with a regular beat. Q - Uncategorizable beat. Figure 2. shows the sampling of each class.

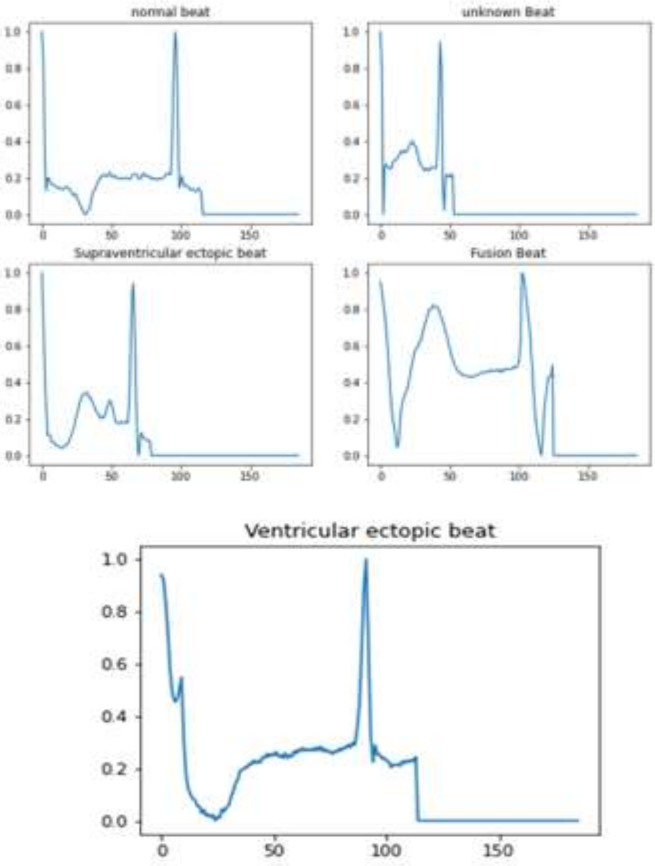


Fig. 2 Sampling of Each ECG Class [28]

1) Pre-Processing

Preprocessing of the data has been done to see if it needs to be cleaned. Clean data is required for model fitting in the following steps. A dataset's missing values can have an impact on how well a classifier built using that dataset as a training sample performs. Numerous approaches can be used to deal with missing data. In this work, we examine missing values using the (msno) matrix to display the dataset histogram and the is-null and not-null Pandas Data Frame functions. Then, we use the drop-Na (dropna) method to remove rows that contain null values. Unless the in-place option is set to True, the drop-Na method creates a new data frame object; in that case, the drop-Na function removes the previous data

2). Data Augmentation

To effectively train the model, it is necessary to standardize the level of augmentation for all the inputs. Due to the presence of bias in our data, it is necessary to employ data augmentation techniques to mitigate bias achieve equitable data distributions and improve the accuracy of models in classification. We have created two augmentations along with wrapper classes to facilitate their usage. It is important to note that these augmentations are generated randomly, resulting in two layers of randomization in the development of fresh input.

3) Dataset Balancing

The dataset is rather unbalanced. Therefore, we must up-sample every class. Although class F (fusion of ventricular and normal beat b) may overfit, this will have the same effect on the model as other classes. Consequently, it has been resampled for each group to acquire 20,000 observations for each class.

4) Feature Extraction by Machine Learning

The supervised approach recognizes ECG signals based upon several extracted features, which are then compared to a baseline learnt model. This comparison helps to establish if the ECG signal to normal or arrhythmia. The supervised techniques label a new exemplar as normal if the example baseline learnt model. This comparison helps to establish if the ECG signal to normal or arrhythmia. The supervised techniques label a new exemplar as normal if the example lies within the range of normality; otherwise, the exemplar is marked as abnormal. By using a few of the widely used machine learning approaches for threat detection [29].

The machine-learning techniques utilized in the performance appraisal model through the supervised method of ECG signal detection are based on several extracted features. Algorithms are described as three machine-learning used in the performance appraisal model namely SVM, RF and KNN. The test results are shown in Table I.

TABLE I.
MACHINE LEARNING CLASSIFICATION RESULTS OF ECG SIGNALSFOR MIT-BIH DATASET.

		SVM	RF	KNN
Accuracy		91.27	96.08	93.03
Precision (%)	0	85.16	98.12	86.09
	1	70.01	72.23	77.12
	2	35.82	85.06	45.22
	3	85.06	93.47	81.62
	4	16.56	77.98	55.81
Recall (%)	0	90.23	98.07	90.33
	1	82.01	84.10	77.49
	2	90.99	89.23	92.07
	3	93.21	86.16	82.12
	4	94.08	90.45	92.39
F1-Score (%)	0	90.25	90.47	93.08
	1	56.86	71.03	64.64
	2	88.39	90.15	83.14
	3	37.12	56.03	66.22
	4	87.45	88.09	92.05

From Table I it was clear that RF achieved the highest classification results, which gained an accuracy higher of 96.08% than the random forest classifier, It also achieved the highest precision for 4 classes (known Beat, unknown Beat, Ventricular ectopic beat and Supraventricular ectopic beat) and achieved the highest Recall for Normal beat class and the highest F1 score for 2 classes (Unknown Beat and Ventricular ectopic beat). While achieving the Support Vector Machine (SVM) classifier's highest recall accuracy of classification at 91.27% for 2 classes (Unknown Beat and Fusion Beat).

5) Feature Extraction by Deep Learning

In this part, we analyze the classification performance between the 3 DL models namely CNN, LSTM and CNN-LSTM. However, these models failed to gain good results (or even very bad results by the LSTM model), so modified and redesigned models to be more suitable to ECG classification and gain accuracy and higher results in classification this is done by hybridizing it with a convolutional neural network, and the models are also tested with the same input as in ML test and the test results are shown in Table II.

From Table II the higher accuracy in classification is achieved by the hybrid (CNN-LSTM) model while the second good results have been achieved by the CNN model, while the LSTM model achieved lower classification results. The hybrid (CNN-LSTM) model achieves the highest accuracy rather to other ML and DL models which achieved 97.25% accuracy. On the other hand, CNN achieved the second highest accuracy than other ML and DL models which achieved 96% accuracy LSTM is the worst result compared with others, to show results selected hybrid CNN-STM model is a preferred model for classifying ECG signals.

IV. Experimental Setup and Performance Metrics

The test results were analysed using six widely used assessment techniques, or "performance measures," because they were combined to assess the overall performance of the model. These methods included f1 score, accuracy, memory, and precision. The confusion matrix provides a comprehensive view of your model's performance. The test's results allow for the evaluation of a classification model's performance and the identification of problems it encounters when applied to a binary classification task such as the one under investigation, it would have a 2 x 2 matrix of values, as shown below [30][31]: TP = Positive: Occurrence of positive positivity. TN = True Negative: Positive classes were predicted correctly. FP = incorrectly signed geolocation as came rows. FN = false negative: correctly predicts positive signs.

Accuracy= (TP+TN)/(TP+TN+FP+FN).

Precision= TP/(TP+TN).

Recall= TP/(TP+FN).

F1 Score= (2(precision*recall))/((precision recall)).*

6) *Optimization Algorithms on the Classification Performance for the CNN-LSTM Model.*

Training Parameters and Optimization Algorithms can affect classification accuracy. Hence, it has been studying several parameters and optimization algorithms that can be used in the CNN-LSTM model and find the optimum value that can be used.

TABLE II.
DEEP LEARNING CLASSIFICATION RESULTS OF ECG SIGNALS.

		CNN	LSTM	CNN-LSTM
Accuracy		96	79.05	97.25
Precision (%)	0	97.15	55.09	97
	1	75.08	71.26	70
	2	95.11	80.14	96
	3	78.88	70.65	81
	4	97.09	82.56	98.09
Recall (%)	0	96.05	70.66	97.01
	1	80.05	62.11	83
	2	94.34	35.00	97
	3	82.16	88.02	85
	4	98.36	75.17	97.09
F1-Score (%)	0	98	55.23	98.25
	1	82.48	67.92	79
	2	96.09	55.84	94
	3	70.05	81.15	92
	4	97	81.09	98.03

B. *Kernel Size Effects*

This section examines the impact of kernel size variation on the efficacy of training. Four kernel sizes (1), (3), (5), and (7) have been evaluated. Twenty-five epochs are designated as the training epoch, with ten stages comprised of each epoch. The test for two datasets is described previously and the results are shown in Table III.

TABLE III
CLASSIFICATION RESULTS FOR DIFFERENT KERNEL SIZE AND ECG DATASET.

Kernel size	Validation Accuracy	Recall	Precision	F1-score
1	0.8314	0.8145	0.8345	0.8262
3	0.8549	0.9418	0.9355	0.9336
5	0.9449	0.9512	0.8889	0.8735
7	0.8310	0.8415	0.8402	0.8111

The training and validation results for the CNN model for the ECG database are shown in Figure 3.

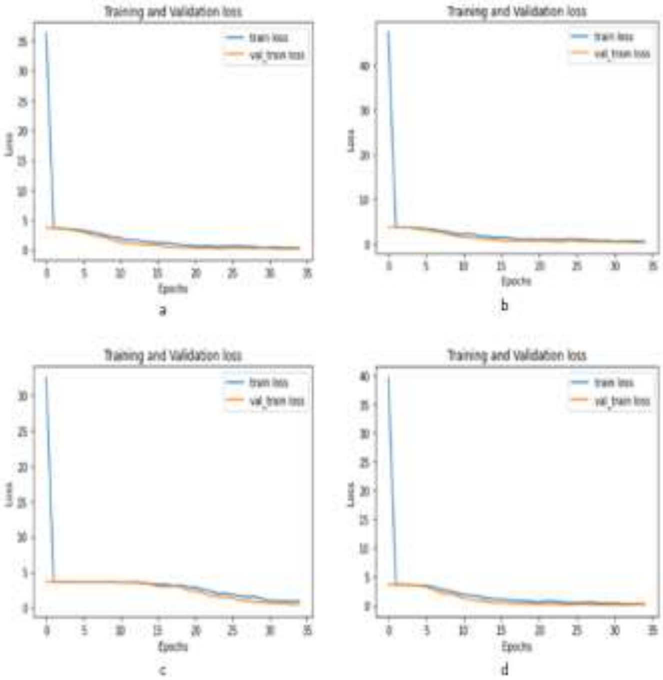


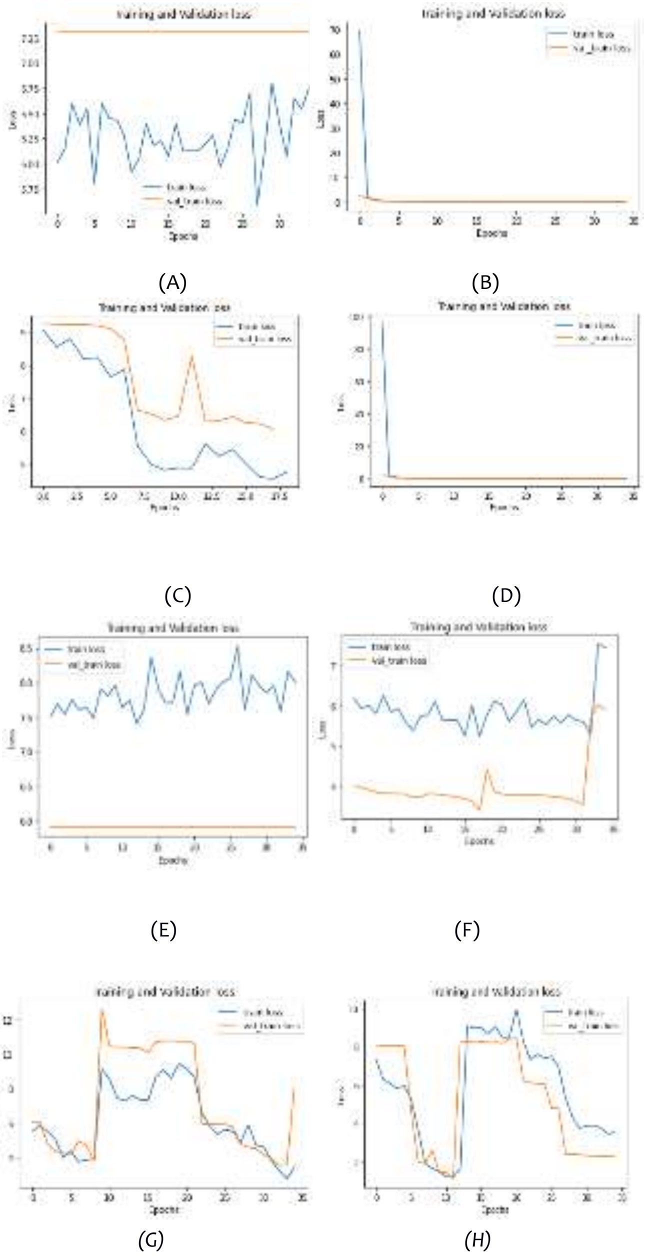
Fig. 3 Training and Test Loss for Various Kernel Sizes for ECG Database. 1 Kernel Size, (B) 3 Kernal Size, (C) 5 Kernel Size, (D) 7 Kernel Size

C. Activation Function Effects

In this part, we used the optimal kernel size of 5, we examined the impact of employing various activation functions for the output layer. For this test, four common 4 activation functions from keras have been employed, including SoftMax, sigmoid, Relu, tanh, and Softplus. Table IV and Figure 4 display the results of the tests.

TABLE IV.
THE RESULTS WITH SEVERAL ACTIVATION FUNCTIONS.

Activation Function Type	Test Accuracy	Recall	Precision	f1-score
softmax	0.9732	0.9780	0.9735	0.9756
sigmoid	0.9512	0.9418	0.9355	0.9336
relu	0.0319	0.9631	0.0328	0.0111
tanh	0.0274	0.9741	0.0267	0.0018
soft plus	0.0382	0.9371	0.0383	0.0034



(A) (B) (C) (D) (E) (F) (G) (H)

Fig. 4 ECG Classification Results with Various Activation Functions (A) Tanh, (B) Sigmoid, (C) Softmax, (D) Relu, (E) Softsign, (F) Softplus, (G) Elu, (H) Selu.

Based on the data presented in Table IV the validation and training loss of the ECG database indicate that the model performs well when using the activation function of the sigmoid and the softmax activation function. The validation and training loss consistently reduce and become stable at certain times (at 5 epochs), indicating a good fit. Models with alternative activation functions experience issues with both overfitting and underfitting, as well as a lack of stability. The variation in loss of training is usually ascribed to the presence of disappearing or exploding gradients. It is clear that only sigmoid and SoftMax, two popular activation functions, work well and produce positive results. On the other hand, all other activation functions lead to overfitting and produce notably low accuracy. Even though both perform better in the provided dataset, it is clear that SoftMax performs more accurately than Sigmoid while training the electrocardiogram (ECG) database. It has been concluded that the sigmoid and SoftMax activation functions are appropriate choices for this model.

D. *Optimization Function Effects*

The most efficient activation function, SoftMax, has been utilized to assess how different optimization functions affect the classification accuracy of the suggested model. The seven activation functions that are tested are Adam, Adamax, Adagrad, Nadam, SGD, Ftrl, and RMSprop. TABLE V presents the test results. We set the epoch to 100 in this test so that the accuracy algorithm could compare and optimize them over a longer time frame.

TABLE V.
ECG CLASSIFICATION RESULTS WITH SEVERAL OPTIMIZATION FUNCTIONS.

Activation Function Type	Validation Accuracy	Recall	Precision	F1-score
Adamax	0.9870	0.99	0.9812	0.9813
Adam	0.9875	0.9905	0.9872	0.9885
Nadam	0.9845	0.9815	0.9835	0.9841
Adagrad	0.9715	0.8309	0.9731	0.9721
SGD	0.2105	0.8580	0.1205	0.1524

Based on the results in Table V. the majority of optimization functions perform well and obtain high accuracy for ECG datasets, except for Ftrl and SGD. Specifically, these two approaches produce low accuracy when used with the ECG dataset. Nevertheless, the values of Adam and Adamax are relatively high and they are near to each other. As a result, we decided that Adamax is the best approach for the proposed model.

IV. CONCLUSION

After conducting an inquiry on the impact of various training settings on the accuracy as well as the stability of the DL models, and can summarize the findings as follows: The stability and precision of the findings can be greatly impacted by choosing an appropriate kernel size. Our results suggest that for these kinds of networks, a kernel size of 5 is more appropriate. By contrasting the outcomes of deep learning and machine learning, Using Sigmoid and SoftMax activation functions, the hybrid deep learning model LSTM-CNN achieved the highest accuracy in ECG classification, reaching 98.10% with a kernel size of 5. Adam's activation function achieved 98.75%, the highest accuracy for the proposed model, and a balance between accuracy and speed was achieved. The choice of activation function greatly impacts the training and testing results, it has been selected Adam as the preferred method for training the electrocardiogram (ECG) database. The use of state-of-the-art fast computational ML algorithms, such as SVM, DT, and KNN and compared with high complexity DL algorithms in ECG classification applications to determine the most preferred method that can give a balance between performance and speed. Figure 1 shows that the training and test losses of the ECG database and the dataset that is provided for all kernel sizes have a good match, with both training and testing losses decreasing as they stabilize at a given time (about one epoch). Following that, it decreased steadily until the 35 designated epochs came to an end. As a result, it is evident that the training and testing curve fittings, which begin at 25 epochs and remain steady until the conclusion, were similar to one another when the model employs a kernel size of the outcome goal of this research, that intend to implement a heartbeat classification system from adult ECGs by using several machine learning and deep learning network architectures.

ACKNOWLEDGMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] T. Gaziano, K. S. Reddy, F. Paccaud, and S. Horton, “Cardiovascular Disease,” *Dis. Control Priorities Dev. Ctries. (2nd Ed.*, no. Cvd, pp. 645–662, 2006, doi 10.1596/978-0-8213-6179-5/chpt-33.

[2] H. C. Kim, “Epidemiology of cardiovascular disease and its risk factors in Korea,” *Glob. Heal. Med.*, vol. 3, no. 3, pp. 134–141, 2021, doi: 10.35772/ghm.2021.01008.

[3] Mørk, M. S. (2022). *Cilostazol a medical treatment for bradycardia of cardiac origin in dogs* (Doctoral dissertation).

[4] X. Yang et al., “The highly-cited Electrocardiogram-related articles in science citation index expanded: characteristics and hotspots,” J. Electrocardiol., vol. 47, no. 5, pp. 738–744, 2014, doi: https://doi.org/10.1016/j.jelectrocard.2014.03.005.

[5] E. A. Ashley and J. Niebauer, *Conquering the ECG*. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK2214/

[6] K. Prashant, P. Choudhary, T. Agrawal, and E. Kaushik, “OWAE-Net: COVID-19 detection from ECG images using deep learning and optimized weighted average ensemble technique,” *Intell. Syst. with Appl.*, vol. 16, no. November, p. 200154, 2022, doi: 10.1016/j.iswa.2022.200154.

[7] T. A. A. Abdullah, M. S. M. Zahid, and W. Ali, “A review of interpretable ml in healthcare: Taxonomy, applications, challenges, and future directions,” *Symmetry (Basel).*, vol. 13, no. 12, pp. 1–28, 2021, doi: 10.3390/sym13122439.

[8] K. Rasheed, A. Qayyum, M. Ghaly, A. Al-Fuqaha, A. Razi, and J. Qadir, “Explainable, trustworthy, and ethical machine learning for healthcare: A survey,” *Comput. Biol. Med.*, vol. 149, no. September, p. 106043, 2022, doi 10.1016/j.compbiomed.2022.106043.

[9] G. Yang, Q. Ye, and J. Xia, “Unbox the black box for the medical explainable AI via multi-modal and multi-centre data fusion: A mini-review, two showcases and beyond,” *Inf. Fusion*, vol. 77, no. May 2021, pp. 29–52, 2022, doi: 10.1016/j.inffus.2021.07.016.

[10] G. Stiglic, P. Kocbek, N. Fijacko, M. Zitnik, K. Verbert, and L. Cilar, “Interpretability of machine learning-based prediction models in healthcare,” *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 10, no. 5, pp. 1–13, 2020, doi: 10.1002/widm.1379.

[11] T. A. A. Abdullah, M. S. M. Zahid, and W. Ali, “A Review of Interpretable ML in Healthcare: Taxonomy, Applications, Challenges, and Future Directions,” Symmetry 2021, Vol. 13, Page 2439, vol. 13, no. 12, p. 2439, Dec. 2021, doi: 10.3390/SYM13122439.

[12] K. Rasheed, A. Qayyum, M. Ghaly, A. Al-Fuqaha, A. Razi, and J. Qadir, “Explainable, trustworthy, and ethical machine learning for healthcare: A survey,” Comput Biol Med, vol. 149, p. 106043, Oct. 2022, doi: 10.1016/J.COMPBIOMED.2022.106043.

[13] A. A. Ahmed, W. Ali, T. A. A. Abdullah, and S. J. Malebary, “Classifying Cardiac Arrhythmia from ECG Signal Using 1D CNN Deep Learning Model,” *Mathematics*, vol. 11, no. 3, pp. 1–16, 2023, doi: 10.3390/math11030562.

[14] Á. T. Escottá, W. Beccaro, and M. A. Ramírez, “Evaluation of 1D and 2D Deep Convolutional Neural Networks for Driving Event Recognition,” *Sensors*, vol. 22, no. 11, pp. 1–21, 2022, doi: 10.3390/s22114226.

[15] G. Yang, Q. Ye, and J. Xia, “Unbox the black box for the medical explainable AI via multi-modal and multi-centre data fusion: A mini-review, two showcases and beyond,” Information Fusion, vol. 77, pp. 29–52, Jan. 2022, doi: 10.1016/J.INFFUS.2021.07.016.

[16] G. Stiglic, P. Kocbek, N. Fijacko, M. Zitnik, K. Verbert, and L. Cilar, “Interpretability of machine learning-based prediction models in healthcare,” Wiley Interdiscip Rev Data Min Knowl Discov, vol. 10, no. 5, p. e1379, Sep. 2020, doi: 10.1002/WIDM.1379.

[17] A. Y. Hannun *et al.*, “Cardiologist-level arrhythmia detection and classification in ambulatory electrocardiograms using a deep neural

network," *Nat. Med.*, vol. 25, no. 1, pp. 65–69, 2019, doi: 10.1038/s41591-018-0268-3.

[18] E. A. Ashley and J. Niebauer, "explained Euan A Ashley and Josef Niebauer explained".

[19] C. Antzelevitch and A. Burashnikov, "Overview of Basic Mechanisms of Cardiac Arrhythmia," *Card. Electrophysiol. Clin.*, vol. 3, no. 1, pp. 23–45, 2011, doi: 10.1016/j.ccep.2010.10.012.

[20] H. Liu *et al.*, "A large-scale multi-label 12-lead electrocardiogram database with standardized diagnostic statements," *Sci. Data*, vol. 9, no. 1, pp. 1–10, 2022, doi: 10.1038/s41597-022-01403-5.

[21] P. Wagner *et al.*, "PTB-XL, a large publicly available electrocardiography dataset," *Sci. Data*, vol. 7, no. 1, pp. 1–16, 2020, doi: 10.1038/s41597-020-0495-6.

[22] D. Watson, "Conceptual Challenges for Interpretable Machine Learning," *SSRN Electron. J.*, no. June, 2020, doi: 10.2139/ssrn.3668444.

[23] G. Hinton, "Deep belief networks," *Scholarpedia*, vol. 4, no. 5, p. 5947, 2009, doi: 10.4249/scholarpedia.5947.

[24] P. Sharma, M. Kumar, H. K. Sharma, and S. M. Biju, *Generative adversarial networks (GANs): Introduction, Taxonomy, Variants, Limitations, and Applications*, no. 0123456789. Springer US, 2024. doi: 10.1007/s11042-024-18767-y.

