International Journal on Perceptive and Cognitive Computing

Volume 10, Issue 2, Year 2024

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. 10 No. 2 (2024): July 2024
DOI: https://doi.org/10.31436/ijpcc.v10i2

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.

Editorial Team

TABLE OF CONTENT

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.468

Suicide Risk Prediction Using Artificial Intelligence

Elean Sugafta Rafa, Adeeba Mahmooda, Takumi Sase*
Dept. of Computer Science, KICT, International Islamic University Malaysia, 53100 Kuala Lumpur, Malaysia.

*Corresponding author: takumi@iium.edu.my
(Received: 8th May 2024; Accepted: 25th June 2024; Published on-line: 30th July 2024)

Abstract— Over the past decade, social media has been attracting a growing number of people to the online space. Due to the increase in internet usage, a huge number of text data has been produced. Such data can reflect users' mental health status, but it is still challenging to predict suicide risk from data, due to the high complexity of texts. This research aims to predict the suicide risk from Reddit posts using artificial intelligence (AI). The data were collected from the Kaggle dataset, which included postings of suicide subreddits. The data were pre-processed through natural language processing techniques. Logistic regression, naive Bayes, and random forest models were then used for classifying the Reddit users, i.e., to predict if they are in a suicidal or non-suicidal mental state. These models were compared to identify an AI approach that provides the best performance among the three models. Then, the logistic regression model with doc2vec showed the highest precision of 0.92, recall 0.92, and F_1 score of 0.92.

Keywords— Suicide Risk, Artificial Intelligence, Machine Learning, Reddit

I. Introduction

The sad reality is that a lot of individuals in contemporary society are so stressed or hurt that they think of taking their own life. According to the reports, 703 000 individuals attempted suicide annually [1]. Even more alarming are the findings of a recent study conducted on 32 children's hospitals in the United States [2]. The study revealed a steady rise in the incidence of serious self-harm and suicide among children and adolescents between 2008 and 2015. Among teenagers, there is a noticeable tendency to discuss suicide pacts, seek methodological guidance, and post suicidal thoughts in online groups on social media [3].

The Reddit is a social media platform where users can post content, ask questions, and receive answers [4]. With more than 330 million active users worldwide, Reddit is expanding at twice the rate of Twitter. Subreddits are groups on Reddit where content is categorised. One subreddit, called 'SuicideWatch', was founded in 2008 with approximately 214000 users. Members can use this platform to share their suicidal thoughts or leave encouraging remarks.

Since social media data as in Reddit can reflect users' mental health, many studies have attempted to detect suicide risk from the postings using artificial intelligence (AI) [4-6]. For example, a study analysed the data posted on 'SuicideWatch' to identify patterns in individuals, ranging from the stage of suicidal thoughts to the stage of suicide attempts, using a deep learning approach [4]. However, it is still challenging to perform suicide risk prediction due to the high complexity of text data.

The objectives of this research are to construct the models that can classify social media users as suicidal or non-suicidal through training, to evaluate the performance of the models through testing, and to suggest an AI algorithm that can be used for suicide risk prediction. The algorithm will consist of natural language processing (NLP), training, and classification.

This significance of this research is to provide an AI algorithm that can help the prediction of suicide risk based on Reddit. The algorithm comprises an NLP technique and a machine learning model. A good combination of an NLP technique and a machine learning model was determined through comparison of the three models: logistic regression, naive Bayes, and random forest. The doc2vec was used as NLP preprocessing for the logistic regression. For the naive Bayes model, bag-of-words (BOW) and term frequency–inverse document frequency (TF-IDF) were used as NLP preprocessing and compared. The data were collected from the two subreddits: 'SuicideWatch' and 'depression'.

The rest of this paper is organised as Literature Review, Materials and Methods, Results, and Conclusions. The Literature Review will show recent research related to suicide risk prediction using AI. The Materials and Methods section consists of four parts: Data Collection, NLP Preprocessing, Classification Models, and Model Evaluation. The Results section displays the performance of each model, and this research will be summarised in Conclusions.

II. Literature Review

A methodology for building a suicidal ideation detection was proposed based on social media using deep learning

and machine learning models [5]. They used a model consisting of convolutional neural network (CNN) and bidirectional long short-term memory (LSTM), in addition to the XGBoost model, to classify social posts as suicidal or non-suicidal. The data were collected from the subreddit 'SuicideWatch', and TF-IDF and word2vec were used for text representation. The accuracy, precision, recall, and F_1 score of the CNN-bidirectional LSTM model were 0.95, 0.943, 0.949, and 0.95, respectively. This model outperformed the XGBoost model whose accuracy was 0.915. The study suggests that the proposed method may help identify individuals who require medical treatment [5].

Another research extracted several informative sets of features, to detect suicidal ideation [6]. The suicidal ideation texts were collected from a subreddit 'SuicideWatch'. On the other hand, the texts without suicidal content were collected from other popular subreddits. The study compared six classifiers: support vector machine (SVM), random forest, gradient boost classification tree, XGBoost, multilayer feed forward neural network, and LSTM. Among the six models, the XGBoost using TF-IDF showed the best performance; the accuracy, precision, recall, and F_1 score were 0.9571, 0.9499, 0.9668, and 0.9583, respectively [6].

Twitter was also used for detecting suicide risk [7, 13]. A study collected 14701 suicide-related tweets and compared the two machine learning models: SVM and logistic regression [7]. The results showed that the SVM with TF-IDF and without word removal can be the best performing algorithm. The study suggests that it is possible to distinguish the level of suicidality using machine learning [7]. Another study generated an algorithm for predicting future risk to suicidal ideation [13]. The study constructed neural networks to infer psychological weights. The area under the curve (AUC) of this model was 0.68, and this value was significantly higher than 0.63 that was the AUC of SVMs. The study further used random forest models to predict suicidal ideation, achieving an AUC of 0.88 [13].

A review has been done through 296 studies mainly based on the following countries: USA (47%), Korea (24%), and Canada (18%), regarding AI and suicide prevention [11]. Among the 296 studies, the PRISMA criteria identified 17 studies that were published between the years of 2014 and 2020. Four prospective designs and thirteen retrospective designs were presented in the research using the sample sizes ranging from 182 to almost 19 million. The AI models that were used in these studies are SVM (12%), gradient-boosting algorithms (18%), random forest (35%), logistic regression (53%), and LASSO (12%) [11]. The AUC was ranging between 0.604 to 0.947 in predicting suicide risk. The paper highlighted the potential applications of AI in assessing suicide risk.

A recent study demonstrated the effectiveness of explainable AI for suicide risk prediction [12]. A dataset was selected according to the three criteria and collected [12]. They used random forest, decision tree, logistic regression, SVM, perceptron, and XGBoost. The random forest shows the best performance among the six models; AUC was more than 0.97.

Overall, the choice of a classification model that enables suicide risk prediction can depend on dataset analysed. In this research, we focused on the data posted on Reddit, especially on the two subreddits: 'SuicideWatch' and 'depression'. As shown below, we compared the three models: logistic regression, naive Bayes, and random forest.

III. Materials and Methods

Figure 1 presents the flow of this research. Data Collection, NLP Preprocessing, Classification Models, and Model Evaluation are presented in turn. All the analyses were conducted using Python code.

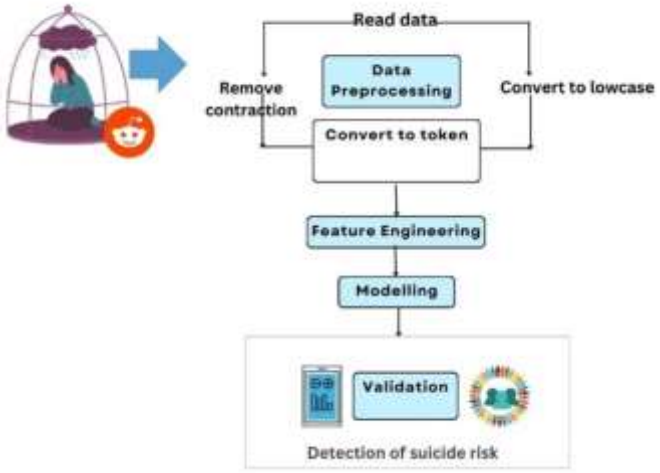

Fig. 1 Methodology Flowchart

A. Data Collection

A dataset of suicide detection datasets was collected from the Kaggle dataset [14], which contains posts of the two Reddit platforms: 'SuicideWatch' and 'depression' subreddits. Postings on 'SuicideWatch' from December 16, 2008, to January 2, 2021, were all gathered; while postings on 'depression' were gathered between January 1, 2009, and January 2, 2021 [14]. We used 116037 posts from each category (suicidal, non-suicidal).