[25] C. Antzelevitch and A. Burashnikov, "Overview of Basic Mechanisms of Cardiac Arrhythmia," Card Electrophysiol Clin, vol. 3, no. 1, p. 23, Mar. 2011, doi: 10.1016/J.CCEP.2010.10.012.

[26] B. B. Sahoo, R. Jha, A. Singh, and D. Kumar, "Long short-term memory (LSTM) recurrent neural network for low-flow hydrological time series forecasting," Acta Geophysica, vol. 67, no. 5, pp. 1471–1481, Oct. 2019, doi: 10.1007/S11600-019-00330-1/METRICS.

[27] P. Wagner et al., "PTB-XL, a large publicly available electrocardiography dataset," Scientific Data 2020 7:1, vol. 7, no. 1, pp. 1–15, May 2020, doi: 10.1038/s41597-020-0495-6.

[28] S. Mukhopadhyay, S. Biswas, A. B. Roy, and N. Dey, "Wavelet-Based QRS Complex Detection of ECG Signal," vol. 2, no. 3, pp. 2361–2365, 2012, [Online]. Available: http://arxiv.org/abs/1209.1563

[29] H. A. Marzog and H. J. Abd, "Machine Learning ECG Classification Using Wavelet Scattering of Feature Extraction," *Appl. Comput. Intell. Soft Comput.*, vol. 2022, 2022, doi: 10.1155/2022/9884076.

[30] H. M and S. M.N, "A Review on Evaluation Metrics for Data Classification Evaluations," *Int. J. Data Min. Knowl. Manag. Process*, vol. 5, no. 2, pp. 01–11, 2015, doi: 10.5121/ijdkp.2015.5201.

[31] R. Mathur, C. P. Gupta, V. Katewa, D. S. Jat, and N. Yadav, Eds., "Emerging Trends in Data-Driven Computing and Communications," 2021, doi: 10.1007/978-981-16-3915-9.

https://doi.org/10.31436/ijpcc.v11i1.529

Assessing the Alignment of Automotive Privacy Practices with Malaysia's PDPA

Nur Shahirah Hafizah Mohd Shani, Hafizah Mansor
Department of Computer Science, Kuliyyah of ICT, International Islamic University Malaysia

*Corresponding author hafizahmansor@iium.edu.my

(Received: 24th December 2024; Accepted: 29th December, 2024; Published on-line: 30th January, 2025)

Abstract— Every day, the technology around us rapidly develops, and we see a global shift in the car industry. Despite the growth of car technology, we can see many data breaches in the car ownership life cycle. In one research by Mozilla, 84% of car brands surveyed reserve the right to share user data with third-party companies, and 76% can sell it. It has drawn a lot of attention in the car privacy industry as customers should have control over their data and privacy because of the different sensitivity levels of this data. In Malaysia, any connected device that handles personal data is subject to the Personal Data Protection Act 2010 (PDPA) which is an act that regulates the processing of personal data regarding commercial transactions. This study evaluates the compliance of automotive privacy policies with Malaysia's Personal Data Protection Act (PDPA), focusing on the privacy policies of Honda, Perodua, BMW, Nissan, Toyota, and Tesla. As connected car technologies become more prevalent, concerns regarding data privacy have intensified, necessitating strict adherence to privacy regulations. The study analyses these brands' privacy policies by extracting and evaluating keywords related to PDPA principles, such as data processing, security, retention, and data subject rights using Python keyword extraction. The extracted keywords are then used in the manual analysis for each privacy policy across PDPA. Findings reveal varying levels of compliance: Toyota emerges as the most compliant brand with a score of 2.571 out of 3, followed by Tesla at 2.285, indicating relatively high adherence to PDPA requirements. In contrast, Perodua shows the lowest compliance score at 1.428, highlighting critical gaps in data retention, security, and access principles. BMW, Honda, and Nissan demonstrate moderate compliance, scoring 1.857, 1.714, and 1.571, respectively. These results suggest that while some brands have made progress in aligning with PDPA principles, significant gaps remain in key areas, particularly in security, retention, and access, indicating a need for substantial policy revisions to improve data protection in the automotive sector.

Keywords— Automotive, PDPA, GDPR, Privacy Policy, Keywords, Compliance

I. Introduction

The rapid advancement of vehicle technologies, including connected cars and the Internet of Things (IoT), has transformed the automotive industry into a data-driven ecosystem. Modern vehicles now collect extensive personal and environmental data, raising significant privacy concerns. As car manufacturers adopt data-intensive technologies, ensuring the protection of user data has become a critical issue in the industry [1].

Despite claims of compliance with data privacy regulations, many car manufacturers fail to implement robust privacy measures. According to a report by the Mozilla Foundation, the automotive industry ranks as “the official worst category of products for privacy” ever reviewed, with most car brands drafting privacy policies but failing to enforce them effectively [2]. Data breaches affecting sensitive customer information are frequently reported, further exposing the vulnerabilities in current automotive privacy frameworks. Moreover, vehicle manufacturers often provide limited options for users to control how their personal data is collected, shared, and used.

From a consumer perspective, the level of engagement with privacy policies remains low. A survey conducted by the Pew Research Center found that only 9% of Americans consistently read privacy policies before agreeing to them, reflecting a widespread lack of awareness and understanding of privacy terms [3]. This passive acceptance raises critical questions about whether privacy policies in the automotive industry are truly effective or merely symbolic. Many consumers unknowingly provide blanket consent to data collection practices, leaving them vulnerable to unauthorised data use and privacy violations. This lack of transparency and awareness weakens consumer trust in automotive companies and the data protection frameworks that safeguard their privacy.

The compliance of automotive privacy policies also has broader societal implications. Privacy policies that are poorly implemented or inadequately enforced can lead to increased risks of data misuse, unauthorised sharing, and exposure to cyber threats. Conversely, robust privacy practices promote accountability, transparency, and trust, benefiting both consumers and society by reducing the risk of data breaches and ensuring that personal data is handled responsibly. Therefore, effective privacy compliance is crucial for fostering ethical data practices in the automotive industry.

Failing to comply with privacy regulations poses significant risks to car companies and users. For automotive companies, non-compliance can result in legal penalties, loss of customer trust, and damage to brand reputation. The financial consequences of regulatory fines under privacy laws such as the General Data Protection Regulation (GDPR) or the Personal Data Protection Act (PDPA) can be substantial. Furthermore, users are exposed to privacy risks such as unauthorised data access, identity theft, and loss of control over their personal information. Inadequate privacy practices can undermine consumer confidence in connected vehicles, affecting user adoption of new technologies and impacting the industry's growth.

However, compliance alone does not guarantee that privacy policies are properly enforced or implemented. There is a critical distinction between compliance, enforcement, and implementation in the context of privacy practices. While a company may formally comply with privacy laws by drafting privacy policies and including the necessary terms, enforcement mechanisms are often weak, and the actual implementation of privacy practices varies widely across companies. For instance, a company may claim compliance by providing users with privacy policies but fail to actively protect user data or address potential security vulnerabilities. This gap between compliance on paper and real-world enforcement remains a major challenge in ensuring data privacy in the automotive sector.

Therefore, for privacy policies to be effective, compliance must go beyond documentation to include meaningful enforcement and operational implementation of data protection measures. Companies must ensure that privacy frameworks are not merely symbolic but are actively monitored, audited, and enforced across all levels of operations. Without this, even companies that comply with privacy regulations may expose users to privacy risks due to inconsistent enforcement and incomplete implementation.

To address these privacy concerns, various legal acts and frameworks have been established worldwide. The European Union's GDPR has set a global standard for data privacy governance. Similarly, countries such as Japan, the United States, and Malaysia have enacted their own privacy laws, including Japan's Act on the Protection of Personal Information (APPI), California's Consumer Privacy Act (CCPA), and Malaysia's PDPA. These regulations provide legal guidance for organisations to structure and implement privacy policies that align with internationally recognised principles [4].

Despite the presence of such regulations, many automotive companies still struggle to apply privacy principles effectively. This study focuses on assessing the compliance of privacy policies from six prominent car brands (Honda, Perodua, BMW, Nissan, Toyota, and Tesla) against the seven core principles outlined in Malaysia's PDPA - i. General Principle, ii. Notice and Choice Principle, iii. Disclosure Principle, iv. Security Principle, v. Retention Principle, vi. Data Integrity Principle and vii. Access Principle. The research involves keyword extraction and policy evaluation to determine the extent of compliance and identify gaps between regulatory expectations and actual implementation.

The contribution of this study is both practical and academic. This study provides actionable insights for automotive companies to strengthen their privacy policies and improve compliance practices. This study aims to develop a comprehensive privacy compliance evaluation framework tailored specifically to the automotive sector.

The two research questions for this study are: 1. How well do automotive privacy policies align with the seven principles of Malaysia's PDPA? and 2. What gaps exist between current privacy policies and legal requirements as specified by the PDPA?

By addressing these questions, this research seeks to enhance data privacy practices in the automotive industry while promoting greater transparency and user understanding of privacy policies.

II. RELATED WORKS

The rapid growth of connected vehicles has brought significant privacy concerns due to the massive amounts of personal data car manufacturers collect. As connected vehicles gather vast amounts of sensitive data - ranging from GPS location to driving behaviour - privacy issues related to transparency, user control, and data security have emerged as major challenges. Many automotive companies lack clarity in disclosing data collection practices, and users are often provided with limited control over their personal information [5]. Furthermore, these concerns raise important questions regarding compliance with privacy acts and regulations, as automotive companies may face significant challenges in securing personal data, particularly in the face of frequent vulnerabilities in vehicle data-sharing platforms [7]. However, it is crucial for both manufacturers and users to recognise the importance of data protection. Users must be educated on the extent of personal data shared by vehicles and be empowered to make informed decisions regarding their consent [8], [20].

Connected vehicles, designed to enhance user experience through real-time data sharing, raise substantial privacy issues. The sheer volume of personal data collected, such as geolocation, driving behaviour, and vehicle status, requires manufacturers to implement stringent data protection measures. The lack of transparency regarding data collection practices is a significant challenge in the automotive industry. Many companies fail to fully disclose how data is used, where it is stored, and who has access to it, making it difficult for consumers to understand the implications of their data being collected. Furthermore, limited user control over their personal information, including the ability to opt-out of data collection, exacerbates privacy concerns [5], [6]. With data breaches and cybersecurity risks on the rise, automotive companies face increasing pressure to ensure the privacy and security of personal data [7].

To address these privacy challenges, compliance with data protection regulations such as the GDPR and Malaysia's PDPA is essential. The GDPR provides a comprehensive framework for managing personal data in the European Union, establishing privacy rights and data security as fundamental principles [13]. The PDPA, enacted in Malaysia in 2010, serves as a legal framework for regulating personal data protection in commercial transactions, ensuring that data controllers and processors meet specific requirements for data collection, processing, and retention [19].

However, many automotive companies struggle to create clear, enforceable privacy policies that comply with these regulations. A study by Smit indicates that before and after the enforcement of the GDPR, privacy policies in the automotive sector showed significant improvements in terms of transparency and user consent. These regulations emphasise the importance of obtaining informed consent for sensitive data, such as geolocation and driving behaviour. As a result, it is imperative for manufacturers to update their privacy policies to align with these legal standards and ensure better user transparency [9], [10]. The role of consent, data security, and the right to be forgotten is central to both the GDPR and PDPA, but enforcement remains inconsistent, particularly in regions like Malaysia, where many organisations face compliance challenges [12], [19].

The GDPR and PDPA are critical in ensuring that personal data is protected throughout its lifecycle, particularly in industries like automotive, where data collection is extensive. The GDPR's two main pillars—privacy rights and data security—are designed to ensure that individuals' personal data is handled ethically and securely. For instance, the regulation mandates businesses to seek explicit consent before collecting sensitive information and grants individuals the right to access, rectify, or delete their personal data [13].

The PDPA, similarly, regulates personal data collection and processing in Malaysia, focusing on principles such as Notice and Choice, Security, Retention, and Data Integrity. Despite its comprehensive structure, PDPA enforcement has been limited, and many businesses, including those in the automotive industry, have struggled with consistent implementation [19]. This challenge is highlighted by studies that reveal organisations often fail to define clear data collection and retention policies, leading to potential non-compliance with the Act [12]. Furthermore, while the GDPR has inspired similar privacy rules in various countries, such as Chile, Brazil, and Japan, the automotive industry must still adapt its practices to ensure compliance with local data protection laws like PDPA, especially when operating across international borders [13], [19].

Despite the comprehensive nature of both the GDPR and PDPA, many organisations, particularly in the automotive industry, face significant challenges in complying with these regulations. Key areas of difficulty include consent management, data portability, and ensuring the right to be forgotten. These provisions are difficult to implement due to the complexities of managing vast amounts of data collected from connected vehicles. In Malaysia, businesses often face challenges translating these regulatory requirements into actionable policies that are aligned with the PDPA. For example, obtaining user consent for data collection in connected vehicles requires clear communication of what data is being collected and how it will be used. Similarly, ensuring data portability and facilitating the right to be forgotten in the context of highly interconnected vehicle data systems presents considerable obstacles. The automotive sector, with its data-intensive technologies, must address these challenges to ensure full compliance with both GDPR and PDPA regulations [17].

To assess compliance with privacy regulations, methodologies such as keyword extraction have proven invaluable in evaluating the contents of privacy policies. By identifying and analysing relevant keywords, researchers can automate the process of determining whether a privacy policy aligns with the principles of data protection laws like GDPR and PDPA [14], [15]. Keyword extraction techniques are particularly useful in evaluating large datasets of privacy policies, enabling more efficient and comprehensive analysis of how automotive companies adhere to privacy regulations [16].

A framework using keyword-based methods for privacy policy enforcement in connected automotive systems has been proposed to enhance the compliance process [14], [15]. This framework can be applied to assess how automotive companies handle data collection, security, retention, and user consent, ensuring they meet the regulatory requirements set forth by laws such as the GDPR and PDPA. Moreover, studies such as McDonald's comparative policy analysis also provide foundational methods for analysing privacy policies and improving compliance evaluation [16]. In other paper, by Das Chaudhury and Choe further highlight that the adoption of regulatory regulation like the GDPR requires organizations to implement systematic compliance mechanisms, such as privacy-by-design approaches, to ensure that privacy safeguards are embedded throughout data processing activities [18].

The intersection of connected vehicles, privacy regulations, and data protection presents a complex landscape for the automotive industry. While regulations like the GDPR and PDPA provide robust frameworks for protecting consumer data, challenges in enforcement and compliance persist, particularly in the automotive sector. This literature review highlights the importance of data protection regulations and the growing need for automotive companies to ensure compliance with both local and international data privacy laws [13], [19].

Despite the existing frameworks, there are significant gaps in the enforcement of these regulations, particularly in countries like Malaysia where the PDPA faces implementation challenges. The literature also suggests that innovative methodologies, such as keyword extraction, can be instrumental in assessing privacy policy compliance. By addressing these research gaps and applying advanced methods to evaluate compliance, this study aims to contribute both practical and theoretical insights into improving data privacy practices in the automotive industry, ultimately helping to bridge the enforcement gaps in privacy policy compliance [10], [12], [13], [14].

III. METHODOLOGY

A. *RESEARCH DESIGN*

The study follows a qualitative content analysis framework, focusing on the textual evaluation of automotive privacy policies. This design is chosen because privacy policies are inherently text-based legal documents. The research assesses compliance by matching policy content against pre-defined PDPA criteria using both automated and manual methods. This dual approach ensures accuracy and context-aware analysis.

B. *DATA COLLECTION*

The study focuses on six major car brands: Perodua, BMW, Tesla, Nissan, Toyota, and Honda, selected based on their industry significance, market reach, and relevance to data privacy concerns. Perodua, Malaysia's top-selling local car brand, provides a crucial perspective on compliance with the Malaysian Personal Data Protection Act (PDPA). BMW enables an analysis of how global automotive brands adapt their privacy policies to meet international data protection standards. Similarly, Toyota recognised as the world's best-selling car brand with record-breaking sales in September 2024, was selected to explore how a globally dominant automotive manufacturer ensures privacy compliance across multiple jurisdictions. Tesla earned its place due to its notable privacy controversies, including being flagged by the Mozilla Foundation for poor privacy practices and untrustworthy Artificial Intelligence (AI) implementations. This makes Tesla an important case for understanding privacy risks in AI-powered connected vehicles. Nissan was chosen because of its reputation for collecting some of the most intrusive categories of personal data, such as "sexual activity," raising serious concerns about excessive data collection practices. Honda, positioned as a mid-tier performer in privacy assessments, provides a balanced perspective, bridging the gap between brands with strong privacy policies and those facing significant privacy challenges.

To collect and extract privacy policies from these car brands, the study employed web scraping using the BeautifulSoup library in Python. This method automated the retrieval of publicly available privacy policy text from the official websites of the selected brands. The process involved sending web requests using the "request" library and parsing the HTML content using BeautifulSoup for efficient text extraction.

However, for Tesla and Toyota, there is a restriction to directly retrieve the policies. Hence, we manually copied it from the official website and saved it into PDF and we read the PDF and extracted the keywords using Python.

C. *DATA PRE-PROCESSING*

Data pre-processing involved automated and manual methods to ensure the collected privacy policies were clean, standardised, and ready for analysis. This two-fold approach maximised accuracy and minimised noise in the data, enabling precise evaluation of compliance with data privacy regulations.

In pre-processing, we performed web scraping, text processing, and data analysis to assess the compliance of all car brands' privacy policies with Malaysia's PDPA. It starts by importing essential libraries: "requests" for fetching web content, "BeautifulSoup" for parsing HTML, "re" for text cleaning and pattern matching, "pandas" for data organisation, and "matplotlib.pyplot" for visualisation.

We fetched the privacy policy webpage of the selected car brands using requests.get() and checked if the retrieval was successful. If successful, then "BeautifulSoup" was used to parse the page's HTML content, extracting the relevant privacy policy section based on a specified HTML tag and class. If the section is found, the text is cleaned using a function that preserves key phrases, removes special characters, and standardises the text to lowercase.

We used the clean_text() function that prepares the privacy policy text for keyword matching by standardising its format. It starts by defining a list of important multi-word phrases like "up-to-date," "unauthorised access," and "correct personal data" to preserve them during text cleaning. To prevent these phrases from being split, it temporarily replaces spaces within them with underscores. The function then removes excess whitespace using a regular expression that condenses multiple spaces, tabs, or newlines into a single space. It also removes special characters, punctuation, and symbols while keeping only letters, numbers, underscores, and spaces. After cleaning, the function restores the preserved phrases by replacing underscores with spaces. Finally, it converts the entire text to lowercase, ensuring case-insensitive keyword matching. This process standardises the text, making it easier to search for relevant terms accurately.

D. *DATA ANALYSIS*

1) *Automated Data Analysis*

Following text cleaning in Section C, the system uses a Python function, count_keywords, to identify and count occurrences of the defined keywords. The function operates by scanning the cleaned text for exact matches of each keyword using regular expressions. It ensures that only whole-word matches are detected, avoiding partial or unintended matches, and tracks the keywords found in a list of unique matches.

The keyword counts are then analysed to determine compliance with each PDPA principle. A compliance percentage is calculated by comparing the number of matched keywords against the total number of keywords defined for a given principle (see Table 1).

TABLE I
SCORING TABLE

Range	Score	Compliance Level	Description
75% - 100%	3	High Compliance	Most or all relevant keywords are present
50% - 74%	2	Moderate Compliance	Partial Coverage
1% - 49%	1	Low Compliance	Limited references
0%	0	Non-Compliance	No relevant keywords found

This percentage quantifies the degree of alignment between the policy and PDPA requirements. Based on the calculated percentages, compliance levels are assigned using predefined thresholds: High Compliance (75%-100%), Moderate Compliance (50%-74%), Low Compliance (1%-49%), or Non-Compliance (0%) as stated in Table 1. Compliance scores are then calculated using a standard percentage formula: Compliance Score=Number of Keywords/Sum of Keyword Matches×100 This formula evaluates how well the policy aligns with each PDPA principle. Our formula assesses compliance by calculating the proportion of matched keywords for each principle, serving as a proxy for the presence of required provisions [21], [22]. If all relevant keywords are present, the principle receives a 100% compliance score. If some keywords are missing, the score reflects partial compliance based on the proportion of matched keywords. The scoring level is shown in Table 1.

This automated process provides a fast and objective assessment of the privacy policy's coverage of PDPA principles. However, it cannot interpret the context or accuracy of keyword usage, limiting its ability to fully evaluate compliance. As a result, a manual review is conducted to complement the automated findings, ensuring a thorough and context-aware analysis.

Next, to calculate the overall compliance, we take the level of compliance for each principle and compute the average:

Overall Compliance Level = ∑Compliance Levels/Number of Principles

This formula is used because averaging the compliance levels gives a single metric that summarises how well an organisation adheres to the principles outlined in privacy policies. This approach is valuable because it simplifies complex compliance assessments into a single, interpretable figure that reflects the organisation's overall adherence to privacy standards across multiple dimensions [23].

2) *Manual Data Analysis*

Due to the inability of automation to interpret context, a manual review was conducted to ensure a comprehensive and accurate assessment of compliance with the PDPA. This manual process began with an in-depth examination of the privacy policy for each car brand. For each matched keyword identified during the automated analysis, its context within the policy was carefully reviewed to determine alignment with the specific requirements and intent of the PDPA principles.

Further analysis was performed to identify synonyms or alternative expressions of missing keywords. This included checking for variations in grammatical forms, such as past or present tense, noun forms, or other terminology that may convey the same meaning as the original PDPA keywords. By analysing these linguistic variations, the review accounted for any differences in language that may still reflect compliance with PDPA standards.

Additionally, the entire privacy policy was thoroughly re-read to evaluate its overall structure, language, and alignment with PDPA principles. This holistic review ensured that the provisions in the policy collectively adhered to the regulatory framework, even if certain keywords were not explicitly present.

Compliance scoring was manually updated using the same scoring in Table 1 to reflect the findings from the contextual review. These manual adjustments provided a refined and accurate evaluation of the privacy policy's adherence to PDPA principles, addressing limitations in the automated methodology and ensuring a robust assessment of compliance.

IV. RESULTS AND FINDINGS

The findings indicate that the car privacy policy demonstrates moderate compliance, with notable strengths in data collection but room for improvement in areas such as data retention and security. Perodua, shows consistent compliance, particularly in data access and integrity, although greater transparency in data processing and third-party disclosures is needed. BMW exhibited high compliance, particularly in data security and retention practices, aligning well with PDPA requirements. In contrast, Nissan exhibited moderate to low compliance, particularly in areas related to data subject rights and third-party disclosures, highlighting potential vulnerabilities. Toyota displayed moderate compliance, with strengths in data collection and security but areas for improvement in retention and data integrity. Finally, Tesla demonstrated high compliance overall, excelling in data security and access, although gaps in data retention and third-party disclosures were observed.

A comprehensive set of keywords for each PDPA principle is defined. These keywords were derived by thoroughly studying the PDPA, consulting legal websites, and analysing privacy resources to ensure their alignment with the principles' intent. For example, the "General Principle" includes keywords like "processing," "personal data," and "consent," while the "Security Principle" focuses on terms such as "data protection," "unauthorised access," and "security measures." These keywords encapsulate the essential aspects of each principle, forming the backbone of the automated compliance evaluation. Table 2 defines all the keywords considered.

Next, in the case of Honda brand, the automated analysis for the General Principle showed a match of 3 out of 6 keywords, resulting in a compliance score of 50% and an initial score of 2. Upon manual review, it was observed that the missing keyword "sensitive personal data" was indirectly addressed in the policy under the section detailing the types of data being processed. This implied compliance with the General Principle's intent, leading to an adjustment in the score from 2 to 3, as documented in Table 3.

Similarly, for Perodua, the automated analysis identified two matched keywords—"data protection" and "protect"—under the Security Principle. However, manual analysis revealed that these terms were not used in the context of data security measures as required by the PDPA. Furthermore, a detailed review of the privacy policy found no mention of security principles. Consequently, the compliance level was adjusted from 1 to 0, as noted in Table 4.

The same methodology was applied across the privacy policies of other car brands. Each principle was carefully scrutinised to ensure that the context of matched keywords aligned with PDPA requirements, and any indirect or implied compliance was accounted for. Missing or irrelevant keywords were also verified to prevent overestimation of compliance. These adjustments provided a more accurate and nuanced evaluation of each brand's adherence to PDPA principles. The details of other adjustments can be referred to in Table 5 to Table 8 for BMW, Nissan, Toyota and Tesla respectively.

The findings reveal considerable variability in compliance levels, indicating partial alignment with the PDPA. Toyota demonstrated the highest overall compliance, with strong performance across principles such as Notice and Choice, Disclosure, Security, and Access. Tesla followed closely, with similar strengths but notable weaknesses in Retention and Data Integrity. Honda, BMW, Nissan, and Perodua showed lower levels of compliance overall, with significant deficiencies in Security, Retention, and Access, highlighting critical vulnerabilities. Figures 1 to 6 present the analysis for each car brand. Figure 7 shows the chart for each car brand across the compliance for each principle.

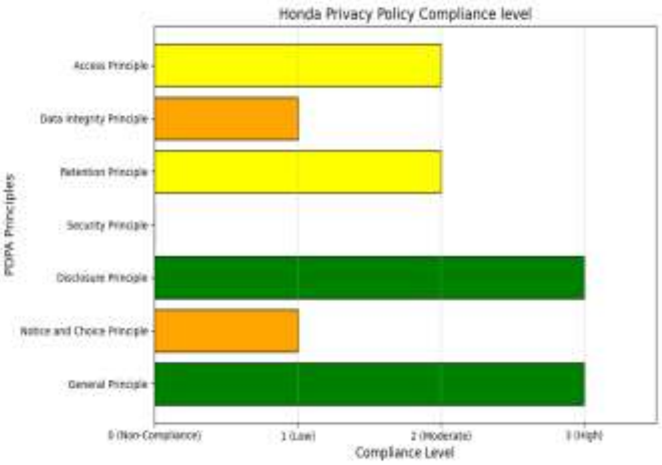


Fig. 1: Honda privacy compliance across PDPA

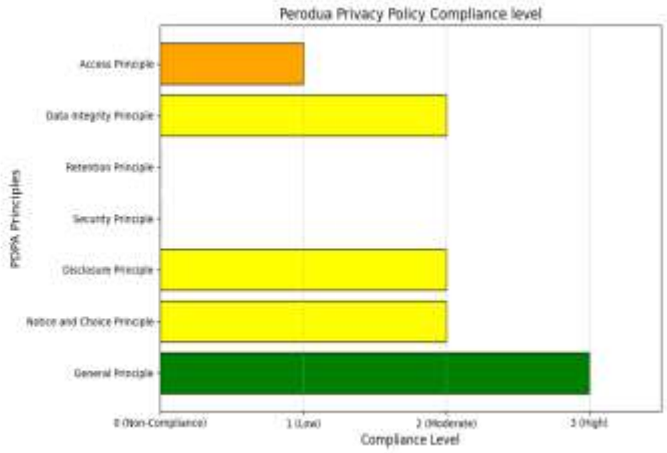


Fig. 2: Perodua privacy compliance across PDPA

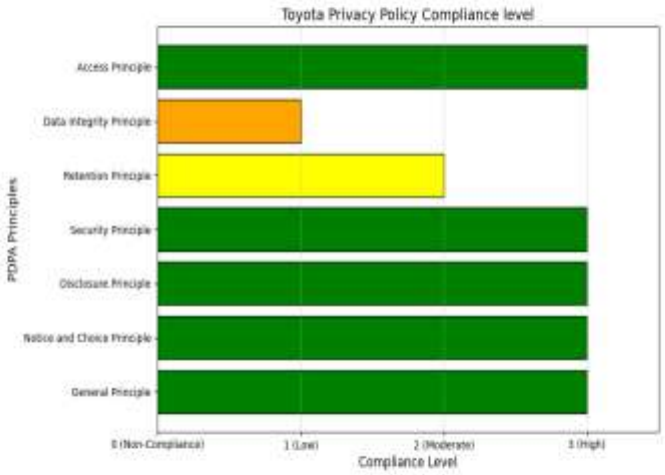


Fig. 5: Toyota privacy compliance across PDPA

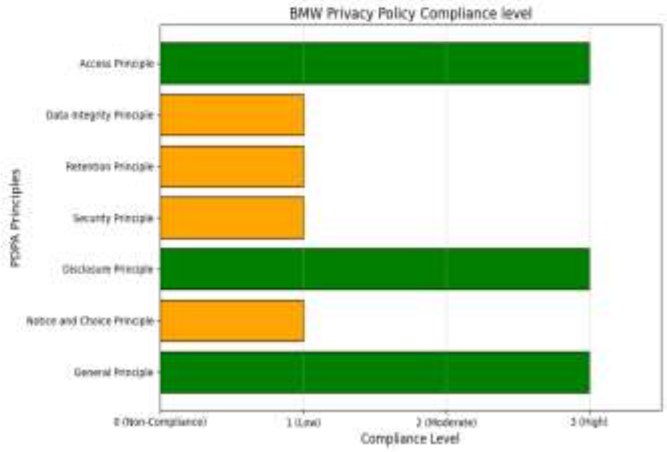


Fig. 3: BMW privacy compliance across PDPA

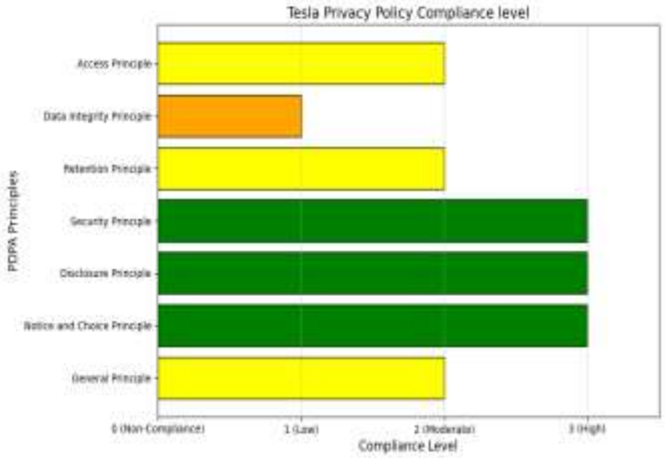


Fig. 6: Tesla privacy compliance across PDPA

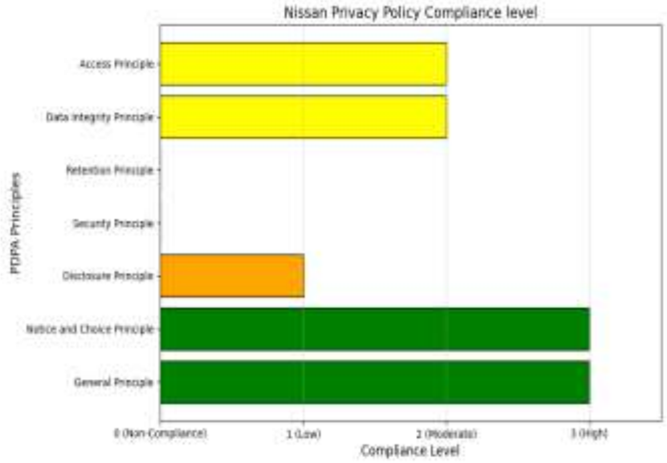


Fig. 4: Nissan privacy compliance across PDPA

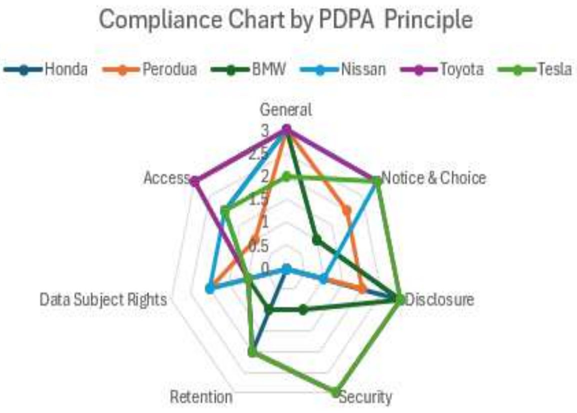


Fig. 7: Compliance chart by PDPA Principle

The analysis shows that most brands achieve moderate compliance with General, Notice and Choice, and Disclosure, showing efforts to inform users about data collection, processing purposes, and third-party relationships. However, principles like Security, Retention, and Data Integrity were poorly addressed across all brands except Toyota and Tesla, which provided some details on security measures and data retention. In contrast, brands like Perodua and Nissan failed to mention security practices, and most brands lacked clear policies on data retention timelines and deletion protocols.

The results answer the study's research questions by demonstrating that the automotive brands' privacy policies align only partially with the seven principles of the PDPA. Significant gaps exist in areas critical to data protection, such as Security, Retention, and Data Integrity. These gaps indicate an urgent need for automotive companies to enhance their privacy policies to ensure full compliance with PDPA requirements. The findings suggest that while progress has been made in areas like Notice and Choice, and Disclosure, there is still much work needed to address deficiencies in Security and Retention, which are essential for safeguarding personal data. The study underscores the importance of a comprehensive and uniform approach to privacy policy development within the automotive industry.

Looking at the data in Figure 8, Toyota emerges as the most compliant car manufacturer, with an overall compliance score of 2.571, indicating that it is better aligned with the privacy principles compared to others. Tesla follows with a score of 2.285, suggesting a relatively high level of compliance. On the other end, Perodua shows the lowest compliance level with a score of 1.428, highlighting areas for improvement in its privacy practices. Other companies like BMW (1.857), Honda (1.714), and Nissan (1.571) display varying levels of compliance.

The overall results conclude that most of the brands studied do not fully comply with the PDPA, and there is a clear need for revisions to their privacy policies. These revisions should focus on improving transparency, ensuring data retention practices align with legal requirements, and addressing the rights of data subjects, to better protect consumer privacy and align with Malaysia's data protection laws. For compliance to be effective, it must go beyond documentation to enforcement and practical implementation, ensuring that users' personal data is genuinely protected. Only by bridging this gap can the automotive industry achieve meaningful and lasting improvements in data privacy practices.

Nonetheless, the compliance evaluation framework developed in this study is adaptable and can serve as a baseline for assessing other car brands' privacy policies. The keyword extraction method and PDPA principles used in this analysis offer a scalable approach to measuring privacy policy compliance across the automotive industry. However, differences in legal environments, data collection practices, and enforcement mechanisms must be considered when applying these results to other brands.

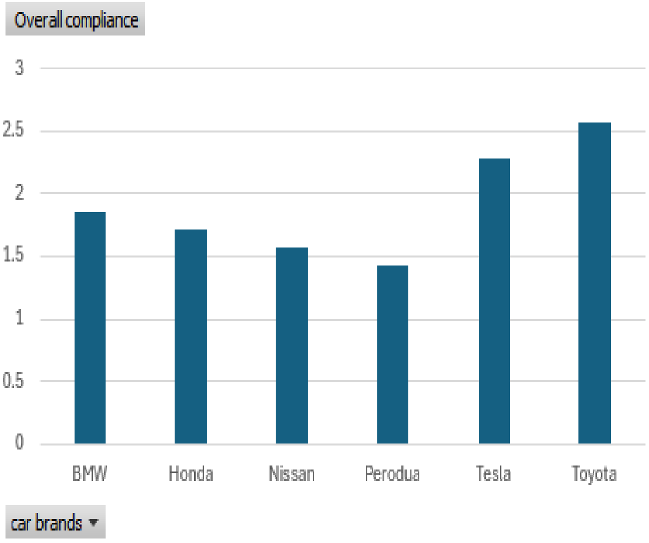


Fig.8 Overall compliance across PDPA

However, it is important to highlight that compliance does not always translate into effective enforcement and implementation. While companies may draft privacy policies that formally meet regulatory requirements, these policies must be enforced through proper governance mechanisms and implemented in practice. The gap between compliance, enforcement, and implementation varies across companies, meaning that even if a company claims compliance, the actual measures taken to protect user data may be insufficient. For instance, a privacy policy may mention security practices, but without clear enforcement or practical implementation, users remain vulnerable to data breaches and misuse. Therefore, compliance on paper alone is not enough to guarantee robust data protection.

The impact of non-compliance can be severe for both car manufacturers and consumers. For car companies, failing to comply with privacy laws can result in financial penalties, loss of customer trust, and reputational damage. Data breaches and poor privacy practices may also deter consumers from adopting connected car technologies, ultimately affecting the company's growth and market position. For consumers, non-compliance increases the risk of unauthorised data use, identity theft, and privacy violations, leading to diminished control over personal information and potential harm.

Additionally, the study's findings raise the question of whether the results can be generalised to all car brands. While the research focused on six prominent car manufacturers, the varying compliance levels observed suggest that the results may not apply uniformly across the entire automotive industry. Differences in compliance could be influenced by regional policies, corporate governance structures, and market priorities. Therefore, further research is needed to assess whether similar gaps exist in the privacy policies of other brands and different jurisdictions.

In conclusion, this study provides a repeatable methodology, but the results should be interpreted with caution when applied to other car manufacturers. Further analysis would be required to account for specific privacy practices and legal obligations applicable to different regions and brands.

V. LIMITATIONS AND FUTURE WORKS

A key limitation of this study is the reliance on publicly available privacy policies, which may not fully represent a company’s actual practices. The analysis uses keyword matching, which may miss important nuances in the policies, leading to incomplete compliance assessments. The study also only includes a small number of automotive brands, so the findings may not apply to all manufacturers or regions.

There is a potential source of bias in this study that lies in the selection of keywords used to evaluate compliance with Malaysia’s PDPA. The keywords were chosen based on the researcher’s interpretation of the seven PDPA principles and the common language used in privacy policies. However, this process may have unintentionally excluded certain synonyms or phrases that could indicate compliance, leading to an underestimation of adherence. Similarly, over-reliance on specific keywords may cause an overestimation of compliance if policies use the right terminology without adequately implementing the corresponding privacy measures.

Bias also exists in the selection of car brands for the study. The research focused on six major car manufacturers — Toyota, Tesla, Honda, BMW, Nissan, and Perodua — chosen for their global presence and relevance in the Malaysian automotive market. While these brands provide valuable insights, the selection may not represent smaller or emerging car brands that could have different privacy practices. Additionally, the study primarily evaluated the English versions of privacy policies, which may introduce language-based bias and limit the generalisability of the results to brands that publish policies in other languages.

These biases impact the study by potentially affecting the accuracy of compliance scores and limiting the applicability of findings to other car brands. The keyword-based approach might not capture nuanced privacy practices, and the brand selection may overlook regional differences or variations in policy enforcement. Future studies should incorporate more comprehensive keyword sets, consider a wider range of car brands, and explore policies in multiple languages to enhance the generalisability of the findings.

Future research could broaden the analysis to include more automotive brands and regions, with a deeper review of policy language to assess true compliance. It could also explore the effects of low compliance on consumer trust and legal risks. Additionally, future studies could examine how companies update their policies in response to changing regulations and gather insights from experts to better understand compliance gaps. Using advanced keyword extraction methods like spaCy and KeyBERT could improve keyword identification accuracy, while stronger evaluation techniques could provide deeper insights into policy effectiveness.

ACKNOWLEDGEMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

References

[1] A. Smith and B. Jones, "Data privacy challenges in the automotive industry: Navigating the era of connected vehicles," Journal of Automotive Technology and Ethics, vol. 15, no. 2, pp. 123–145, 2023.

[2] M. Jen, R. Misha, and M. Zoe, "It's official: Cars are terrible at privacy and security," Mozilla Foundation, 2023. [Online]. Available: https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

[3] G. A. Fowler, "Few read privacy policies. Would they if they were shorter?," The Washington Post, 2022. [Online]. Available: https://www.washingtonpost.com/business/2023/09/07/car-privacy-mozilla-report

[4] C. Brown, "Global data protection regulations and their impact on automotive data management," International Journal of Data Law, vol. 8, no. 1, pp. 78–102, 2022.

[5] C. Bodei et al., "Vehicle data collection: A privacy policy analysis and comparison," in International Conference on Information Systems Security and Privacy, 2023, pp. 626–633.

[6] G. Madzudzo, M. Cheah, and M. Kukova, "Data protection and connected vehicles: Privacy policy analysis from a consumer perspective," 2020. [Online]. Available: https://doi.org/10.13140/RG.2.2.28097.17769

[7] S. Prevost and H. Kettani, "On data privacy in modern personal vehicles," in ACM International Conference Proceeding Series, 2019. [Online]. Available: https://doi.org/10.1145/3372938.3372940

[8] G. Bella and P. Biondi, "Car drivers’ privacy awareness and concerns," 2023. [Online]. Available: https://doi.org/10.13140/RG.2.2.14411.98080

[9] R. N. Zaeem and K. S. Barber, "The effect of the GDPR on privacy policies," ACM Transactions on Management Information Systems, vol. 12, no. 1, 2021. [Online]. Available: https://doi.org/10.1145/3389685

[10] F. Vallet, "The GDPR and its application in connected vehicles—Compliance and good practices," in Lecture Notes in Mobility. Springer Science and Business Media Deutschland GmbH, 2019, pp.

245–254. [Online]. Available: https://doi.org/10.1007/978-3-030-14156-1_21

[11] M. D. Pesé and K. G. Shin, "Survey of automotive privacy regulations and privacy-related attacks," SAE Technical Papers, vol. 2019-April, no. April, 2019. [Online]. Available: https://doi.org/10.4271/2019-01-0479

[12] S. Miskam et al., "Data privacy practices of private higher education institutions in Malaysia: A preliminary study," Journal of Information and Communication Technology, vol. 8, no. 2, 2023.

[13] I. Kara, M. Aydos, and A. Akca, "Privacy, security and legal aspects of autonomous vehicles," Çukurova Üniversitesi, 2020

[14] Z. H. Amur et al., "Unlocking the potential of keyword extraction: The need for access to high-quality datasets," 2023. [Online]. Available: https://doi.org/10.3390/app

[15] A. Bkakria, L. Brika, and L. A. Brika, "A framework for privacy policy enforcement for connected automotive systems," 2023.

[16] A. M. McDonald et al., "A comparative study of online privacy policies and formats," 2009.

[17] Ž. Spalević and K. Vićentijević, "GDPR and challenges of personal data protection," 2022.

[18] R. Das Chaudhury and C. Choe, "Digital privacy: GDPR and its lessons for Australia," Australian Economic Review, vol. 56, no. 2, pp. 204–220, 2023. [Online]. Available: https://doi.org/10.1111/1467-8462.12506

[19] A. Alibeigi and A. B. Munir, "Malaysian personal data protection act: A mysterious application," 2020.

[20] M. C. Gaeta, "Data protection and self-driving cars: The consent to the processing of personal data in compliance with GDPR," vol. 24, pp. 1–48, 2019.

[21] O. A. Cejas et al., "NLP-based automated compliance checking of data processing agreements against GDPR," IEEE Transactions on Software Engineering, vol. 49, no. 9, pp. 4282–4303, 2023. [Online]. Available: https://doi.org/10.1109/TSE.2023.3288901

[22] A. J. Aberkane, G. Poels, and S. vanden Broucke, "Exploring automated GDPR-compliance in requirements engineering: A systematic mapping study," IEEE Access, vol. 9, pp. 66542–66559, 2021 [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3076921

[23] J. Smith, Compliance in the Digital Age: Methods and Models. Compliance Press, 2020.

APPENDIX

TABLE II
DEFINITION AND KEYWORDS FOR EACH PRINCIPLE

Principle	Definition	Keywords
General	Personal data must be processed lawfully and fairly with consent for legitimate purposes.	processing, personal data, consent, sensitive personal data, lawful purpose, legal obligation
Notice and Choice	Data subjects must be informed of data collection, purpose, and rights, giving consent when needed	written notice, inform, right to access, third parties, third party, third party disclosure, access and correction, obligation, supply data, data subject rights, data processing, data collection purpose, data collection, data source, processed, on behalf of, request
Disclosure	Personal data must not be disclosed without consent unless required by law.	disclosure, without consent, data subject consent, third parties, purpose of disclosure, third party disclosure
Security	Reasonable security measures must be taken to protect personal data from risks like loss or misuse.	data protection, protect, security measures, unauthorised access, loss, misuse, modification, data storage location, secure transfer, data processor guarantees, guarantees
Retention	Personal data must not be kept longer than necessary for the purpose it was collected.	retention, deletion, destruction, data retention period, data deletion, purpose fulfillment, not be kept longer, permanently, destroyed
Data Integrity	Data must be accurate, complete, and up-to-date to avoid misleading information.	accuracy, accurate, complete, completeness, up-to-date, not misleading data
Access	Data subjects have the right to access and correct their personal data when necessary.	access to personal data, correct personal data, inaccuracy, data access right, data correction, access, correct, inaccurate, incomplete

TABLE III
SUMMARY OF KEYWORD EXTRACTION FOR HONDA

Principle /Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Giving extra details on processing "your personal data may be collected, processed and used for the following optional purposes"	3
Notice and Choice	1	Very little explanation of this principle	1
Disclosure	1	Explained clearly who is the third party even though the keyword is not found but it refers to the disclosure	3
Security	1	Does not mention anything regarding Security	0
Retention	0	Does not mention anything regarding retention	0
Data Integrity	0	Does mention complying with the Honda Data Integrity Policy	1
Access	1	Mentioned that "you may request for access to, correction, update"	2

TABLE IV
SUMMARY OF KEYWORD EXTRACTION FOR PERODUA

Principle /Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	This notice explains how we collect and handle your personal data in accordance with the law even though the 'lawful' keywords are missing	3
Notice and Choice	1	Mentioned that "This written notice serves to inform you that your personal data is being processed by or on behalf of Perodua."	2
Disclosure	1	Personal data may be disclosed to the relevant third parties and it defines who are the third parties	2
Security	1	The 2 keywords matched do not refer to the Security principle	0
Retention	0	Does not mention anything regarding retention	0
Data Integrity	1	Mentioned ensuring that "the personal data you provide is accurate, complete and not misleading" and that such personal data is kept up to date	2
Access	1	Mentioned that "You may access and request for correction of your personal data". However there is only one line explanation and general.	1

TABLE V
SUMMARY OF KEYWORD EXTRACTION FOR BMW

Principle /Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Personal data are collected, processed and used for the business activities of BMW Group Malaysia but are not limited and also for optional purposes. They highlight all the purposes clearly.	3
Notice and Choice	1	All keywords matched are correct as per the context	1
Disclosure	1	Mentioned clearly that personal data may be disclosed to and processed by	3
Security	1	Mention little about the loss and security.	1
Retention	1	Mentioned deletion once but not detailed.	1
Data Integrity	0	Mentioned about the confidentiality and integrity of your personal data is a matter of prime importance	1
Access	1	Mentioned that “can request access to see any information stored about you and request correction, updating, or disabling of the same at any time”	3

TABLE VI
SUMMARY OF KEYWORD EXTRACTION FOR NISSAN

Principle /Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Mentioned clearly that "we are processing your personal data, including any additional information you may subsequently provide”	3
Notice and Choice	1	Mentioned that “This written notice serves to inform you that your personal data is being processed by or on behalf of ETCM”. Also mentioned about purpose of personal data	3
Disclosure	1	Matched the keywords	1
Security	1	The keywords are not related to Security	0
Retention	0	Not mention anything regarding retention	0
Data Integrity	1	Mentioned that “You are responsible for ensuring that the personal data you provide us is accurate, complete and not misleading and that such personal data is kept up to date.”	2
Access	1	Mentioned that “You may access and request for correction of your personal data and to contact us with any enquiries or complaints in respect of your personal data as follows in accordance with the PDPA:”	2

TABLE VII
SUMMARY OF KEYWORD EXTRACTION FOR TOYOTA

Principle/Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Mentioned clearly what are the data collected and "given your consent for one or more specific purpose"	3
Notice and Choice	1	Mentioned clearly that "Your personal data is collected and further processed as required or permitted"	3
Disclosure	1	Mentioned clearly that "Your personal data provided to us may also be disclosed to the following classes of third parties." Define the third parties.	3
Security	1	Mentioned clearly that "UMWT takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of your personal data."	3
Retention	1	Mentioned that "The personal data collected shall be processed and stored for as long as required by the purpose they have been collected for. However, UMWT may be obliged to retain personal data for a longer period whenever required to do so for the performance of a legal obligation or upon order of an authority." A full score is not possible due to a lack of clarity	2
Data Integrity	1	Just mentioned about accurate data	1
Access	1	Mentioned clearly that "You have the right to access, verify, update and correct your personal data held by us"	3

TABLE VII
SUMMARY OF KEYWORD EXTRACTION FOR TESLA

Principle/Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Mentioned clearly but also states about Collection and Use of Non-Personal Data	2
Notice and Choice	1	Mentioned clearly this principle using other words with the same context as PDPA	3
Disclosure	1	Mentioned clearly this principle using other words with the same context as PDPA	3
Security	1	Mentioned clearly about "Security features to consistently protect your information. For example, your Tesla Account includes owner resources, guides and important documents, so we offer multi-factor authentication to protect your account"	3
Retention	1	Mentioned about retention. However, it does not clearly mention how long the data will be kept and is is based on the consideration of its use. Hence the scoring only increased to 2	2
Data Integrity	1	Matched the keywords	1
Access	1	Mentioned that "You can access your Tesla Account to update the information from or about you in that account at any time"	2

https://doi.org/10.31436/ijpcc.v11i1.539

Predictive Analytics for Sustainable Tourism Development: A Data-Driven Approach

Irfan Qayyim Abdul Mohaimin, Aida Najihah Mohd Marzuki, Raini Hassan*

Department of Computer Science, Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia, Gombak, Malaysia

*Corresponding author hrai@iium.edu.my

(Received: 30th July 2024; Accepted: 7th December, 2024; Published on-line: 30th January, 2025)

Abstract— Tourism plays a significant role in Malaysia's economic and social development, with efforts increasingly aligned to Sustainable Development Goals (SDGs), particularly SDG 8 (Decent Work and Economic Growth). This project addresses the lack of predictive analytics for sustainable tourism by employing a structured methodology encompassing data collection and preparation, exploratory data analysis (EDA), descriptive and predictive analytics, and feature engineering to identify key factors influencing sustainable tourism in Malaysia. The results show trends and patterns in tourism that inform the development of robust machine learning models to forecast sustainable tourism outcomes, in which 92% and 100% accuracy were achieved with Gradient Boosting and Support Vector Machine respectively. These models aim to support data-driven decision-making and promote long-term sustainability in Malaysia's tourism industry.