Figures 2 and 3 highlight words that occur most frequently in texts. A word's frequency in the text increases

https://doi.org/10.31436/ijpcc.v10i2.468

with its size in the visual. The dataset contains same number of suicidal and non-suicidal posts (Fig. 4).

Fig. 2 Mostly used words in suicide posts

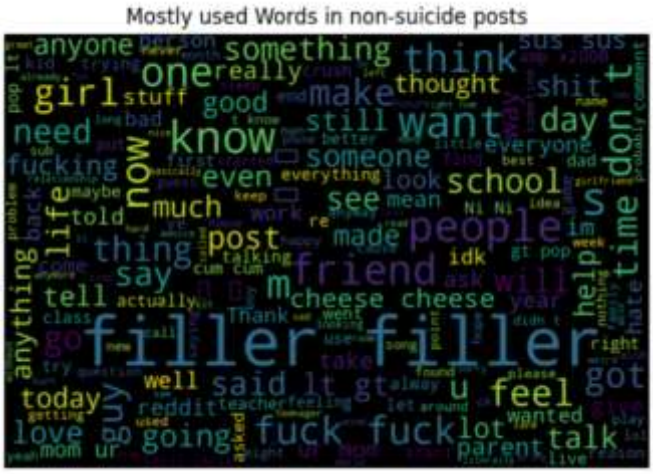

Fig. 3 Mostly used words in non-suicide posts

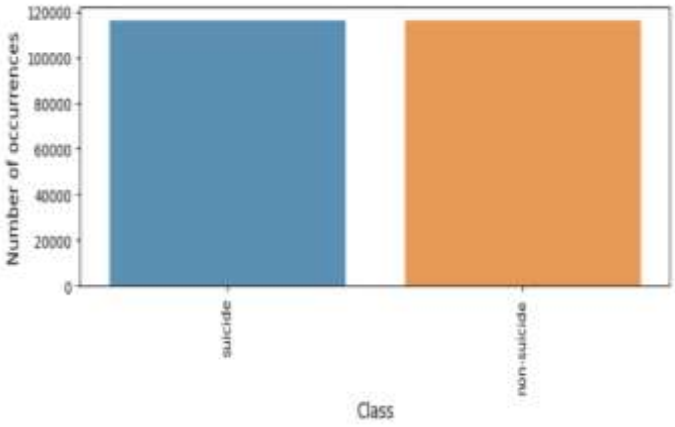

Fig. 4 Suicidal & Non-Suicidal post count

B. NLP Preprocessing

Figure 5 shows data preprocessing. After reading the data, the texts were converted to lowercase. Then, the contractions were removed and converted into tokens. We built a dictionary and prepared the data for vocabulary. These data were labelled for the prerequisite of doc2vec model.

Fig. 5 Data preprocessing steps

1) Doc2vec: The doc2vec was used to generate vectors for documents, as preprocessing for the logistic regression model. The documents were converted to a vector as the following algorithm:

$$Post_i = TaggedDocument(words = [word_1, word_2, \ldots., word_n] \quad (1)$$

$$Tags = [PostID_i] \quad (2)$$

$$Models_{Doc2Vec} = Doc2Vec(Documents = [Post_1, Post_2, \ldots., Post_m]) \quad (3)$$

2) BOW (Bag-of-Words): BOW was created as preprocessing for the naive Bayes model. The BOW is a vector of zeros and ones such as

$$BOW_{Posti} = [0,1,0,1,\ldots,0] \quad (4)$$

3) TF-IDF (Term Frequency–Inverse Document Frequency): The TF-IDF was computed as preprocessing for the naive Bayes model.

$$TFIDF_{Posti} = TF_{Posti} \times IDF_{term} \quad (5)$$

C. Classification Models

The three models: logistic regression, naïve Bayes, and random forest models were used for the classification, and were compared based on the classification performance of each model.