Keywords— Predictive analytics, sustainable tourism, machine learning, data science, Malaysia.

I. Introduction

Tourism is a rapidly growing industry and a key driver of economic development, fostering regional and national growth, foreign exchange, and social advancement. In Malaysia, the government has consistently supported the sector since its formal recognition in 1959, with initiatives like the Sustainable Tourism Recovery Project (2022) aligning with the National Tourism Policy 2020-2030 to enhance community resilience and promote eco-tourism [1].

However, despite Malaysia's emphasis on sustainable tourism and its alignment with Sustainable Development Goals (SDGs), the sector lacks robust predictive analytics tools to assess and plan for sustainable tourism outcomes effectively. For instance, in 2019, Malaysia welcomed 26.1 million international tourists, contributing RM86.14 billion to the economy [2]. Yet, the COVID-19 pandemic led to a significant decline in tourist arrivals and receipts, highlighting the sector's vulnerability to external shocks and the need for predictive tools to enhance resilience.

A. *Project Objectives*

- Identify key factors influencing sustainable tourism development in Malaysia using statistical and machine learning techniques.
- Provide data-driven insights to support informed decision-making and strategies for integrating sustainability into the tourism sector.
- Develop a machine learning model to predict sustainable tourism outcomes based on analysed factors.

B. *Project Questions*

- What are the critical factors driving sustainable tourism in Malaysia?
- How can predictive analytics enhance decision-making in sustainable tourism?
- What actionable strategies can be derived to balance economic, environmental, and social sustainability?

C. *Contributions to Data Science and Machine Learning*

- This study demonstrates the application of ML in sustainable tourism, offering methods to analyse complex relationships between tourism activities and sustainability outcomes.
- It will equip policymakers and businesses with tools to forecast trends, optimize resources, and minimize environmental and community impacts.
- It integrates predictive analytics into sustainable tourism practices, expanding applications of machine learning in this underexplored domain.
- Supports informed, proactive strategies for long-term resilience and sustainability in Malaysia's tourism industry.

This project addresses challenges in integrating advanced technologies into the tourism sector, aiming to balance growth with sustainability and delivering impactful tools and insights for policymakers, businesses, and researchers.

II. Related Works

Recent studies on sustainable tourism have explored key factors, advanced analytics, and machine learning techniques to better understand and predict trends. These approaches offer valuable insights into tourism patterns and help create models to guide decision-making. Table 1 showcases some of the notable works, highlighting their methods, findings, and practical contributions to the field.

TABLE I
REVIEW OF PREVIOUS WORKS

Year	Authors	Research Problem	Techniques Used	Result
2020	Mai, A., Thi, K., Thi, T., & Le, T.	Factors for sustainable tourism in Vietnam	SPSS, Smart-PLS-SEM	Social engagement is most important
2020	Nasir, N. F., Nasir, M. A., Nasir, M. N. F., & Nasir, M. F.	Understanding of domestic tourism in Malaysia	Qualitative study	Public health and safety are top priorities for travel
2022	Agrawal, R., Wankhede, V. A., Kumar, A., et al.	Role of BDA in sustainable tourism	Literature review, network analysis	Insights into trends and collaborations
2022	Hoffmann, F. J., Braesemann, F., & Teubner, T.	Predicting sustainability using TripAdvisor data	Machine learning, grid search	Identified patterns of sustainability
2024	Louati, A., Louati, H., Alharbi, M., et al.	Predicting tourist spending	Decision Trees, Random Forest, KNN, SVM, ARIMA	Spending trends identified

III. METHODOLOGY

The framework of this project is based on the data science lifecycle which usually consists of data collection, data preprocessing, exploratory data analysis (EDA), model building and machine learning, model evaluation, and data visualization. The key steps involved in the research process are outlined in the flowchart below (see Figure 1).

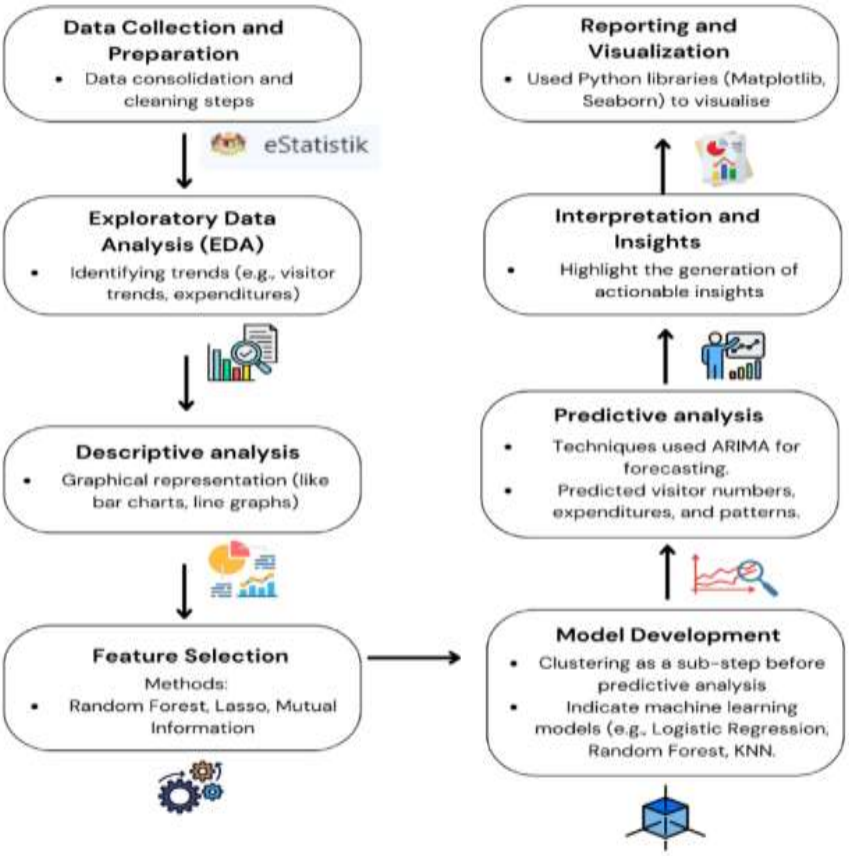

Data Collection and Preparation
• Data consolidation and cleaning steps
eStatistik
Exploratory Data Analysis (EDA)
• Identifying trends (e.g., visitor trends, expenditures)
Descriptive analysis
• Graphical representation (like bar charts, line graphs)
Feature Selection
Methods:
• Random Forest, Lasso, Mutual Information
Model Development
• Clustering as a sub-step before predictive analysis
• Indicate machine learning models (e.g., Logistic Regression, Random Forest, KNN.
Predictive analysis
• Techniques used ARIMA for forecasting.
• Predicted visitor numbers, expenditures, and patterns.
Interpretation and Insights
• Highlight the generation of actionable insights
Reporting and Visualization
• Used Python libraries (Matplotlib, Seaborn) to visualise

Fig. 1 The methodology flowchart

A. *Data Collection*

The Domestic Tourism Survey (DTS), published by the Department of Statistics Malaysia (DOSM) on eStatistik, provides annual data on domestic tourism by state from 2011 to 2023. It includes metrics such as visitor numbers, trips, expenditures, and demographic profiles. DOSM also offers the data in Excel sheets for easier analysis. For this project, data from 108 Excel sheets and reports were consolidated, covering 41 features and 112 entries related to social, economic, and tourism factors (see Figure 2).

B. *Exploratory Data Analysis (EDA)*

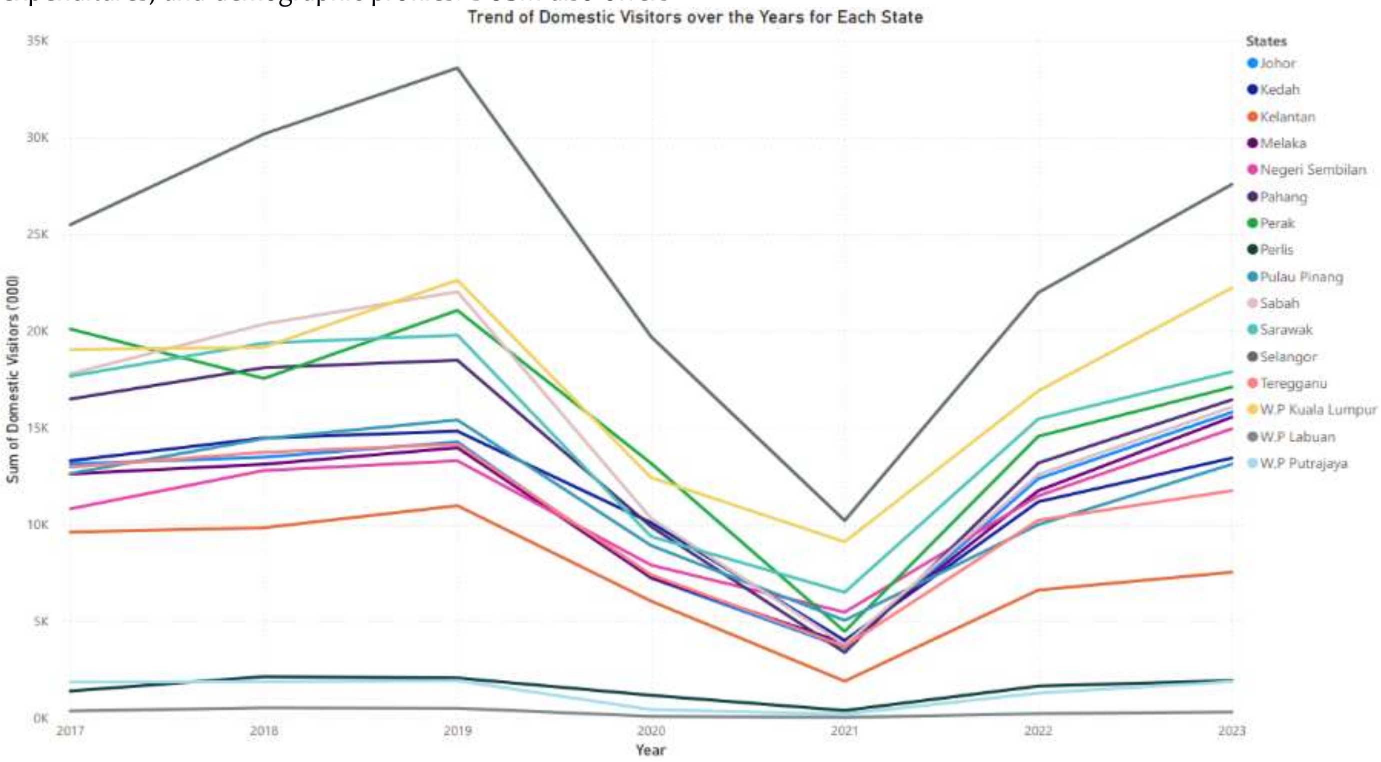


Fig. 2 Trend of domestic visitors over the years for each state

Domestic visitors increased from 2017 to 2019 across most states but dropped sharply in 2020 due to COVID-19. Recovery began in 2021 but remained below 2019 levels. Selangor had the most visitors, while Perlis, W.P. Putrajaya, and W.P. Labuan consistently recorded the lowest numbers, showing minimal pandemic impact due to their smaller size (see Figure 3).

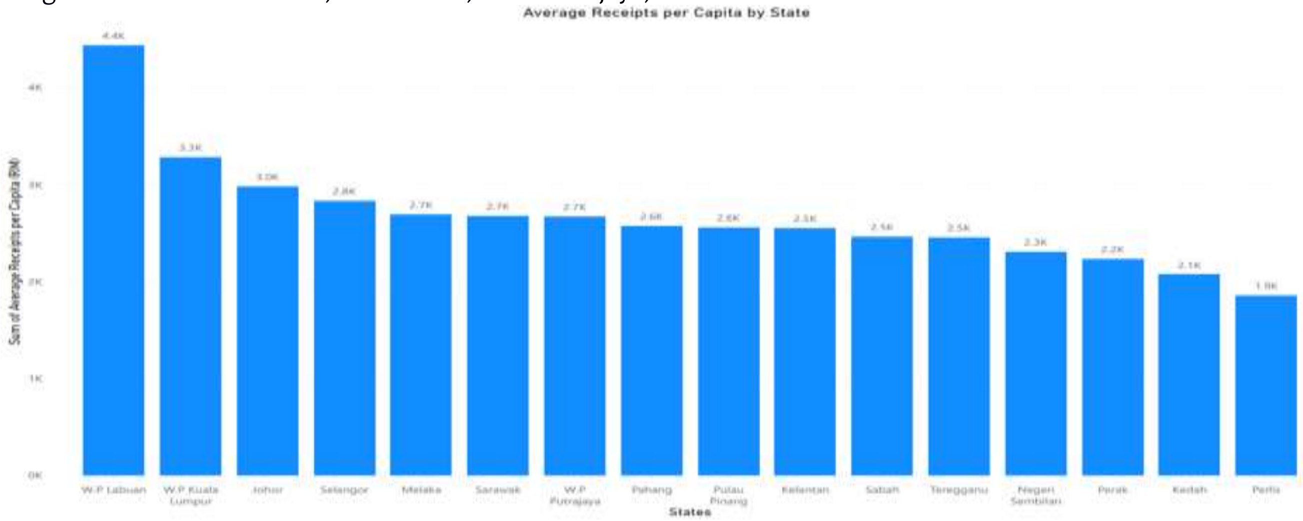


Fig. 3 Top 3 average receipts per capita by state

https://doi.org/10.31436/ijpcc.v11i1.539

W.P. Labuan leads in average receipts per capita, surpassing RM600. W.P. Kuala Lumpur and Johor rank second and third, respectively. Perlis records the lowest average receipts, under RM300, reflecting varying spending patterns across states (see Figure 4).

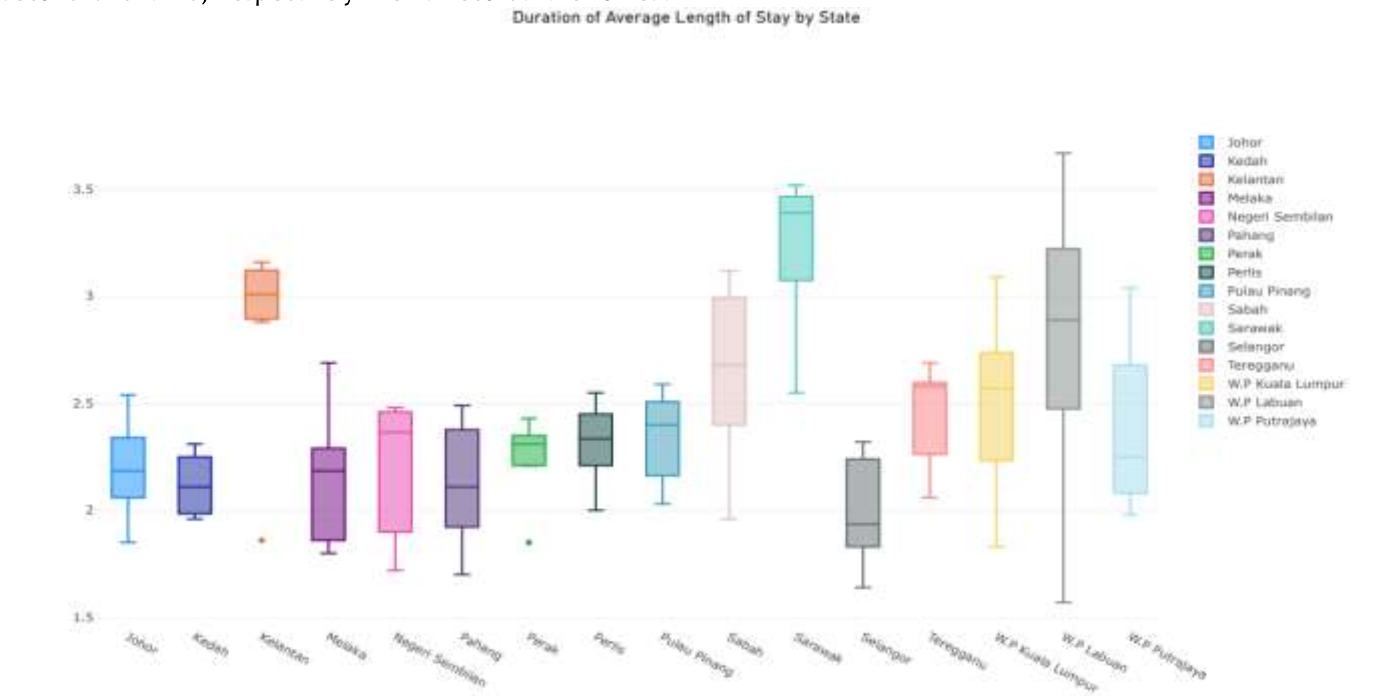


Fig. 4 Distribution of average length of stay by state

Sarawak has the highest median stay (3–3.5 days), while Kelantan shows consistent durations with minimal variability. W.P. Labuan exhibits significant variability with a wide range of stay lengths, reflecting diverse travel behaviours (see Figure 5).

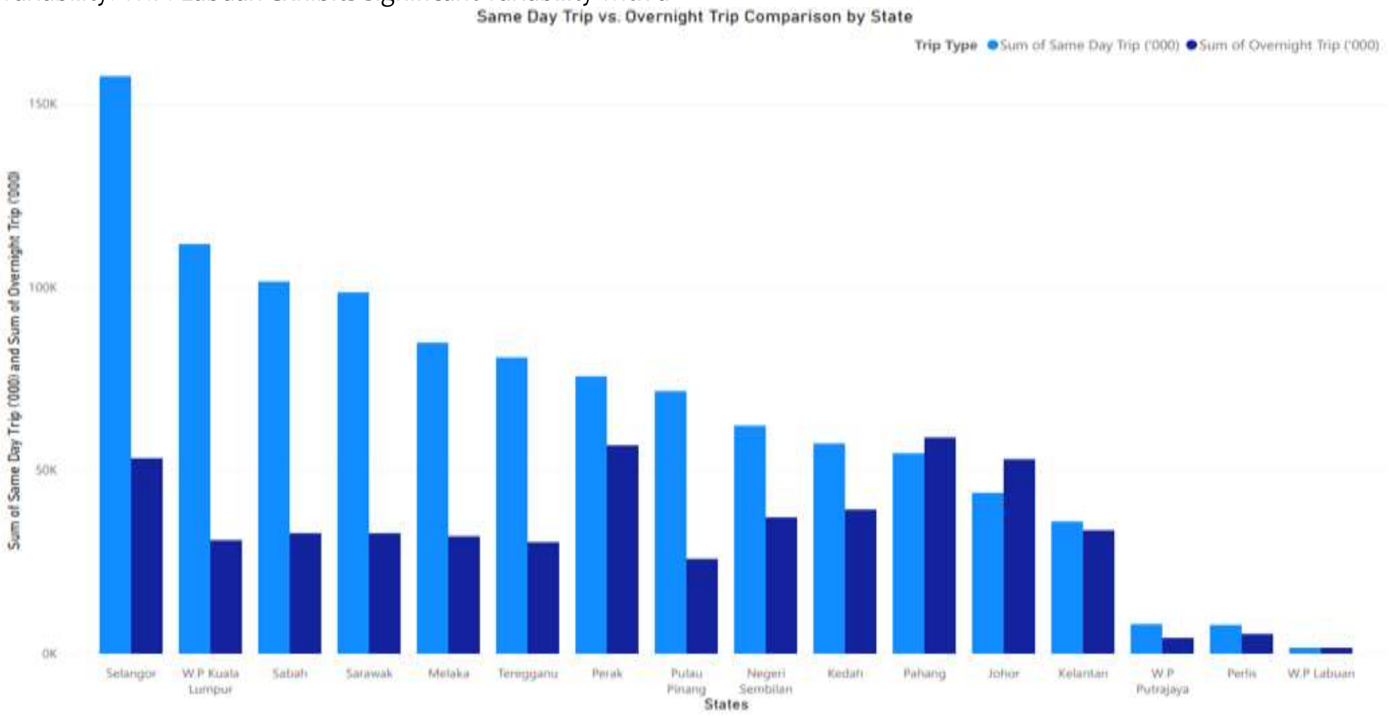


Fig. 5 Same day trip vs. overnight trip comparison by state

Selangor dominates both same-day and overnight trips, with same-day trips outnumbering overnight stays. Conversely, Johor, Pahang, and W.P. Labuan see more overnight trips, indicating longer stays. Kelantan and Pahang display balanced distributions between the two trip types (see Figure 6).