https://doi.org/10.31436/ijpcc.v10i2.468

1) *Logistic Regression*: The logistic regression model was used to classify the data after doc2Vec. This can be represented as

$$Probability\ of\ Suicide = sigmoid(W \cdot Doc2Vec + b) \quad (6)$$

2) *Naive Bayes:* The naive Bayes model was applied to the BOW.

$$Probability\ of\ Suicide = \frac{P(BOW|Suicide) \times P(Suicide)}{P(BOW)} \quad (7)$$

3) *Random Forest:* For the random forest model, none of doc2vec, BOW, and TF-IDF were applied.

D. Model Evaluation

Seventy percent of the dataset was used for training, and the rest was for testing. The confusion matrix was then computed to evaluate the above models. The accuracy, precision, recall, and F_1 score were calculated as follows.

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

$$precision = \frac{TP}{TP + FP} \quad (9)$$

$$recall = \frac{TP}{TP + FN} \quad (10)$$

$$F_1 = 2 \times \frac{precision \times recall}{precision + recall} \quad (11)$$

The Cohen's kappa was used to evaluate agreement between two evaluators [8]. The kappa was computed from the confusion matrix and used to estimate the levels of agreement, as shown in Table 1.

TABLE I
KAPPA VALUE INTERPRETATION TABLE

Kappa values	Interpretation
< 0	Lack of agreement
0 - 0.20	Minimum agreement
0.21 - 0.40	Reasonable agreement
0.41 - 0.60	Moderate agreement
0.61 - 0.80	Substantial agreement
0.81 - 1	Near-perfect agreement

IV. RESULTS

Figure 6 shows the comparison of accuracy of the three models: logistic regression, naive Bayes, and random forest. For the logistic regression model, doc2vec was applied to the dataset as NLP preprocessing. For the naive Bayes model, the two NLP techniques, i.e. BOW and TF-IDF, were compared. Then, the logistic regression model with doc2vec achieved the highest accuracy of 0.93. Accuracy of the naive Bayes model with BOW and naive Bayes model with TF-IDF were 0.89 and 0.90, respectively. The accuracy of the random forest model was 0.83.

Figures 7, 8, and 9 present the receiver operating characteristic (ROC) curves of the logistic regression model, naive Bays model with BOW, and naive Bayes model with TF-IDF, respectively. The closer the ROC curve was to the upper left, the greater the overall accuracy of the model. The AUCs of the logistic regression model, naive Bayes model with BOW, and naive Bayes model with TF-IDF were 0.97, 0.96, and 0.97, respectively. This result suggests that these three models have the potential of becoming a model that can classify the posts as suicidal or non-suicidal.