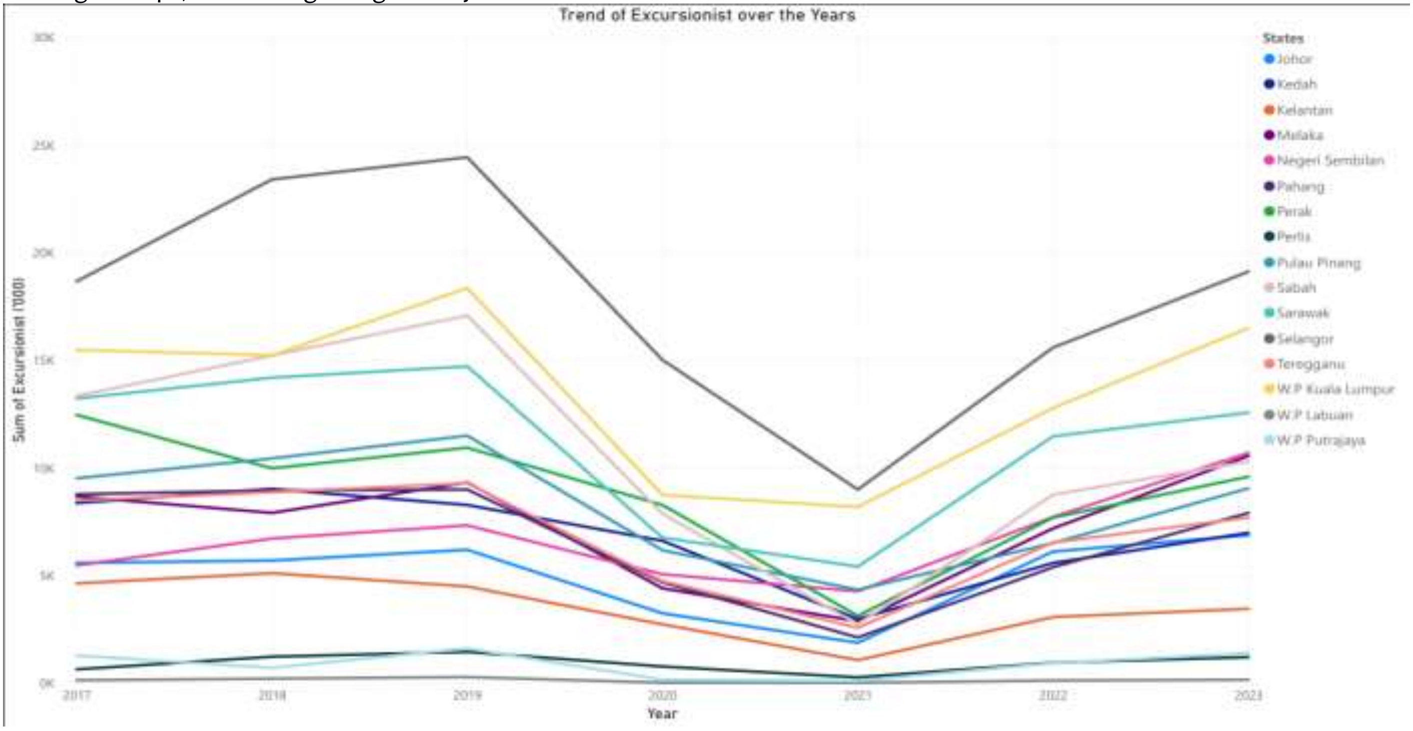


Fig. 6 Trend of excursionists over the years

Excursionist numbers declined in 2020 due to the pandemic but began recovering by 2022. Selangor and W.P. Kuala Lumpur consistently recorded the highest numbers, with Sarawak also showing relatively high but fluctuating figures (see Figure 7).

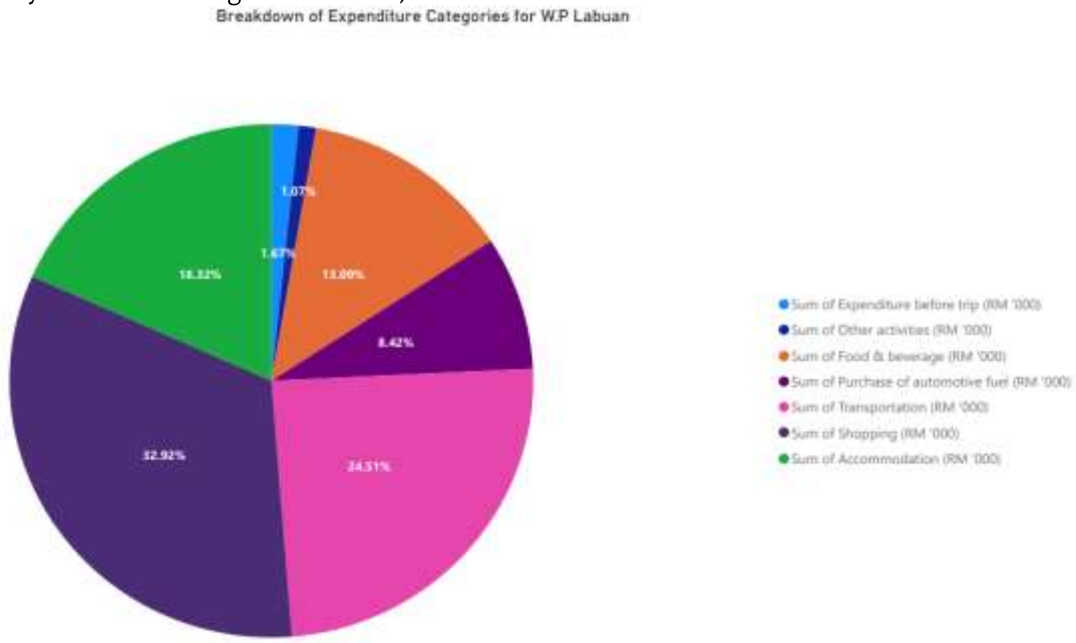


Fig. 7 Breakdown of expenditure categories for W.P Labuan

W.P. Labuan's spending patterns are unique, with the highest share allocated to transportation (31.4%), followed by accommodation (26.2%), and lower spending on food and beverages (13.0%). This contrasts with other states, where shopping dominates expenditure categories (see Figure 8).

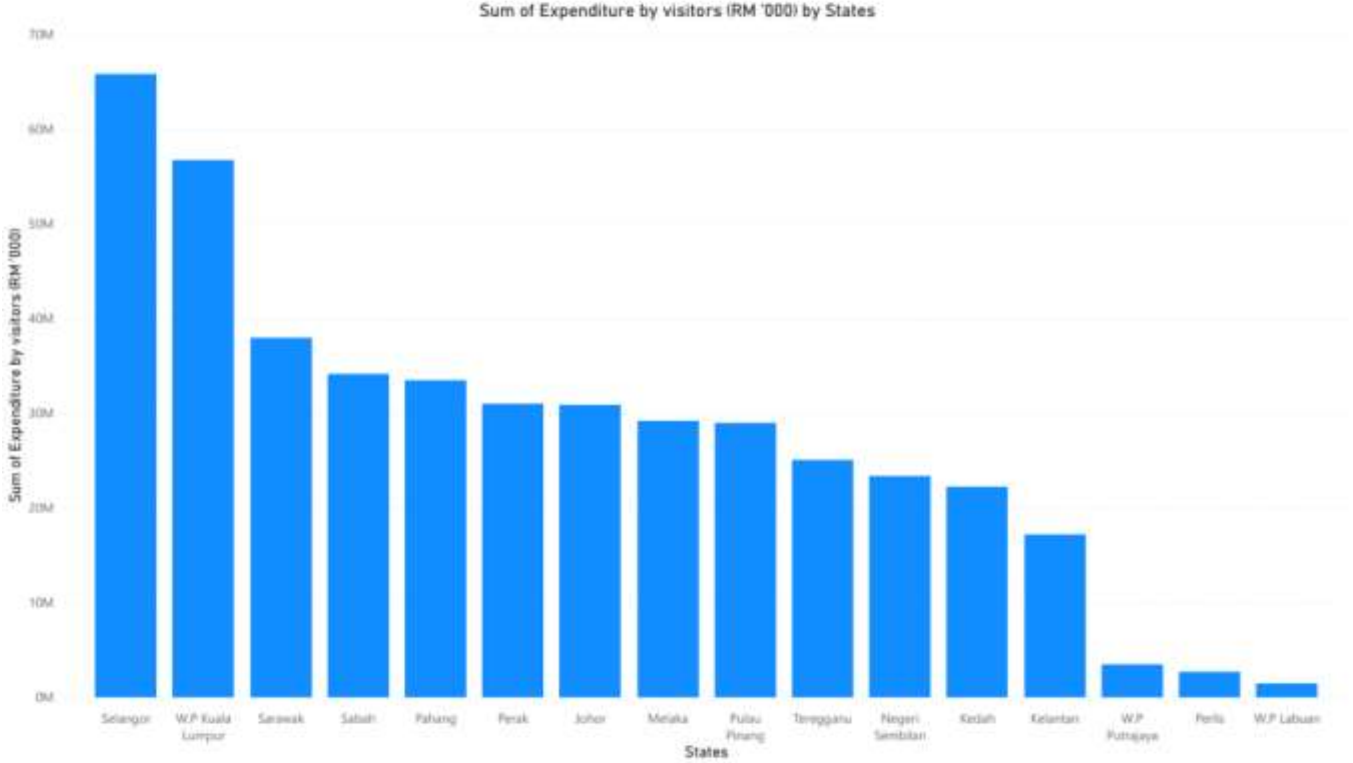


Fig. 8 Total expenditure by visitors for each state in Malaysia

Selangor leads in total visitor expenditure, surpassing RM5 billion, followed by W.P. Kuala Lumpur. W.P. Labuan, Perlis, and W.P. Putrajaya record the lowest expenditures, each under half a billion ringgit.

C. *Descriptive Analytics*

W.P. Labuan is the most expensive tourist destination in Malaysia, with the highest average receipt per capita and per trip. Tourists spend primarily on transportation, accommodation, and food & beverages due to its appeal as a luxury getaway offering activities like diving and island hopping. Limited-service availability further raises costs. Labuan attracts more overnight tourists, with high-end accommodations like Dorsett Grand Labuan catering to affluent visitors.

Selangor leads Malaysia's tourism sector, generating over RM50 billion in revenue over six years. It ranks first in domestic visitors, trips, and same-day visits, driven by its strategic location near W.P. Kuala Lumpur and well-connected transport networks. Attractions range from cultural landmarks like Batu Caves to urban hubs like Sunway Lagoon, supported by a vibrant culinary scene and growing staycation popularity.

Sarawak ranks third in excursionist and same-day trip numbers despite its geographic disconnection from mainland Malaysia. Affordable air travel and efficient infrastructure facilitate short trips. Unique attractions like the Mulu Caves, Dayak cultural experiences, and adventure activities make Sarawak a top destination for eco-tourism and memorable excursions.

D. *Data Preprocessing*

A structured data preprocessing approach was implemented to ensure data quality and consistency for analysis.

1) *Handle missing data*

The dataset contained several columns representing percentages related to tourism activities. Upon analysis, it was found that approximately 14.29% of the data in these columns were missing. To address this, mean imputation was applied, a technique that replaces missing values with the mean of the respective column. This approach was chosen as it assumes that the data's missingness is random and ensures that no rows or columns are dropped, thereby preserving the dataset's integrity. This approach ensured that the dataset remained reliable and complete, ready for subsequent analysis and modelling.

2) *Feature selection*

To identify the most relevant features, multiple feature selection techniques were employed to ensure a robust and comprehensive analysis which are as below:

- *Random Forest Feature Importance*
- *Mutual Information Regression*
- *Lasso Regularization*
- *Recursive Feature Elimination (RFE)*
- *Correlation Heatmap*

This multi-method approach ensures the selection of a highly predictive and diverse set of features, capturing both statistical and model-driven insights for downstream analysis and modelling. After analysis, the final selected features were States, Year, Domestic Visitors ('000), Average Receipts per Capita (RM), and Average Length of Stay (see Figure 9).

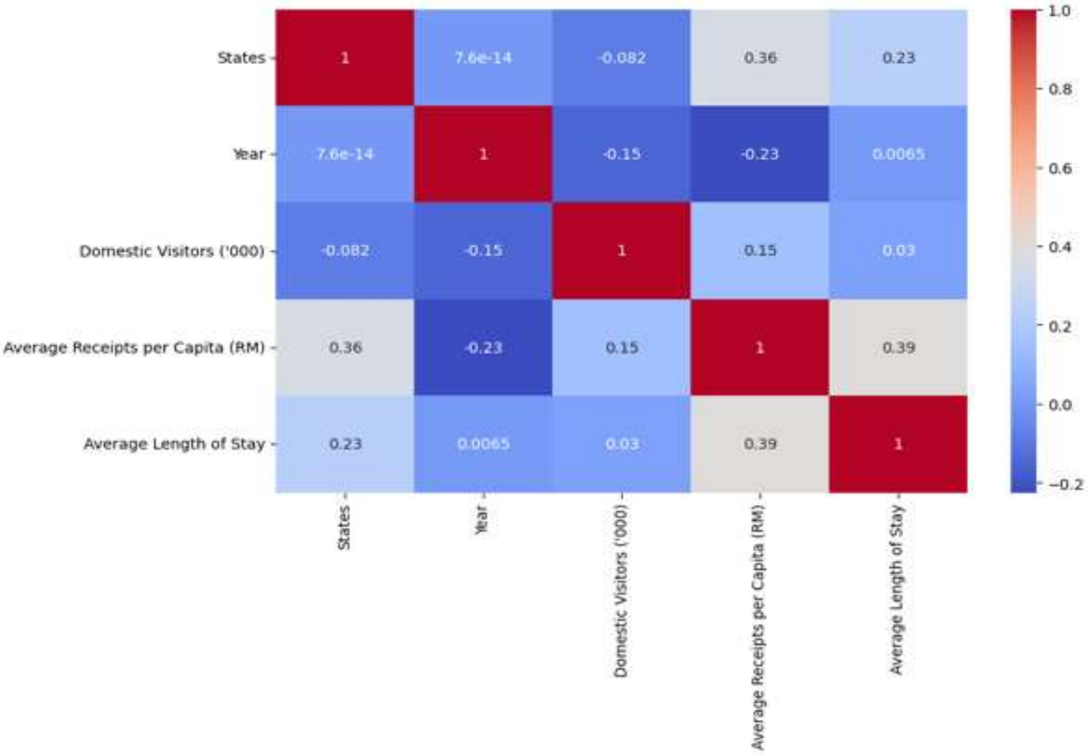


Fig. 9 Correlation heatmap of selected features

3) *Clustering*

Clustering was performed to uncover underlying patterns and group the data into meaningful clusters. The clustering analysis aimed to segment the dataset into homogeneous groups, which would later serve as the target variable for supervised learning tasks. Additionally, the ideal result for clustering would be that each entry for each state belong to their respective clusters only. This is to ensure consistency and accuracy in further analysis. Hence, cluster reassignment will be performed to data entries of each state that do not align with their supposed designated clusters. The approach employed K-Means clustering, a widely used method for partitioning data into non-overlapping clusters based on their similarity.

K-Means clustering was chosen for its simplicity, scalability, and ability to efficiently handle large datasets. It partitions data into distinct, non-overlapping clusters based on similarity, providing clear and interpretable groupings for analysis. Alternative methods like hierarchical clustering were less suitable due to their computational intensity and limited scalability for large datasets, making K-Means the optimal choice.

a) *Features*

- Domestic Visitors ('000): The number of domestic tourists visiting each state.
- Average Receipts per Capita (RM): The revenue generated per tourist.
- Average Length of Stay: The average number of days spent by tourists. These features capture the economic and behavioural aspects of tourism, making them ideal for segmentation.

b) *Preparation*

- Dataset was split to before, during, and after COVID-19

- Pre COVID-19: 2017-2019
- During COVID-19: 2020-2021
- Post COVID-19: 2022-2023

c) *Elbow Method*

The optimal number of clusters was determined using the Elbow Method, which involves plotting the within-cluster sum of squares (WCSS) against the number of clusters. A "bend" in the curve was observed, suggesting that five clusters (before and after COVID-19) and four clusters (during COVID-19) were optimal (see Figure 10-15).

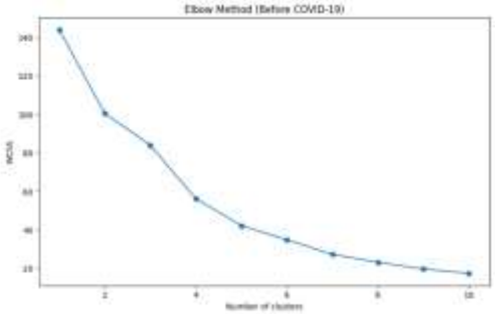


Fig. 10 Elbow method for before COVID-19

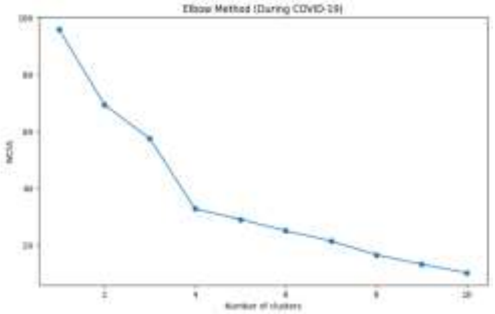


Fig. 11 Elbow method for during COVID-19

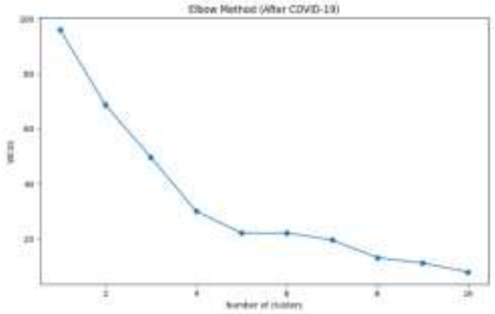


Fig. 12 Elbow method for after COVID-19

d) *Clustering Execution*

- Before and After COVID-19: The data from 2017-2019 (pre-COVID) and 2022-2023 (post-COVID) were clustered separately, each with five clusters.
- During COVID-19: Data from 2020-2021 were clustered using four clusters, reflecting the irregular tourism patterns during the pandemic.
- W.P. Labuan (Cluster 3) was identified as an outlier due to its distinct characteristics, including low domestic visitors and high receipts per capita with an extended length of stay.

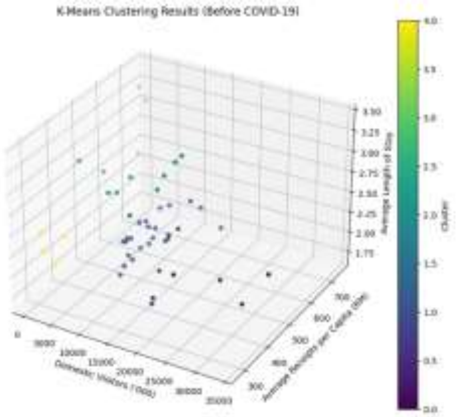


Fig. 13 K-Means clustering results (before COVID-19)

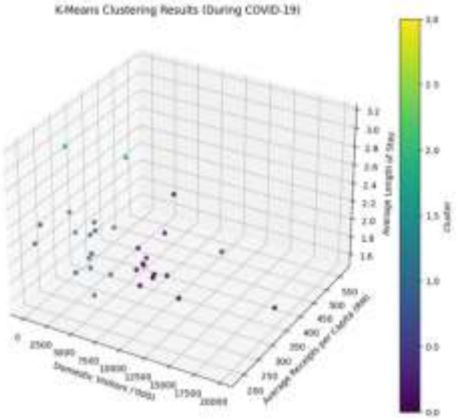


Fig. 14 K-Means clustering results (during COVID-19)

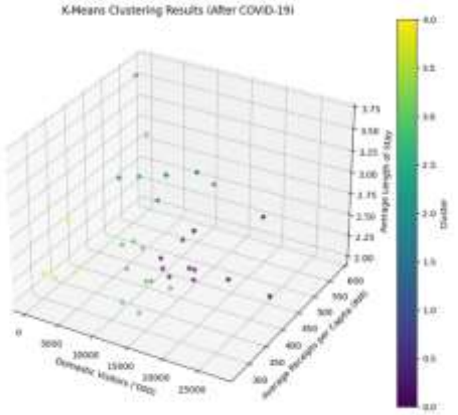


Fig. 15 K-Means clustering results (after COVID-19)

e) Sankey Diagram

- Sankey diagrams were used to determine which entries from each state belong to which cluster.
- Before and After COVID-19: Most data entries consistently belong to respective cluster for each state
- During COVID-19: A large amount of data belongs to cluster 0 or 1 only, showing that states with supposed different characteristics are now grouped up together, indicating unreliability
- During COVID-19 data will be disregarded from the dataset for future machine learning purposes as its massive inconsistency in cluster assignment is deemed unreliable
- Before and After COVID-19 data is combined (see Figure 16-18)

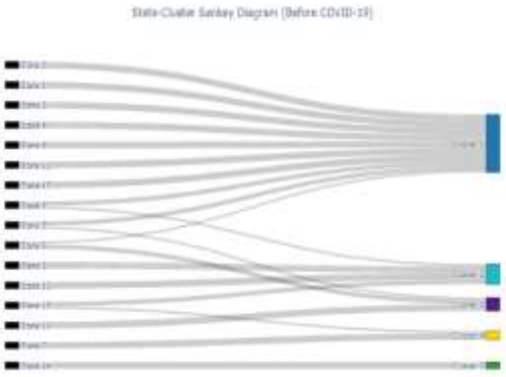


Fig. 16 State-cluster Sankey diagram (before COVID-19)

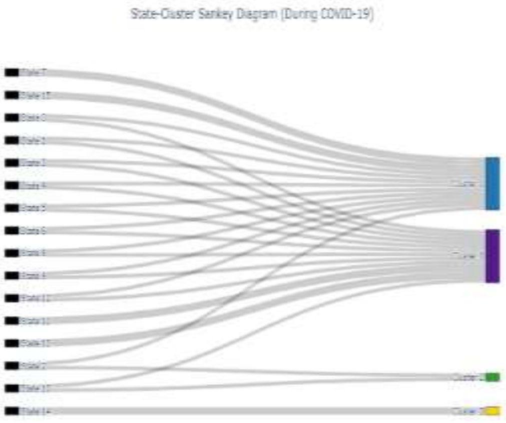


Fig. 17 State-cluster Sankey diagram (during COVID-19)

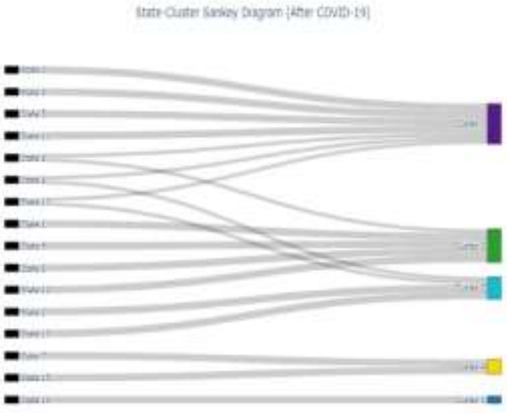
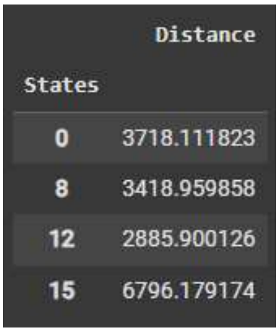


Fig. 18 State-cluster Sankey diagram (after COVID-19)

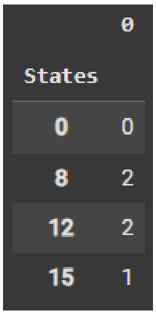
f) Cluster Reassignment

- States with a singular data entry grouped into a different cluster will be assigned to its majority cluster (see Figure 19-21)
- This includes states 3, 6, 9, 10, 13, 14
- States with many data entries grouped into different clusters will undergo cluster reassignment by Euclidean distancing
- This includes states 0, 8, 12, 15



	Distance
States	
0	3718.111823
8	3418.959858
12	2885.900126
15	6796.179174

Fig. 19 Euclidean distancing for states 0, 8, 12, and 15



	0
States	
0	0
8	2
12	2
15	1

Fig. 20 Cluster reassignment for states 0, 8, 12, and 15

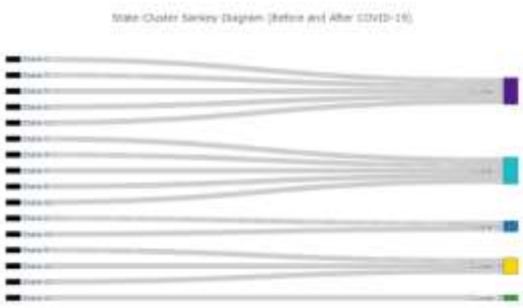


Fig. 21 State-cluster Sankey diagram after removing before COVID-19 and cluster reassignment

g) Cluster Characteristics

Cluster 0 (Purple):

- Mid to high domestic visitors
- Mid to high average receipts per capita
- Low average length of stay
- States: Pahang, Selangor, Melaka, Perak, Johor

Cluster 1 (Blue):

- Low domestic visitors
- High average receipts per capita
- Mid average length of stay
- States: Kelantan, W.P Putrajaya

Cluster 2 (Cyan):

- Low to mid domestic visitors
- Mid average receipts per capita
- Low to mid average length of stay
- States: Kedah, Negeri Sembilan, Perlis, Pulau Pinang, Terengganu

Cluster 3 (Green):

- Low domestic visitors
- High average receipts per capita
- Mid to high average length of stay
- States: W.P Labuan

Cluster 4 (Yellow):

- Low to mid domestic visitors
- High average receipts per capita
- Low to mid average length of stay
- States: Sabah, Sarawak, W.P Kuala Lumpur

h) Potential Limitations of K-Means Clustering

- K-Means depends on initial centroid placement, which can lead to suboptimal results. This was addressed using "k-means++" for better initialization
- The algorithm assumes spherical clusters, which may not match real-world data. Outliers like W.P. Labuan challenged this assumption
- K-Means is sensitive to outliers, as seen with W.P. Labuan, consistently grouped in a separate cluster (Cluster 3)

E. Model Development

The clustering labels (Cluster 0 to Cluster 4) obtained from the prior K-Means analysis were used as the target variable for classification tasks. Special attention was given to Cluster 3 (W.P. Labuan), identified as a potential outlier due to its unique characteristics.

1) Data Preparation

The dataset underwent preprocessing to ensure consistency and reliability. Two separate datasets were used:

- With Cluster 3 (C3): Included all clusters from the K-Means analysis
- Without Cluster 3 (No C3): Excluded Cluster 3 to evaluate its impact as an outlier

2) Machine Learning Methods

Six supervised learning algorithms were employed for cluster classification, each chosen for their strengths in handling specific data characteristics: Logistic Regression (LR), a probabilistic model effective for linearly separable data, was selected due to the somewhat linear relationships among features in the dataset, despite its tendency to overfit in high dimensions. Decision Trees (DT), Random Forest (RF), and Gradient Boosting (GB)were included for their robustness and ability to handle the distinct characteristics and varied data patterns across states, making them well-suited for the complex and heterogeneous nature of tourism data. K-Nearest Neighbors (KNN) was selected as a distance-based algorithm that could serve as a benchmark, while Support Vector Machines (SVM) was chosen for its effectiveness in high-dimensional spaces and its ability to capture complex decision boundaries, providing a versatile comparison to tree-based methods.

3) Grid Search for Hyperparameter Tuning

To optimize model performance, GridSearchCV was used to systematically explore hyperparameters for each model. The hyperparameters were chosen based on best practices and exploratory data analysis. The grid search process identified the best parameter combinations for improving accuracy and generalizability.

F. Predictive Analytics

ARIMA is a popular method for forecasting time series data, combining autoregression, integration, and moving average components. Autoregression links current values to past values, integration stabilizes the series and moving average smooths fluctuations. By analysing historical data, ARIMA optimizes parameters to forecast future values, making it effective for predicting complex, unstable patterns.

IV. Results

The results of the machine learning models offer critical insights into the application of predictive analytics in Malaysia's sustainable tourism sector. The evaluation of each model, conducted on datasets with and without Cluster 3 (representing W.P Labuan), highlights the impact of outliers on model performance and the effectiveness of hyperparameter optimization through Grid Search.

A. *Performance of Machine Learning Models*

TABLE II
Machine Learning Model Accuracies

Acc.	**Machine Learning Model**					
	LR	**DT**	**RF**	**GB**	**KNN**	**SVM**
C3	0.83	0.88	0.88	0.92	0.79	0.75
No C3	0.87	0.74	0.74	0.78	0.83	0.87
GC3	0.88	0.71	0.83	0.75	0.83	0.96
No GC3	0.91	0.78	0.74	0.78	0.83	1.00

B. *Insights from Results*

The SVM model achieved the best overall performance with an accuracy of 100% on the dataset without Cluster 3 after tuning. The optimal parameters for this model were {'C': 10, 'gamma': 'scale', 'kernel': 'rbf'}. The Gradient Boosting model also performed exceptionally well, achieving an accuracy of 92% on the dataset with Cluster 3 before tuning. Its best parameters were {'learning_rate': 0.1, 'max_depth': 10, 'min_samples_leaf': 2, 'min_samples_split': 2, 'n_estimators': 100, 'subsample': 0.8}.

The performance of SVM is highly influenced by hyperparameter tuning and the inclusion of Cluster 3 (C3). Without C3 and with hyperparameter tuning, SVM achieves perfect classification accuracy (100%), as the absence of noisy and overlapping data simplifies the dataset. Including C3 with tuning slightly reduces accuracy to 96%, as the added complexity introduces noise. Without tuning, performance drops significantly to 87% for datasets without C3 and 75% for those with C3, highlighting the critical role of tuning in optimizing SVM to the dataset's characteristics. Default parameters fail to handle overlapping features and outliers effectively, leading to suboptimal results.

Gradient Boosting demonstrates its strength in handling complex datasets like C3 due to its iterative learning approach. With default parameters, it achieves the highest accuracy (92%) for C3, effectively capturing patterns in noisy data. However, hyperparameter tuning for C3 reduces accuracy to 75%, likely due to overfitting to noise and outliers. When C3 is excluded, the dataset becomes simpler, and Gradient Boosting performs moderately, achieving 78% accuracy regardless of tuning. This suggests that the model’s ability to handle complex relationships is less impactful on simplified datasets.

C. *ARIMA*

To forecast future domestic tourism demand, an ARIMA model was used, identifying 'Domestic Tourism Trips ('000)' as a key variable. Selangor, with the highest historical trip volumes, was selected for analysis to predict domestic tourist numbers for the next 10 years. The results provide valuable insights for tourism stakeholders in Selangor, aiding in planning and development decisions, while also highlighting the impact of including or excluding COVID-19 years in the analysis. The decision to exclude COVID-19 data was made to avoid skewing the predictive models with irregular and non-representative trends.

1) *Forecasting excluding COVID-19*

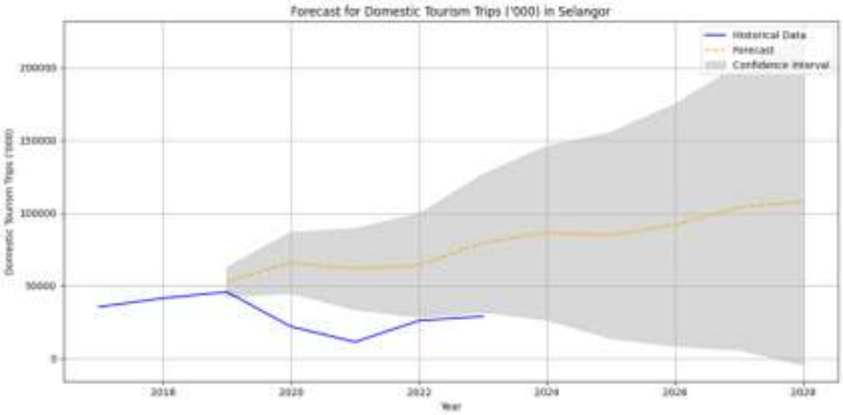


Fig. 22 Forecast for domestic tourism trips ('000) in Selangor starting from the year 2019

The ARIMA model's forecast for Selangor starting from 2019 demonstrates a growth in domestic tourism over the next decade. The confidence interval for this forecast is narrower in the early years (2020-2023), reflecting greater certainty in the predictions. As the forecast progresses, the confidence interval gradually widens, showing increasing uncertainty but maintaining a generally optimistic upward trajectory (see Figure 22).

Policymakers can use these insights to invest in better infrastructure, promote hidden gems like Kampung Kuantan Firefly Park and Farm in The City. The RM200,000 grant allocated under the Visit Selangor Year (VSY) 2025 [8] campaign can support local tourism players in developing innovative products that cater to both domestic and international tourists. Furthermore, Selangor's digital campaign portal, *visitselangor2025.my*, can serve as a platform for promoting these initiatives and engaging with tourists in real-time [9].

Businesses, especially hotels and travel agencies, should prepare for higher demand by improving services and offering tailored packages. Strategic moves, such as planning around peak travel times and encouraging public-private partnerships, can help make tourism both profitable and sustainable. These findings highlight how predictive analytics can guide smart decisions and support long-term tourism development (see Figure 23).

2) *Forecasting including COVID-19*

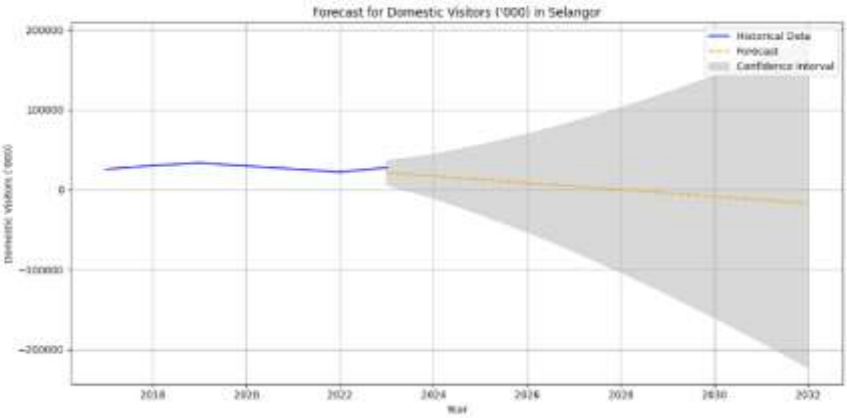


Fig. 23 Forecast for domestic tourism trips ('000) in Selangor starting from the year 2023

This forecast presents a more complex trajectory, with a gradual decline in domestic tourism trips. The confidence interval for this forecast is much wider immediately following 2023, indicating significant uncertainty caused by the inclusion of the COVID-19 years. Over time, the confidence interval expands rapidly, reflecting greater variability and difficulty in predicting long-term trends under disrupted conditions.

Unlike the 2019 forecast, where the trajectory was upward and the confidence interval symmetrical, the 2023 forecast highlights a declining trend, with the lower bound suggesting the possibility of sharp declines in domestic tourism. This highlights the lingering effects of COVID-19 on tourism recovery and the challenges in achieving stability.

To mitigate these risks, policymakers should diversify tourism offerings and invest in resilience strategies to stabilize the tourism sector. By integrating predictive insights with ongoing initiatives like VSY 2025, Selangor can achieve its goal of attracting eight million tourists and generating RM11.7 billion in tourism receipts by 2025 [10]. These data-driven strategies will ensure the long-term sustainability and resilience of Selangor's tourism industry.

V. Future Work

Future work will focus on expanding data collection to include monthly metrics, enabling detailed analysis of seasonal variations and short-term trends. Extending the study to incorporate international tourism data will provide a comprehensive view of global trends impacting Malaysia. Moreover, developing real-time predictive systems integrated with dashboards will enhance decision-making and allow timely responses to changing tourism patterns.

Additionally, incorporating more variables such as weather conditions, socio-economic factors, transportation accessibility, and major event schedules could improve the model's predictive accuracy. Integrating real-time data through IoT devices will enable the model to adapt continuously to changing tourism behaviours, leading to more precise prediction and proactive data-driven strategies.

Apart from that, integrating Internet of Things (IoT) technology into tourism data collection can significantly enhance the accuracy and responsiveness of predictive models. Deploying IoT devices such as smart sensors at popular tourist sites can provide real-time data on visitor numbers, crowd density, and resource usage. This live data can be directly integrated into the ARIMA forecasting model to allow dynamic updates. These efforts will contribute to a more comprehensive and effective approach to forecasting and decision-making in sustainable tourism development.

This study has several limitations that need to be addressed for more robust outcomes. The dataset used covers only the period from 2017 to 2023, limiting the model's ability to capture long-term trends. Incorporating more extensive historical data and monthly datasets would improve model robustness.

VI. Conclusions

This study highlights the role of data science and machine learning in promoting sustainable tourism in Malaysia. By analyzing patterns and forecasting trends with models like SVM and ARIMA, it identifies key factors influencing tourism and provides actionable insights for sustainable development. Despite limitations, the research supports data-driven strategies for balancing economic, social, and environmental goals, offering a foundation for future advancements in predictive analytics and sustainable tourism practices.

Acknowledgment

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

Conflict of Interest

The authors declare that there is no conflict of interest.

References

[1] Ministry of Tourism, Arts and Culture Malaysia (MOTAC), "National Tourism Policy 2020-2030," 2020. [Online]. Available: https://motac.gov.my/en/archives/2020/national-tourism-policy-2020-2030

[2] Tourism Malaysia, "Tourism contributes RM86.14 billion to Malaysia economy with 26.1 million tourists in 2019," 2019. [Online]. Available:https://www.tourism.gov.my/media/view/tourism-contributes-rm86-14-billion-to-malaysia-economy-with-26-1-million-tourists-in-2019

[3] A. Mai, K. Thi, T. Thi, and T. Le, "Factors influencing on tourism sustainable development in Vietnam," 2020. [Online]. Available: http://growingscience.com/beta/msl/3686-factors-influencing-on-tourism-sustainable-development-in-vietnam.html

[4] N. F. Nasir, M. A. Nasir, M. N. F. Nasir, and M. F. Nasir, "Understanding of Domestic Tourism in Malaysia," International Research Journal of Modernization in Engineering Technology and Science, 2020. [Online]. Available: https://www.irjmets.com/uploadedfiles/paper/volume2/issue_10_october_2020/4490/1628083177.pdf

[5] R. Agrawal, V. A. Wankhede, A. Kumar, S. Luthra, and D. Huisingh, "Big data analytics and sustainable tourism: A comprehensive review and network-based analysis for potential future research," International Journal of Information Management Data Insights, vol. 2, no. 2, p. 100122, 2022. [Online]. Available: https://doi.org/10.1016/j.jjimei.2022.100122

[6] F. J. Hoffmann, F. Braesemann, and T. Teubner, "Measuring sustainable tourism with online platform data," EPJ Data Science, vol. 11, no. 1, 2022. [Online]. Available: https://doi.org/10.1140/epjds/s13688-022-00354-6

[7] A. Louati, H. Louati, M. Alharbi, E. Kariri, T. Khawaji, Y. Almubaddil, and S. Aldwsary, "Machine Learning and Artificial Intelligence for a sustainable tourism: A case study on Saudi Arabia," Information, vol. 15, no. 9, p. 516, 2024. [Online]. Available: https://doi.org/10.3390/info15090516

[8] E. S. Journal, "State grant for tourism product development to roll out by end-Jan - tourism Selangor," Selangor Journal, 2025. [Online]. Available: https://selangorjournal.my/2025/01/state-grant-for-tourism-product-development-to-roll-out-by-end-jan-tourism-selangor/

[9] A. Sharon, "Malaysia: New Digital Portal Drives Tourism in Selangor," OpenGov Asia, 2024. [Online]. Available: https://opengovasia.com/2024/12/25/malaysia-new-digital-portal-drives-tourism-in-selangor/

[10] S. Online, "Selangor looking to sports tourism to boost figures," The Star, 2024. [Online]. Available: https://www.thestar.com.my/news/nation/2024/11/04/selangor-looking-to-sports-tourism-to-boost-figures

A Comprehensive Review of Zero Trust Network Architecture (ZTNA) and Deployment Frameworks

Zainab Senan Mahmod Attar Bashi[1*], Shayma Senan[2]

[1]Department of Computer Science, International Islamic University Malaysia, Gombak, Malaysia.
[2]Electrical and Computer Engineering Department, International Islamic University Malaysia, Gombak, Malaysia.

*Corresponding author Zainab_senan@iium.edu.my

(Received: 30th July 2024; Accepted: 7th December, 2024; Published on-line: 30th January, 2025)

***Abstract*— –** The zero trust (ZT) approach has initiated significant advancements in network security, addressing the limitations of traditional security models. Traditional network security approaches have faced challenges adapting to modern trends such as bring your own device (BYOD) and cloud computing, resulting in increased complexity in meeting new security requirements. The zero trust security model operates on the principle that no entity within the network, whether internal or external, is inherently trusted. Therefore, all users and devices must undergo strict authentication and authorization processes prior to accessing organizational resources. This review paper provides a comprehensive analysis of zero trust network architecture (ZTNA) and outlines a general deployment framework model, highlighting the critical role of zero trust in modern network security.

***Keywords*—** Zero Trust, Network Security, Identity and Access Management.

I. Introduction

Zero Trust, a groundbreaking network security strategy introduced by [1], represents a shift from the conventional "trust but verify" approach to a more determined "never trust, always verify" approach. This paradigm challenges the traditional belief that devices inside the network are inherently trustworthy while those outsides are suspicious. In the Zero Trust model, every user and device, regardless of their location or prior access history, is treated with skepticism until their identity and authorization are thoroughly verified. This departure from the historical perimeter-based security concept is especially related in the contemporary landscape of remote work and cloud computing, where the traditional network perimeter has become increasingly vulnerable. Zero Trust stands as a robust response to this evolution, emphasizing the continuous connectivity and access, limiting the potential security breaches, and acknowledging that the threat landscape demands continuous monitoring.

Prior to the emergence of the Zero Trust security model, companies typically granted network access exclusively to users deemed inherently trustworthy. The assumption was that internal employees and collaborators were inherently reliable. However, the rapid development of the internet, cloud computing, and the Internet of Things (IoT) has necessitated the integration of different technologies and systems within organizational operations, consequently making data more accessible to both internal and external actors. This shift has increased vulnerabilities, leading to a higher risk of data breaches and cyber-attacks.

In response to these challenges, the Zero Trust security model was proposed to mitigate the risks associated with implicit trust. The model requests that all users, devices, and systems must authenticate and authorize their identities before accessing network resources.

In 2018, the Zero Trust model by introducing the Zero Trust eXtended (ZTX) framework was introduced [2], which encompasses seven core pillars: workforce security, device security, workload security, network security, data security, visibility and analytics, and automation and orchestration as shown in table (1). These pillars assist organizations in constructing a security architecture that denys implicit trust in favor of continuous authentication and authorization of identities, devices, and network activities.

TABLE I
SUMMARY OF THE PILLARS OF ZERO TRUST EXTENDED (ZTX) FRAMEWORK [2]

Zero Trust Pillar	**Actions**
Users	- Flag excessive access - Limit and enforce data access - Alert on abnormal behavior - Assign data owners based on activity
Devices	- Assess device trustworthiness - Pair users to devices for detecting suspicious behavior
Network	- Fix misconfigurations - Analyze VPN, DNS, and web activity - Report on network threats
Applications	- Monitor and manage application access

	- Track and alert on configuration changes - Alert on access from unsanctioned locations
Automation	- Classify sensitive data - Detect threats - Remediate overexposed files - Enforce privacy policies
Analytics	- Monitor and analyze events - Perform risk assessments - Run data classification scans - Maintain an audit trail

The same year, Google advanced the practical implementation of Zero Trust by developing its own Zero Trust architecture. This framework is defined as a set of concepts and ideas designed to minimize uncertainty in enforcing accurate, on-demand access decisions within network-facing information systems and services. The Zero Trust Architecture (ZTA) serves as an enterprise cybersecurity blueprint that integrates Zero Trust principles into component relationships, workflow planning, and access policies. Full implementation of a Zero Trust Architecture solution involves three key elements: enhanced identity governance and policy-based access control, micro-segmentation, and software-defined perimeter and overlay networks. These elements collectively ensure a comprehensive and resilient security posture, capable of addressing the dynamic threats faced by modern organizations. Figure (2) shows the logical components of Zero Trust Architecture (ZTA).

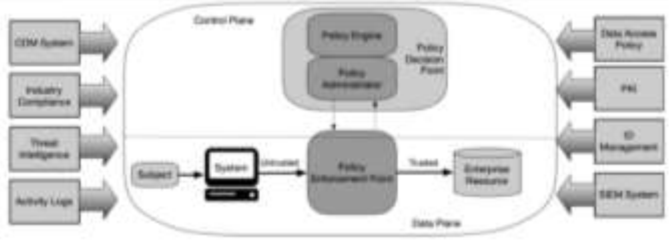


Fig 1. Logical Components of Zero Trust Architecture [3]

This paper is organized into several key sections. The following section highlights related works and presents a detailed examination of traditional network security models, highlighting their limitations and the need for a paradigm shift. Subsequently, the core principles and components of Zero Trust Network Architecture (ZTNA) are discussed, including authentication mechanisms, micro-segmentation, and policy enforcement points. The paper then explores some case studies and real-world implementations, showcasing the impact of Zero Trust in various organizational settings. Finally, the review concludes with a discussion on the future directions of Zero Trust, emphasizing ongoing research, emerging trends, and potential challenges in widespread adoption.

II. Related Works

The field of network security has seen significant advancements over the years, with traditional security models evolving to address emerging threats and challenges. However, these traditional approaches have faced limitations in coping with the dynamic and complex nature of modern network environments. This section explores various traditional security models, highlighting their key features, limitations, and the challenges they encounter in today's context.

Perimeter-Based Security has long been a foundational approach in network defense. This model focuses on protecting the network boundary using firewalls and intrusion detection systems (IDS) [4]. The underlying assumption is that internal network traffic can be trusted, while external traffic is potentially harmful. While effective in its early days, perimeter-based security struggles to address insider threats and manage the complexities introduced by Bring Your Own Device (BYOD) policies and remote access. Additionally, it offers limited protection against advanced persistent threats (APTs) [5], which can intrude into the network.

Virtual Private Networks (VPNs) are another traditional method aimed at securing data transmitted over public networks and providing secure remote access [6]. VPNs encrypt data, ensuring its confidentiality and integrity. However, this approach can introduce performance issues due to encryption overhead, and managing VPNs at scale can be complex and challenging. Furthermore, if endpoints are compromised, VPNs become vulnerable, undermining the security they are meant to provide.

Endpoint Security focuses on securing individual devices using antivirus software, firewalls, and endpoint detection and response (EDR) systems [7]. While this method is essential for protecting devices, its scope is limited to the endpoints themselves and does not encompass the entire network. This high dependency on user behavior makes it ineffective against zero-day threats [8] and sophisticated attacks that can bypass endpoint defenses.

Network Access Control (NAC) [9] solutions aim to control access to network resources based on device compliance and user credentials, providing visibility and control over devices on the network. Despite these advantages, NAC implementation and management can be complex and may not scale well with the increasing number of devices. Additionally, NAC systems can struggle to effectively counter sophisticated attacks that exploit network vulnerabilities.