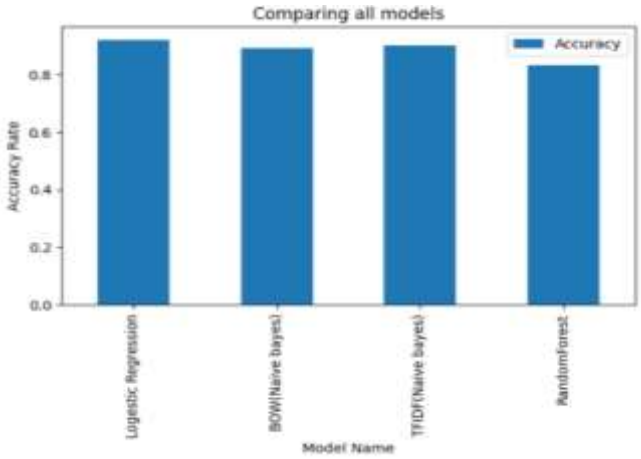

Fig. 6 Accuracy Comparison of Different Models

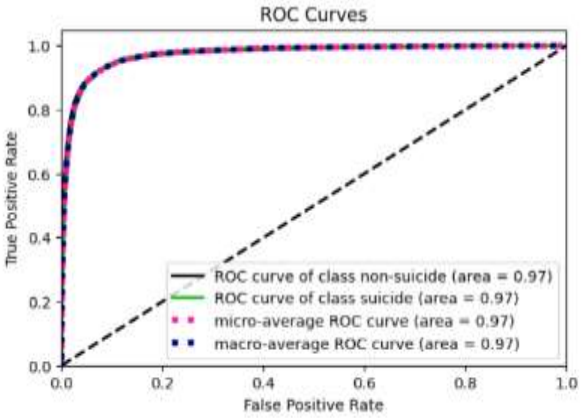

Fig. 7 ROC Curve for Logistic Regression model with Doc2vec

https://doi.org/10.31436/ijpcc.v10i2.468

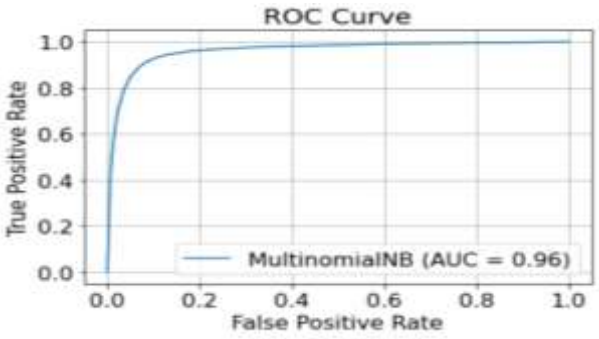

Fig. 8 ROC Curve for Naive Bayes with BOW

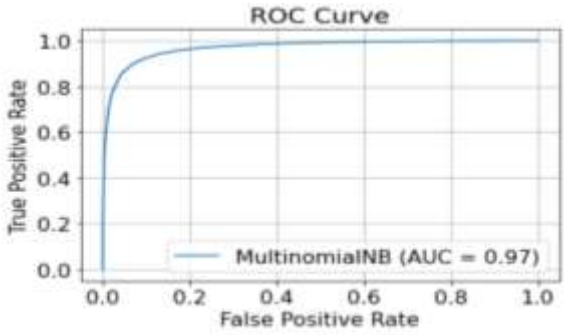

Fig. 9 ROC Curve for Naive Bayes with TF-IDF

Figure 10 shows the comparison of precision, recall, and F_1 score across the three models: logistic regression with doc2vec, naive Bayes with BOW, and naive Bayes with TF-IDF. The precisions of these models were 0.92, 0.89, and 0.89, respectively. The recalls were 0.92, 0.87, and 0.88, and the F_1 scores were 0.92, 0.90, and 0.90. The logistic regression model with doc2vec still had the highest precision, recall and F_1 score.

Figures 11 and 12 display the top 20 suicidal/non-suicidal words used, based on coefficients of the logistic regression model after training. The words 'suicide', 'kill', 'me', and end' were used to categorise suicidal words. On the other hand, the words 'call', 'them', 'matter', 'ago', 'believe' were for non-suicidal words.

To check the validity of the logistic regression model, we computed Cohen's kappa, which was 0.85. According to the Table 1, this means that there is an almost perfect agreement between the classification performed by the model and the classification related to the posts of the subreddits of the Reddit platform.