Signature-Based Detection [10] involves using known signatures of malware and threats to detect and prevent attacks. Common tools in this category include antivirus software and IDS. However, signature-based approaches are inherently limited in their ability to detect new, unknown threats, and they often require constant updates to maintain their effectiveness. High false positive rates and the need for regular updates to signature databases further complicate their use.

Behavior-Based Detection [11] shifts the focus to monitoring network and user behavior to identify anomalies and potential threats. Using machine learning and analytics, this method offers a more dynamic defense mechanism. Nonetheless, it is resource-intensive, complex to manage, and can produce false positives. Effective deployment of behavior-based detection requires advanced expertise to interpret results and manage the systems.

Role-Based Access Control (RBAC) [12] grants access to resources based on users' roles within an organization, simplifying permission management. However, RBAC can become complex in large organizations with dynamic access needs. The static nature of roles may not adapt well to evolving threats, making it challenging to maintain an up-to-date and effective access control framework.

Security Information and Event Management (SIEM) [13] systems collect and analyze security data from various sources, offering real-time monitoring and incident response capabilities. While SIEM provides comprehensive security visibility, it comes with high costs and complexity. Effective use of SIEM systems requires skilled personnel, and there is a risk of data overload and false positives, which can hinder efficient threat detection and response. Table (2) summarizes these traditional security approaches, their key features, and their limitations.

TABLE III
SUMMARY OF RELATED WORKS

Security Model	**Key Features**	**Limitations**
Perimeter-Based Security	- Focuses on protecting the network boundary with firewalls and intrusion detection systems (IDS). - Assumes all internal network traffic is trusted.	- Ineffective against insider threats. - Difficulty in managing BYOD and remote access. - Limited protection against advanced persistent threats (APTs).
VPN (Virtual Private Network)	- Encrypts data transmitted over public networks. - Provides secure remote access.	- Performance issues due to encryption overhead. - Complex management and scalability challenges. - Vulnerable to attacks if endpoints are compromised.
Endpoint Security	- Focuses on securing individual devices using antivirus software, firewalls, and endpoint detection and response (EDR).	- Limited scope, does not protect the entire network. - High dependency on user behavior. - Ineffective against zero-day threats and sophisticated attacks.
Network Access Control (NAC)	- Controls access to network resources based on device compliance and user credentials. - Provides visibility and control over devices on the network.	- Complex implementation and management. - Scalability issues with increasing number of devices. - Limited effectiveness against sophisticated attacks.
Signature-Based Detection	- Uses known signatures of malware and threats to detect and prevent attacks. - Includes antivirus and intrusion detection systems (IDS).	- Ineffective against new, unknown threats. - High false positive rates. - Requires constant updates to signature databases.
Behavior-Based Detection	- Monitors network and user behavior to detect anomalies and potential threats. - Utilizes machine learning and analytics.	- High complexity and resource-intensive. - May produce false positives. - Requires advanced expertise to manage and interpret results.
Role-Based Access Control (RBAC)	- Grants access to resources based on user roles within the organization. - Simplifies management of permissions and access control.	- Can become complex with large organizations. - Difficult to manage dynamic access needs. - Static roles may not adapt well to changing threats.
Security Information and Event Management (SIEM)	- Collects and analyzes security data from various sources. - Provides real-time monitoring and incident response.	- High cost and complexity. - Requires skilled personnel for effective use. - Potential for data overload and false positives.

III. DEPLOYMENT FRAMEWORKS FOR ZTNA

The deployment of Zero Trust Network Architecture (ZTNA) requires a systematic and comprehensive framework to ensure its effective implementation and operation. The following subsections detail the key components and methodologies involved in deploying ZTNA, focusing on main steps, tools, and best practices.

A. *Defining the Zero Trust Security Policy*

The first step in deploying ZTNA involves defining a robust security policy that aligns with the Zero Trust principles of "never trust, always verify." This policy should encompass the following elements:

- *Identity Verification:* Establishing strict identity verification processes for users, devices, and applications. This includes multi-factor authentication (MFA) and continuous monitoring of identity attributes.

- *Access Control:* Implementing access control policies that grant the least privilege necessary for users and devices to perform their tasks. Role-based access control (RBAC) and attribute-based access control (ABAC) can be utilized to enforce these policies.

- *Data Protection:* Ensuring that sensitive data is encrypted both in transit and at rest. Data loss prevention (DLP) tools should be deployed to monitor and control data access and movement.

B. *Network Segmentation*

Network segmentation is a critical component of ZTNA, aimed at limiting the potential threats within the network. This involves dividing the network into smaller, isolated segments, each with its own security controls. Key practices include:

- *Micro-Segmentation:* Using software-defined networking (SDN) and network virtualization techniques to create isolated segments. This limits access to resources based on predefined policies and real-time context.

- *Firewalls and Gateways:* Deploying next-generation firewalls (NGFW) and secure web gateways (SWG) to monitor and control traffic between segments. These tools help enforce security policies and detect anomalous behavior.

C. *Continuous Monitoring and Analytics*

ZTNA relies heavily on continuous monitoring and real-time analytics to detect and respond to security incidents promptly. This involves:

- *Security Information and Event Management (SIEM):* Implementing SIEM systems to collect, analyze, and correlate security events from various sources. SIEM provides real-time visibility into network activities and helps identify potential threats.

- *User and Entity Behavior Analytics (UEBA):* Using UEBA to monitor user and device behavior, detect anomalies, and identify malicious activities. Machine learning algorithms can be used to analyze behavior patterns and generate alerts for suspicious actions.

- *Endpoint Detection and Response (EDR):* Deploying EDR solutions to continuously monitor endpoints for signs of compromise and to enable rapid incident response. EDR tools provide detailed visibility into endpoint activities and facilitate threat hunting.

D. *Secure Access Service Edge (SASE)*

Secure Access Service Edge (SASE) is an emerging framework that integrates networking and security services into a single cloud-delivered solution [14]. SASE provides a scalable and flexible approach to implementing ZTNA by combining the following components:

- *SD-WAN:* Software-defined wide area networking (SD-WAN) optimizes network performance and ensures secure connectivity for remote users and branch offices. SD-WAN enables dynamic traffic routing based on application requirements and security policies.

- *Cloud Access Security Broker (CASB):* CASBs provide visibility and control over cloud applications and data. They enforce security policies, protect against data breaches, and ensure compliance with regulatory requirements [15].

E. *Automation and Orchestration*

Automation and orchestration play a crucial role in the effective deployment and management of ZTNA. Key strategies include:

- *Policy Automation:* Automating the creation, enforcement, and updating of security policies based on predefined criteria and real-time context. This reduces the risk of human error and ensures consistent policy application.

- *Incident Response Automation:* Using automated workflows to respond to security incidents promptly. This includes automated threat detection, containment, and remediation processes.

- *Orchestration Tools:* Deploying orchestration tools to integrate and manage security solutions across the network. These tools provide a unified interface for configuring, monitoring, and controlling security policies and operations.

Table 3 is summarizing the key components of the ZTNA implementation framework:

TABLE IIIII
KEY COMPONENTS OF THE ZTNA IMPLEMENTATION FRAMEWORK

Component	Key Actions
Identity Verification	Implement MFA, continuous monitoring of identity attributes.
Access Control	Use RBAC/ABAC, enforce least privilege access.
Data Protection	Encrypt data in transit and at rest, deploy DLP tools.
Micro-Segmentation	Utilize SDN, network virtualization for granular segmentation.

Firewalls and Gateways	Deploy NGFW and SWG to monitor and control inter-segment traffic.
SIEM	Implement SIEM for real-time security event analysis.
UEBA	Use machine learning for behavior analytics and anomaly detection.
EDR	Deploy EDR solutions for continuous endpoint monitoring and incident response.
SD-WAN	Use SD-WAN for optimized, secure remote connectivity.
CASB	Deploy CASB for cloud application visibility and control.
ZTNA Solutions	Implement ZTNA solutions for secure, identity-based access.
Policy Automation	Automate policy creation, enforcement, and updates.
Incident Response	Use automated workflows for threat detection and remediation.
Orchestration Tools	Deploy orchestration tools for unified security management.
Training and Awareness	Conduct regular security training and simulations.

IV. AUTHENTICATION AND AUTHORIZATION IN ZTNA

Identity and Access Management (IAM) plays an importnt role in the Zero Trust Network Architecture (ZTNA) by ensuring that only authorized users and devices gain access to critical resources. The IAM framework encompasses policies, processes, and technologies that facilitate the management of digital identities, enforce access controls, and monitor user activities. This section presents the key aspects of IAM in the context of ZTNA, focusing on Multi-Factor Authentication (MFA) and Continuous Authentication and Monitoring.

A. Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security mechanism that requires users to provide multiple forms of verification before granting access to a system. Unlike traditional single-factor authentication, which relies solely on a password, MFA combines two or more independent credentials: something the user knows (password), something the user has (smartphone or hardware token), and something the user is (biometric verification). This layered approach significantly enhances security by making it more challenging for attackers to gain unauthorized access.

By requiring multiple forms of verification, MFA reduces the risk of credential theft and unauthorized access. Even if one factor is compromised, the attacker would still need to bypass additional security layers. Modern MFA solutions often incorporate user-friendly methods such as push notifications and biometric authentication, minimizing friction for legitimate users while enhancing security.

To implement MFA effectively, organizations should adopt a risk-based approach, ensuring that MFA is applied consistently across all access points without hindering user productivity. This involves integrating MFA with Single Sign-On (SSO) solutions, using adaptive authentication that adjusts the level of verification based on the context (e.g., location, device, behavior), and ensuring that MFA is part of a broader IAM strategy that aligns with the organization's security objectives.

B. Continuous Authentication and Monitoring

In the Zero Trust paradigm, the assumption that no user or device should be implicitly trusted necessitates continuous authentication and monitoring. Continuous authentication goes beyond the initial login, regularly verifying the user's identity throughout their session based on contextual and behavioral data. This approach ensures that access remains secure even if the user's credentials are compromised after initial authentication.

That can be done by evaluating contextual factors such as the user's location, device, and network to determine the legitimacy of the access request. Monitoring user behavior, such as typing patterns, mouse movements, and interaction habits, can also be used to detect anomalies that may indicate compromised credentials. Another key component is to continuously assessing the risk associated with each access request and adjusting authentication requirements accordingly.

Effective implementation of continuous authentication involves integrating advanced analytics and machine learning algorithms to analyze user behavior and detect anomalies. Organizations should use Identity and Access Management (IAM) solutions that support adaptive authentication, enabling dynamic responses to potential threats. Additionally, establishing clear policies and procedures for incident response and user verification is crucial to ensure that continuous authentication operates smoothly and effectively.

V. CONCLUSION

This article presented a significant discussion of the details about the zero trust security model along with their background and implementation of this model. Zero trust is essentially an initiative from a cybersecurity plan to provide more secure networking and safeguarding resources such as assets, workflow planning, and services. By adopting the zero trust model, organizations can improve their security posture and fortify themselves against cyber threats. The foundation of zero trust is changing to a dynamic, identity-centric, and policy-based approach that makes it reliable to cope with the complexity of enterprise environments.

Therefore, optimize the technology and security architecture for future adaptability.

ACKNOWLEDGMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] J. Kindervag, “No More Chewy Centers: Introducing The Zero Trust Model of Information Security,” Forrester Research, USA, Sep. 14, 2010. [Online]. Available: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

[2] C. Cunningham, “The Zero Trust eXtended (ZTX) Ecosystem, Strategic Plan: The Zero Trust Security Playbook,” Forrester Research, Jul. 11, 2019.

[3] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, 2020

[4] Z. Sun, D. Huang, S. Li, H. Yang, and C. Zhao, “High Efficiency Positioning of Vibration Intrusions for Long Distance Perimeter Security Monitoring Based on Time-Frequency Variation Envelopes,” IEEE Transactions on Instrumentation and Measurement, vol. PP, pp. 1–1, 2024, doi: 10.1109/TIM.2023.3348889.

[5] N. Wagh and Y. Jadhav, “Eclipsing Security: An In-Depth Analysis of Advanced Persistent Threats,” International Journal of Scientific Research in Engineering and Management, vol. 7, pp. 1–11, 2023, doi: 10.55041/IJSREM27653.

[6] B. Mixon-Baca, J. Knockel, D. Xue, T. Ayyagari, D. Kapur, R. Ensafi, and J. Crandall, “Attacking Connection Tracking Frameworks as Used by Virtual Private Networks,” Proceedings on Privacy Enhancing Technologies, vol. 2024, pp. 109–126, 2024, doi: 10.56553/popets-2024-0070.

[7] S.-J. Lee, S.-E. Jeon, and I.-G. Lee, “A machine learning-enhanced endpoint detection and response framework for fast and proactive defense against advanced cyber attacks,” Soft Computing, pp. 1–15, 2024, doi: 10.1007/s00500-024-09727-7.

[8] M. Wa Nkongolo and M. Tokmak, “Zero-Day Threats Detection for Critical Infrastructures,” arXiv preprint, 2023. doi: 10.48550/arXiv.2306.06366.

[9] M. Xu, B. Chen, Z. Tan, S. Chen, L. Wang, Y. Liu, T. San, S. Fong, W. Wang, and J. Feng, “AHAC: Advanced Network-Hiding Access Control Framework,” Applied Sciences, vol. 14, no. 5593, 2024, doi: 10.3390/app14135593.

[10] M. Schroetter, A. Niemann, and B. Schnor, “A Comparison of Neural-Network-Based Intrusion Detection against Signature-Based Detection in IoT Networks,” Information, vol. 15, no. 164, 2024, doi: 10.3390/info15030164.

[11] A. Badea, V. Croitoru, and D. Gheorghica, “Computer networks security based on the detection of user’s behavior,” in Proceedings of the International Symposium on Advanced Topics in Electrical Engineering (ATEE), 2015, pp. 55–60, doi: 10.1109/ATEE.2015.7133679.

[12] S. Ramakrishnan, “Revolutionizing Role-Based Access Control: The Impact of AI and Machine Learning in Identity and Access Management,” Journal of Artificial Intelligence & Cloud Computing, vol. 2, pp. 1–7, 2023, doi: 10.47363/JAICC/2023(2)236.

[13] M. Jhaveri and V. Parmar, “CLOUD Security Information and Event Management,” GIS-Zeitschrift fü Geoinformatik, vol. 10, pp. 13, 2023.

[14] A. Ragula, “Emerging Trends in Cloud Security: Zero Trust and SASE,” International Journal for Research in Applied Science and Engineering Technology, vol. 12, pp. 10–17, 2024, doi: 10.22214/ijraset.2024.62457.

[15] P. Selvam, “Secure Cloud Services by Integrating CASB Based Approach,” International Journal of Scientific Research in Engineering and Management, vol. 4, 2022, doi: 10.55041/IJSREM15210.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 1 (2025)
https://doi.org/10.31436/ijpcc.v11i1.510

A Study on the Classification of Brain MRI Images for Brain Tumor Detection

A Comparative Analysis

MST Mobasshira Sadia Tanjim, Suhaina Moinuddin, Amelia Ritahani Ismail*
Department of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia

*Corresponding author amelia@iium.edu.my

(Received: 10th December 2024; Accepted: 27th December, 2024; Published on-line: 30th January, 2025)

Abstract**—** Accurate classification of brain tumors is essential for effective diagnosis, as it directly affects treatment choices, patient outcomes, and survival rates. Early and precise detection enables timely interventions, reducing the risk of tumor progression. Without reliable classifiers, traditional feature extraction techniques have drawbacks. Our study suggests a hybrid model that incorporates the advantages of Random Forest Classifier (RFC), Support Vector Machine (SVM), and Visual Geometry Group (VGG16) to improve classification performance. To improve feature extraction, the Magnetic resonance imaging (MRI) images are pre-processed. This includes pixel intensity. To improve data diversity, augmentation techniques such as random flip, random height, random width, horizontal flip, and vertical flip are used. Next, a unique Deep Convolutional Neural Networks (DCNN) that is VGG16 is created to extract significant deep features. Evaluation of the model's performance using various optimizers revealed that the RMSprop optimizer outperformed models employing Adam (80.39%) and SGD (64.71%), achieving the highest validation accuracy (82.35%). SVM obtained a validation accuracy of 47.06%, while RFC obtained 64.71%. These results show the importance of classifier and optimizer selection. This study highlights the efficacy of the VGG16 model with the RMSprop optimizer and shows the potential of integrating deep learning and conventional machine learning approaches for brain tumor classification. It demonstrates the potential of combining deep learning and traditional machine learning techniques for brain tumor classification, highlighting effectiveness of the VGG16 model with the RMSprop optimizer while emphasizing the need for further exploration of optimizers and classifiers to enhance overall model performance and robustness.

Keywords— Brain tumor, MRI scan, Deep learning, Optimizer, Classifier

I. Introduction

The rapid growth in technology has been drastically changing the arena of medical science and, simultaneously, impelling a profound effect on the technique of diagnosis. Deep learning combined with sophisticated computers made various innovative methods possible, especially in the field of medical imaging. The focus is on the critical task of brain tumor classification, utilizing the latest advancements in deep learning to enhance diagnostic accuracy; therefore, the contribution to this rapidly evolving field is significant.

Brain tumors represent an abnormal growths of brain tissue. There are over 120 diverse types of brain tumors, only some of which are malignant. Brain tumors, including malignant ones, accounted for 18,020 adult deaths in the US in 2020, making them the tenth most common cause of death [1]. The variety of tumor forms, such as pituitary tumors, meningiomas, and gliomas, highlights how difficult the situation is. Because brain tumors can quickly become life-threatening and require adequate therapy for patient survival, the importance of early diagnosis is emphasized. In this diagnostic process, medical imaging modalities like computed tomography (CT), magnetic resonance imaging (MRI), and X-rays have become essential tools. Image classification performance has greatly improved with the shift from human to machine-dependent processes, especially in computer-aided design (CAD) systems, where image classification performance now much exceeds that of manual detection.

This introduction sets the context by highlighting recent developments and trends in the field. It emphasizes the importance of technology advancements and their influence on medical knowledge, setting the stage for the study's specific focus on brain tumour classification. The study explores the complexities of feature extraction, post-processing, and preprocessing processes in the CAD system process. It uses methods like noise reduction, image smoothing, and scaling to maximize the input data because it understands how important image preprocessing is. Furthermore, it recognizes the vital role that post-processing methods in particular, segmentation procedures play in enabling the extraction of tumour areas from MRI data. The significance of feature extraction methods in obtaining appropriate features for later classification is emphasized throughout the paper.

The paper presents the most recent developments in deep learning while keeping an eye on the shortcomings of conventional machine learning classifiers. Deep learning, an acknowledged subfield of machine learning, enables computers to learn from data and make judgments. Deep learning is less reliant on preprocessing, which reduces the complexity involved in choosing segmentation processes, feature extraction processes, and classifiers. To improve brain tumor classification accuracy, the paper presents a unique hybrid strategy that combines a Support Vector Machine (SVM) classifier with a Deep Convolutional Neural Network (DCNN: VGG16) and a Random Forest Classifier (RFC) classifier with a Deep Convolutional Neural Network (DCNN: VGG16) for deep feature extraction. The hybrid structure's justification is to overcome the shortcomings of conventional approaches and maximize the core strengths of both deep learning and traditional machine learning classifiers. This provides the way for a comprehensive review of the research's details and highlights its innovative and important applications in the quickly developing field of medical image classification.

II. Literature Review

With the use of several artificial intelligence (AI) algorithms, the classification of brain tumors has advanced significantly. Magnetic Resonance (MR) image feature extraction and subsequent classification based on these retrieved characteristics are critical steps in this complex process. Researchers have worked hard to enhance the traditional classification techniques; below is a thorough rundown of some important studies in this area.

A "Figshare" dataset was used in the work of Biswas et al. [2]. Nevertheless, there were issues with their work, including low data volumes, expensive MRI processing, and decreased accuracy. Damodharan et al. utilized a neural network for brain tumor detection, integrating various classifiers, including Bayesian and K-Nearest Neighbors (KNN), along with multiple preprocessing techniques. Despite KNN achieving an accuracy of 83%, the study faced limitations due to the small dataset used, which affected the generalizability of the findings [3].

Abiwinanda et al. proposed a feature extraction and classification approach entirely based on Convolutional Neural Networks (CNNs) without any preprocessing stages. In their study, the softmax classification layer yielded poor performance despite achieving 84.19% accuracy on the dataset used, highlighting the effectiveness of the CNN-SVM model and the importance of incorporating preprocessing steps for improved results [4].

Khan et al. investigated the application of transfer learning for the classification of brain tumors, employing the VGG19 architecture, which resulted in an accuracy of 94.82%. However, they noted that transfer learning requires significant processing power and involves complex network structures [5].

Pashaei et al. achieved an accuracy of 93.68% by combining Convolutional Neural Networks (CNNs) for feature extraction with an extreme learning machine for classification. Notably, the proposed CNN architecture outperformed both RBF and SVM classifiers. Other experiments utilized different hybrid models, focusing on identifying the most effective feature extraction techniques [6].

Kurmi et al. utilized an MLP classifier, achieving an average accuracy of 91.76%. Their work focused on image enhancement, tumor area initialization, and region refinement, contributing to more effective brain tumor detection [7].

Mahesh and Yogesh proposed a Convolutional Neural Network (CNN)-based approach for brain tumour identification and classification that achieved 97.5% test accuracy across four classes: meningiomas, pituitary tumours, gliomas, and no tumour. Using a strong CNN architecture, their method successfully solved the drawbacks of previous research, which included issues like short datasets or insufficient preprocessing. The model's excellent accuracy and recall across all tumour classifications indicated its dependability and efficacy in supporting diagnosis.[8]

To classifying brain tumours in MRI images, Musa suggested a hybrid deep learning method that combines optimised Softmax Regression with ResNet-50. With an outstanding 98.4% accuracy rate, the technology outperformed current methods for automatically detecting brain tumours. This model showed notable gains in diagnostic performance, making it a useful tool for radiologists. This contrasts with previous research, which frequently struggled with restrictions including the accuracy with poor result and high computational cost [9].

This study outperforms previous research, such as that of Damodharan et al., who used a neural network that included KNN and Bayesian classifiers. Their model had issues because of the tiny dataset, which limited its generalisability even if it achieved 83% accuracy. Like this, Abiwinanda et al. used a CNN-based feature extraction method, however because preprocessing was not used, the softmax classifier's performance suffered and they only obtained 84.19% accuracy.

Mohanty and Sarmadi proposed a deep learning method for classifying brain tumours in MRI images that makes use of convolutional neural networks (CNNs). By achieving 97%

accuracy in tumour identification and 98% accuracy in tumour classification, their model made significant improvements in better targeted treatment and early diagnosis. The system's usability and strong performance in clinical applications were shown by utilising optimisation approaches [10].

Aykat developed a deep learning model for brain tumour identification based on MRI images, using three pre-trained convolutional neural networks as feature extractors and attaining an astonishing 99.58% accuracy with four distinct classifiers. This method beat established approaches and prior CNN-based models, indicating the possibility of improved diagnostic accuracy and reliability in medical applications [11].

Leal et al. proposed a deep learning model for brain tumour classification using Convolutional Neural Networks (CNNs) on MRI images, with a focus on glioma, meningioma, and pituitary tumours. The VGG16 model beat ResNet50 and InceptionV3, having the accuracy of 98.36% and precision of 98.12%, with high recall rates and F1-scores for all tumour types, especially pituitary tumours (100% recall). ResNet50 produced comparable findings, but with lower accuracy (98.28%) and precision (97.56%), whilst InceptionV3 trailed with 93.68% accuracy and 88.56% precision. This work demonstrates VGG16's usefulness for automated brain tumour classification, proving its superiority over other models and emphasising its potential for aiding with early diagnosis and treatment planning in clinical settings.[13]

The literature review offers a thorough summary of developments in the classification of brain tumours using deep learning methods and MRI images. It successfully charts the development from older techniques that suffered from constraints like short datasets, inadequate preprocessing, and mediocre accuracy to more contemporary strategies that make use of innovative CNN architectures and hybrid models. Iterative increases in accuracy, precision, recall, and F1-scores are highlighted by the inclusion of several comparison studies, highlighting the importance of model selection and optimisation in attaining better results.