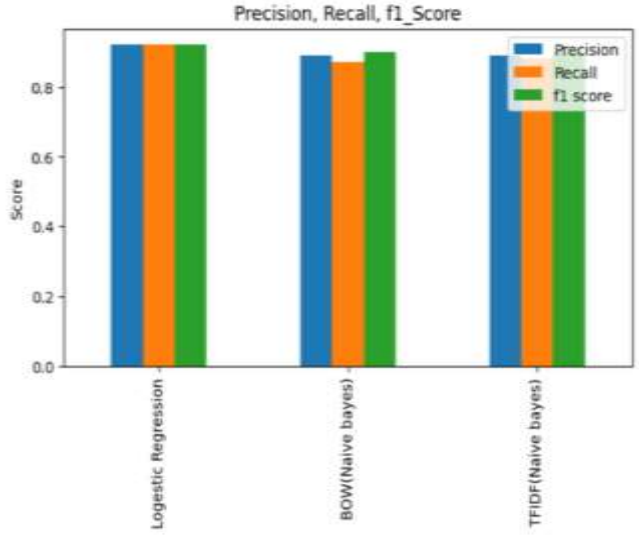

Fig. 10 Precision, Recall and F1-Score comparison

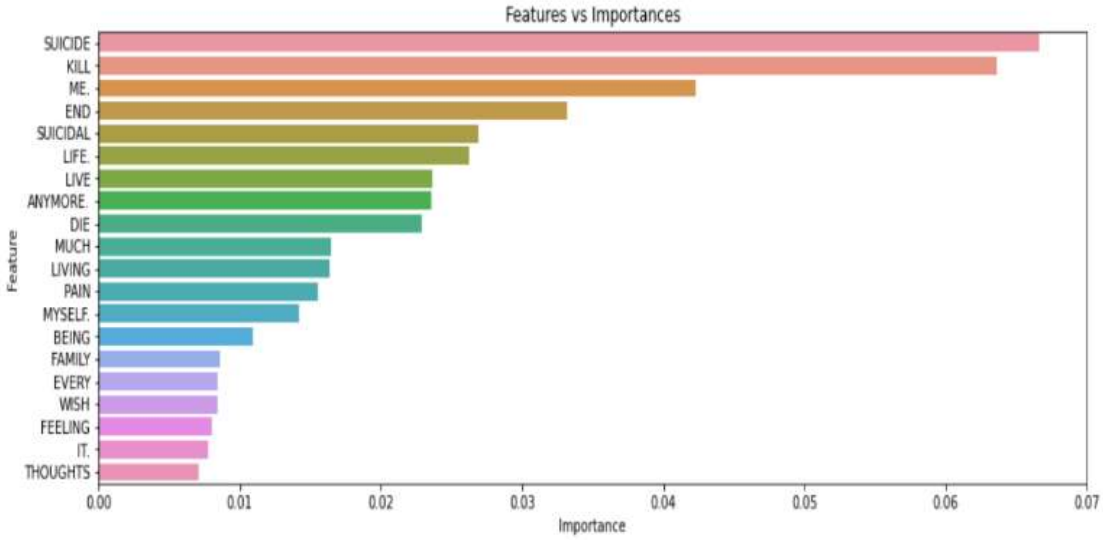

Fig. 11 Suicidal feature importance

https://doi.org/10.31436/ijpcc.v10i2.468

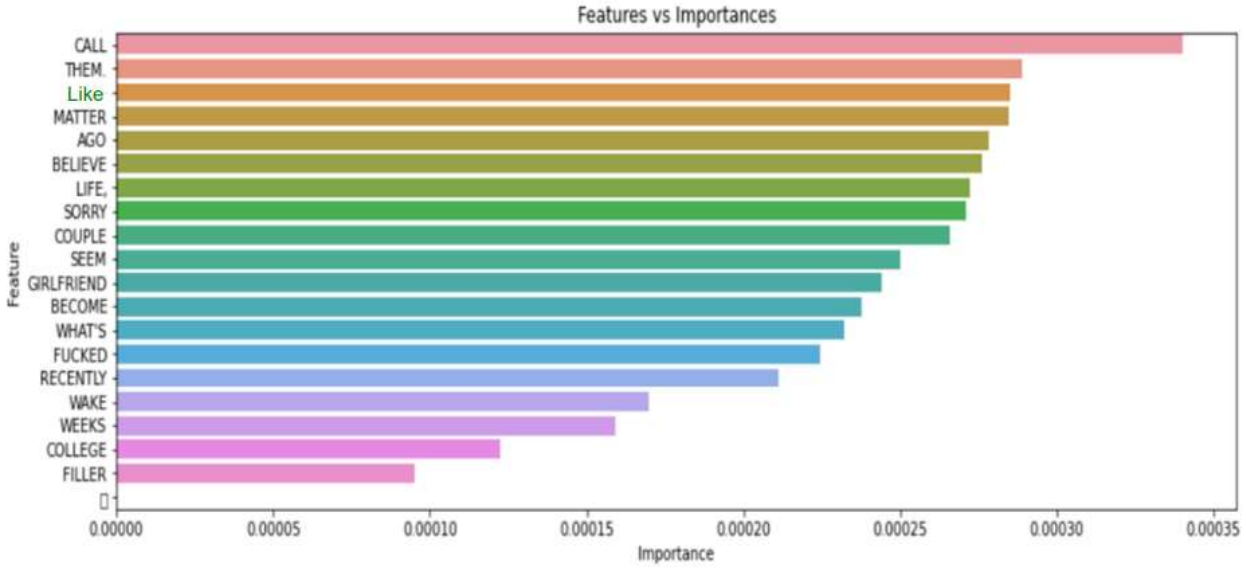

Fig. 12 Non-suicidal feature importance

V. Conclusions

In conclusion, we compared the three models: logistic regression, naive Bayes, and random forest models, to show the possibility of suicide risk prediction from social media data. For the logistic regression model, doc2vec was used as NLP preprocessing. For the naive Bayes model, the two NLP techniques, i.e. BOW and TF-IDF, were compared. Then, the logistic regression model showed the highest precision of 0.92, recall 0.92, and F_1 score of 0.92. Top 20 suicidal/non-suicidal words were identified according to the coefficients of the logistic regression model (Figs. 11 and 12). The suicidal words included 'suicide', 'kill', 'me', and end', while 'call', 'them', 'matter', 'ago', and 'believe' were non-suicidal words. Moreover, the Cohens' kappa was computed, and it was 0.85. This result shows that the model has the potential of classifying posts from people with potential suicidal tendencies.

Further research is necessary to validate the performance of the model. This study suggests that the logistic regression model with doc2vec NLP preprocessing may work for suicide risk prediction.

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] W.H.O. World Health Organization, "Suicide," World Health Organisation, Aug. 28, 2023. https://www.who.int/news-room/fact-sheets/detail/suicide

[2] H.-C. Shing, S. Nair, A. Zirikly, M. Friedenberg, H. Daumé III, and P. Resnik, "Expert, Crowdsourced, and Machine Assessment of Suicide Risk via Online Postings," ACLWeb, Jun. 01, 2018.

[3] S. Ji, C. P. Yu, S. Fung, S. Pan, and G. Long, "Supervised Learning for Suicidal Ideation Detection in Online User Content," Complexity, vol. 2018, pp. 1–10, Sep. 2018.