The review's critical evaluation of earlier research, highlighting both its advantages and disadvantages, is one of its main strengths. As an example, it recognises the work of scholars such as Damodharan et al. and Abiwinanda et al. but also highlights their limited generalisability and absence of preprocessing. In the same way, the review demonstrates the effectiveness of sophisticated CNNs and hybrid approaches by highlighting the notable improvements made by models such those put out by Mahesh and Yogesh, Musa, Aykat, and Leal et al.

The literature review concludes by highlighting the quick progress in classifying brain tumours and showing how each study builds on the one before it to get beyond prior challenges. The rise of highly reliable models, such as those developed by Aykat and Leal et al., suggests that deep learning methods are developing into credible tools for medical diagnosis. However, to guarantee broad application in real-world situations, further effort is required to solve issues including dataset variety, computational efficiency, and clinical validation.

III. METHODOLOGY

MRI brain tumor classification and segmentation have seen significant advancements with the application of Convolutional Neural Networks (CNNs), given their remarkable ability to capture intricate features in medical imaging. In this study, we focus on developing and evaluating CNN-based models to detect brain tumors from MRI scans. By utilizing the powerful VGG16 architecture and its hybrid variants, we aim to achieve precise classification of MRI images into "YES" or "NO" categories, indicating the presence or absence of brain tumors. Our approach leverages supervised learning on a well-curated dataset, facilitating a robust model capable of aiding in critical healthcare diagnostics (see Figure 1).

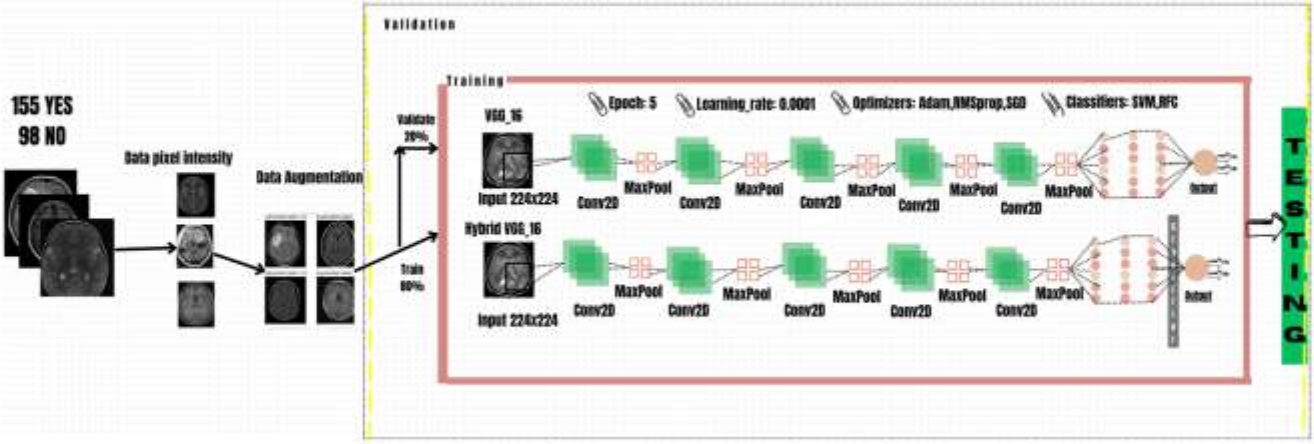
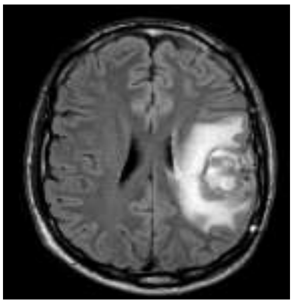
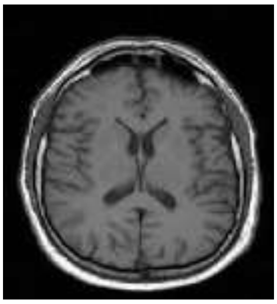


Fig 1. The Training Model

A. *Data Collection*

We collected our Brain MRI image dataset from Kaggle, specifically from the "Brain MRI Images for Brain Tumor Detection" collection by Navoneel. This dataset is publicly accessible, enabling researchers to build models for brain tumor classification. Building two main models is the main goal of the project; the VGG16 design will be the focus, but there will also be other research done on hybrid VGG16 variants. Using MRI images, the models perform a binary classification task to determine if a subject has a brain tumor or not. They do this by differentiating between a "YES" class that indicates a tumor is present and a "NO" class that indicates it is not. Included in the sample are 155 occurrences labelled as "YES," indicating abnormal brain tissues with tumors, and 98 instances labelled as "NO," standing for normal brain tissues. By including both typical and unusual events, the dataset is enhanced. For supervised learning—where the models learn from labelled examples—images must be labelled as either having or not having a tumor. The hybrid version being investigated and the VGG16 architecture selected to demonstrate a purposeful approach to obtaining precise and trustworthy classification findings in this crucial healthcare (see Table 1).

TABLE I
VISUALIZATION OF SAMPLE DATASET

"YES" Labelled	"NO" Labelled
	

B. *Data Preprocessing*

A crucial first step in our preparation of the data for brain tumour diagnosis was finding and dropping corrupted files from the dataset. Six of the "No"-labelled files were found to be corrupted and could not be processed further. That's why, to protect the accuracy and consistency of the remaining data, these files were manually removed from the dataset. A refined dataset with 92 "No" labelled data files for the non-tumor class and 155 "Yes" labelled data files for the tumor class was obtained after this cleanup step, and the preprocessing process continued. This corruption-free selection served as the foundation for other preprocessing procedures such as pixel intensity analysis and data augmentation. Two essential steps have been combined in the data preprocessing process of our study for brain tumor detection to maximize the dataset for training machine learning models. First, a thorough examination of pixel intensities in two distinct classes "Yes" (tumor) and "No" (non-tumor) was done. Plotting pixel value histograms allowed for a thorough visualization of the distribution characteristics. This analysis made it easier to spot trends and variances in pixel brightness, which helped inform further preprocessing decisions. Based on these insights, techniques such as contrast adjustment or normalization can be customized to guarantee pixel value constancy and improve the model's ability to show features that correspond to tumors (see Figure 2 and 3).

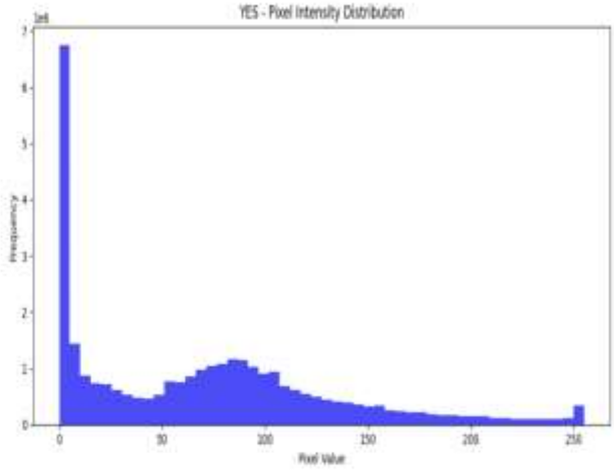


Fig 2: Distribution Characteristics of Pixel Intensity

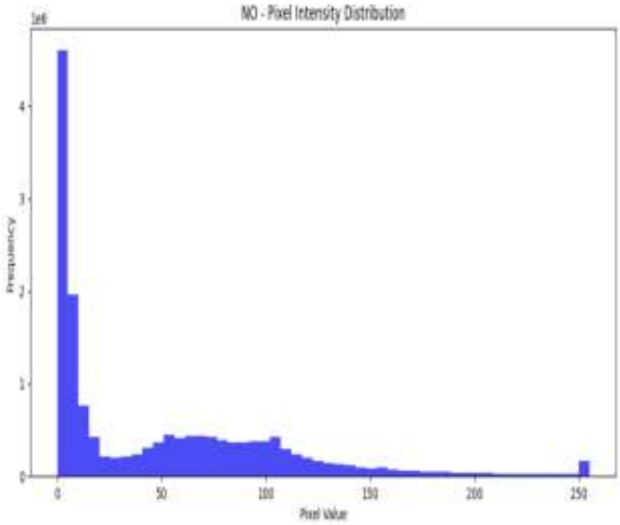


Fig 3: Distribution Characteristics of Pixel Intensity

Additionally, picture augmentation techniques were used to enhance the dataset's diversity and enrichment even more. The training images were subjected to a variety of changes, including random height and width adjustments, horizontal flipping, and bespoke image augmentation using a custom Sequential model created with TensorFlow's "ImageDataGenerator." By adding variability to the dataset, this augmentation procedure helps the model generalize to previously unobserved data more successfully and avoids overfitting (see Figure 4 and 5).

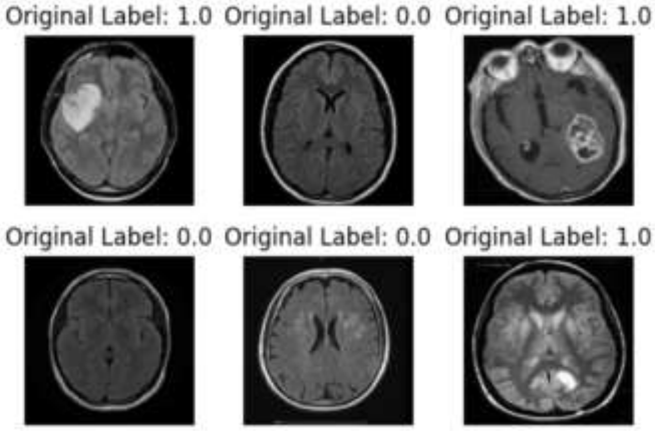


Fig 4: Original Data

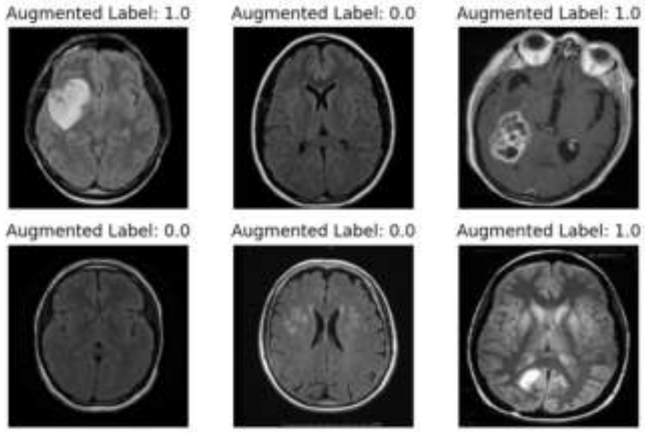


Fig 5: Augmented Data

C. *Model Architecture*

The Visual Geometry Group at the University of Oxford developed the VGG16, a deep convolutional neural network that is well-known for its ease of application and efficacy in image categorisation applications. Thirteen convolutional layers, five max-pooling layers, and three fully linked layers make up the architecture's sixteen weight layers. It is called "VGG16" because of its 16 weight layers, even though it has 21 layers overall. The convolutional layers efficiently capture local information while supporting spatial resolution by using tiny 3x3 filters with a stride of 1 and the same padding. Each block of convolutional layers is followed by max-pooling layers, which provide translation invariance and reduce computational cost by down sampling feature maps. For the ImageNet dataset, the fully connected layers are constructed with 1,000 neurones in the output layer and 4,096 neurones in the first two levels. VGG16's resilience in object identification and classification is showed by its impressive 92.7% accuracy on ImageNet. Throughout, the network uses Rectified Linear Unit (Re-LU) activation functions to introduce non-linearity. To improve generalisation, the network also periodically uses Local Response Normalisation (LRN). VGG16, a basic model in deep learning, was created for input pictures with a pixel size of 224 x 224. Its balanced design and constant use of tiny filters have sparked advances in both research and real-world applications.

D. Data Training

Using the VGG16 architecture, a binary classification model for brain tumor detection was developed during the training phase. First, extra thick layers were added to the pre-trained VGG16 base that served as the model's foundation, leaving off the top classification layer. To preserve learned features, the layers of the basic model were frozen. The model was then constructed using various optimizers, such as Adam, RMSprop, and SGD. The model was also constructed with two traditional machine learning classifiers such as SVM and RFC. After that, the model was trained through five epochs using the training dataset. The training procedure involved minimizing the divergence between the expected and actual labels by iteratively modifying the model's weights depending on the computed loss. The model's generalizability to previously unknown data was assessed by analysing its performance on a different validation dataset. Accuracy and loss were among the training parameters that were examined to evaluate the convergence and performance of the model.

E. *E. Data Testing*

During the testing phase, the validation dataset was used to assess the trained model's performance on fresh, unseen samples. In addition, the pre-trained VGG16 model was used to extract features using other classifiers like Random Forest and Support Vector Machines (SVM). The validation dataset was used to test these classifiers once they had been trained using the acquired features. To determine how well each model performed in comparison to the others, the attained accuracies were compared. Notably, the RMSprop optimizer-equipped VGG16 model showed the highest validation accuracy at 82.35%, highlighting the importance of optimization decisions for model performance. An efficient brain tumor detection system has been produced by following a methodical process from data collection, preprocessing, model architecture design, training, and testing phases. This method provides a dependable tool for precise brain tumor diagnosis, proving the potential of machine learning in medical diagnostics. Sustained efforts to improve the model will be essential to its success in practical healthcare applications.

IV. Results and Discussion

Metrics like precision and recall are often prioritized in medical diagnosis and research, and the AUC/ROC curve offers information on the efficacy of the model. In instances where datasets are imbalanced, as is prevalent in real-world medical settings, precision—which measures the accuracy of positive predictions—and recall—which measures the model's ability to detect all actual positive cases—become extremely important. As an example, we can consider COVID-19 detection, where it is crucial to avoid false negative results because of the virus's infectious nature. The most important thing is to make sure the right steps are taken to stop the spread and not mistakenly categorize a patient who tests positive for COVID-19 as negative. When diagnosing high-risk diseases like cancer or brain tumors, recall becomes a more important evaluation criterion than precision. Since false positives typically have less of an impact, it is undesirable to miss actual positives. A false negative in these circumstances could have serious repercussions and put the patient's life in danger.

When it comes to brain tumor identification, it is crucial to avoid false negative results because of the condition's possible severity. Ensuring prompt medical interventions and therapies for patients with brain tumors depends on the precise identification of those affected. In this situation, false negative results could cause a delay in diagnosis and treatment, which could have an impact on patient outcomes. Reducing false negatives is crucial when dealing with high-risk conditions like brain tumors to prevent situations that need immediate medical treatment from going unnoticed. We have calculated validation accuracy for all our models. The percentage of right predictions a machine learning model makes on a different dataset that was not used for training is known as validation accuracy. It aids in evaluating the model's ability to generalize to fresh, untested data. Precision and recall metrics are typically more important than accuracy in medical cases and diagnosis. Achieving a balance between false positives and false negatives is crucial in medical circumstances. aiming for high recall is often more crucial in situations where false negatives—missing a positive case—can have serious repercussions for the patient than aiming for overall accuracy. For patient outcomes and public health, precision and recall offer more detailed insights into a model's performance in recognizing positive cases and preventing false negatives.

The discrimination ability of a model is evaluated by the AUC/ROC curve, which shows the trade-off between recall and precision. More recall is indicated by a steeper ROC curve, even though it does not directly show precision and recall. The AUC/ROC curve supports precision-recall calculations in medical instances, particularly when there is imbalanced data. It offers information on how effectively a model strikes a balance between recall and precision for efficient disease identification. The F1 score is a metric that combines both precision and recall into a single value. While analyzing the result, a huge focus has been placed on the results of the Yes subset as well as on Recall and Precision.

In our analysis, both VGG16 + Adam Optimizer and VGG16 + RMSprop Optimizer achieved good overall accuracy (80.39% and 82.35%, respectively). However, when considering the AUC curve, VGG16 + Adam performed better with a score of 54.04%. Upon closer examination of recall results for the "Yes" subfolder, VGG16 + Adam showed superior performance, capturing more actual positive cases. Meanwhile, for precision in the "Yes" subfolder, VGG16 + RMSprop outperformed.In the "No" subfolder, VGG16 + RMSprop demonstrated better results across precision, recall, and F1 Score.To summarize, while VGG16 + Adam excelled in overall AUC, VGG16 + RMSprop showed strengths in precision, recall, and F1 Score, particularly for the "No" subfolder. The VGG16 + SGD Optimizer attained ROC/AUC 45.29% which is considered poor, and performed well for the 'Yes' subfolder, giving a perfect score of 1.00 for recall, 0.65 for Precision, hence having a higher F1 Score of 0.79.But the precision, recall and F1 Score for the 'No' subfolder is 0.A recall of 0 for the "No" class suggests that the model is missing all instances of the positive class within the "No" category. Based on performance coming in next is the VGG16 + RFC hybrid algorithm, having 0.61 Precision and 0.70 recall for the 'Yes' subfolder and 0.23 precision, and 0.17 recall for No subfolder.The last algorithm explained is the VGG16 + SVM hybrid algorithm, it has maintained the same score of Precision, recall, and F1 score, 0.61 for 'Yes' as well as the same score of Precision, recall, and F1 score, 0.28 for 'No' subfolder (see Table 2).

TABLE II
Performance Evaluation of the models

Model	Validation accuracy	ROC-AUC	Precision	recall	F1-Score
VGG16 +Adam Optimizer	80.39%	54.04%	Yes:0.67	0.79	0.72
			NO:0.42	0.28	0.33
VGG16 + RMSprop Optimizer	82.35%	46.805%	Yes: 0.69	0.76	0.72
			NO: 0.47	0.39	0.42
VGG16 + SGD Optimizer	64.71%	45.29%	Yes:0.65	1.00	0.79
			No:0.0	0.0	0.0
VGG16 + RFC	64.71%	42.85%	Yes:0.61	0.70	0.65
			No:0.23	0.17	0.19
VGG16 + SVM	47.06%	39.06%	Yes:0.61	0.61	0.61
			NO: 0.28	0.28	0.28

V. Conclusion

By advancing better healthcare results, our research on developing a trustworthy hybrid model for brain tumor classification is in line with medical and sustainable development objectives. One of the main goals of sustainable development is to promote health and well-being. We address the crucial need for precise medical diagnoses, guaranteeing prompt interventions and therapies for patients with brain tumors, by giving precision and recall top priority in our models. The incorporation of advanced approaches such as the DCNN VGG16, RFC, and SVM highlights the dedication to using technology to improve medical decision-making, which is in line with guaranteeing healthy lives and fostering well-being for everybody.

In addition, our focus on customized metrics and hybrid techniques shows our dedication to the advancement of medical technology and research, which is a crucial part of sustainable development. We work to improve the effectiveness and dependability of brain tumor identification by combining machine learning models with conventional classifiers, supporting the overall goal of reaching universal health care and minimizing health disparities. The AUC/ROC curve's complex interpretation shows our commitment to fine-tuning models for practical medical applications, which will lead to more patient outcomes and sustainable healthcare practices.

Future research should focus on fine-tuning model parameters, optimizing learning rates for optimizers, and adjusting parameters related to Random Forest Classifier (RFC) to enhance overall model performance. Implementing advanced data augmentation techniques customized for medical imaging can contribute to better generalization. Exploring ensemble approaches that combine deep learning, and traditional classifiers may lead to potential performance improvements. Ensuring model interpretability through techniques like SHAP or LIME is crucial for showing trust in clinical settings. Addressing class imbalance, obtaining validation from clinical experts using diverse datasets, and conducting robustness testing across varying imaging conditions are essential for practical applicability. In summary, refining parameters, improving interpretability, and addressing practical challenges are critical areas for future research to confirm the model's effectiveness in clinical practice.

ACKNOWLEDGMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

References

[1] N. Dey, "Brain MRI Images for Brain Tumor Detection," Kaggle, Available: https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor-detection. [Accessed: Jan. 19, 2024].

[2] Hopkins Medicine, "Brain tumor types," Johns Hopkins Medicine, https://www.hopkinsmedicine.org/health/conditions-and-diseases/brain-tumor/brain-tumor-types. Accessed Nov. 4, 2024.

[3] A. Biswas and Md. Saiful Islam, "A hybrid deep CNN-SVM approach for brain tumor classification," *Journal of Information Systems Engineering and Business Intelligence*, vol. 9, no. 1, pp. 1–15, 2023. doi: 10.20473/jisebi.9.1.1-15.

[4] S. Damodharan., and Ananthakrishnan, R., "Combining tissue segmentation and neural network for brain tumor detection," ResearchGate,2016.Available: https://www.researchgate.net/publication/281765886_Combining_Tissue_Segmentation_and_Neural_Network_for_Brain_Tumor_Detection

[5] B. R. M. Prabhu and R. K. J. Kumar, "Convolutional Neural Network Based Brain Tumor Classification," in Advances in Computing and Data Sciences, A. P. B. Maheshwari and D. P. S. Kaur, Eds. Singapore: Springer, 2017, pp. 301-311. doi: 10.1007/978-981-10-9035-6_33.

[6] A. Khan, M. I. U. Rahman, M. A. A. Khan, and M. N. M. Ali, "Transfer Learning with Pre-trained CNNs for MRI Brain Tumor Multi-Classification: A Comparative Study of VGG16, VGG19, and Inception Models," in 2021 IEEE International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, Malaysia, 2021, pp. 263–267. doi: 10.1109/ICCCE50845.2021.10352589.

[7] A. Asri, A. J. Anwar, and F. M. Mukhtar, "Brain Tumor Classification via Convolutional Neural Network and Extreme LearningMachines,"2018.Available: https://www.researchgate.net/publication/329559254_Brain_Tumor_Classification_via_Convolutional_Neural_Network_and_Extreme_Learning_Machines. [Accessed: Nov. 4, 2024].

[8] K. R. K. Naik, H. A. L. A. Abdul, A. G. Jain, P. K. A. M. V. Kumar, and A. S. S. Shukla, "A hybrid fuzzy brain-storm optimization algorithm for the classification of brain tumor MRI images," IET Image Process., vol. 14, no. 5, pp. 884–891, 2020. doi: 10.1049/iet-ipr.2019.1631.

[9] G. Mahesh and K. M. Yogesh, "Brain Tumor Detection and Classification Using MRI Images," *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 12, no. 10, Oct. 2024.Available: https://www.ijraset.com/best-journal/brain-tumor-detection-and-classification-using-mri-images[Accessed: Nov. 28, 2024].

[10] M. Musa, "MRI-Based Brain Tumor Classification using ResNet-50 and Optimized Softmax Regression", INFOTEL, vol. 16, no. 3, pp. 598–614, Sep. 2024. doi: 10.20895/INFOTEL.v16i3.1175

[11] N. Mohanty and M. Sarmadi, "Brain tumor MRI classification and identification using an image classification model via Convolutional Neural Networks," medRxiv, Sep. 2024. doi: 10.1101/2024.09.13.23299832.

[12] Ş. Aykat, "Brain Tumor Detection from Brain MRI Images with Deep Learning Methods," 2024 8th International Artificial Intelligence and Data Processing Symposium (IDAP), 2024, doi: 10.1109/IDAP64064.2024.10710648.

[13] L. Leal, F. D. C. A. Lima, R. A. L. Rabêlo, and M. J. A. Moraes, "Brain tumor classification model using convolutional neural networks on magnetic resonance imaging," 2024, doi: https://doi.org/10.54033/cadpedv21n9-025