[4] S. C. Shetty, "A Deep Learning Approach for Suicide Risk Assessment using Reddit," norma.ncirl.ie, 2020. https://norma.ncirl.ie/4420/ (accessed Dec. 29, 2023).

[5] T.H. Aldhyani, T. H., Alsubari, S. N., Alshebami, A. S., Alkahtani, H., & Ahmed, Z. A. (2022). "Detecting and analyzing suicidal ideation on social media using deep learning and machine learning models." International journal of environmental research and public health, 19(19), 12635.

[6] S. Ji, Yu, C. P., Fung, S. F., Pan, S., & Long, G. (2018). "Supervised learning for suicidal ideation detection in online user content." Complexity, 2018.

[7] B. O'dea, Wan, S., Batterham, P. J., Calear, A. L., Paris, C., & Christensen, H. (2015). "Detecting suicidality on Twitter." Internet Interventions, 2(2), 183-188.

[8] L.J. Richard and G. G. Koch, "The Measurement of Observer Agreement for Categorical Data," Biometrics, vol. 33, no. 1, pp. 159–174, Mar. 1977.

[9] M. H. Zweig and G. Campbell, "Receiver-operating characteristic (ROC) plots: a fundamental evaluation tool in clinical medicine," Clinical Chemistry, vol. 39, no. 4, pp. 561–577, Apr. 1993.

[10] L. Vergni and F. Todisco, "A Random Forest Machine Learning Approach for the Identification and Quantification of Erosive Events," Water, vol. 15, no. 12, p. 2225, Jan. 2023.

[11] A. Lejeune, Le Glaz, A., Perron, P.-A., Sebti, J., Baca-Garcia, E., Walter, M., Lemey, C., & Berrouiguet, S. (2022). "Artificial intelligence and

suicide prevention: A systematic review. " European Psychiatry, 65(1), e19, 1–8.

[12] H. Tang, A. M. Rekavandi, D. Rooprai, G. Dwivedi, F. M. Sanfilippo, F. Boussaid, and M. Bennamoun, "Analysis and evaluation of explainable artificial intelligence on suicide risk assessment," Scientific Reports, 15(1), 53426, 2024.

[13] A. Roy., Nikolitch, K., McGinn, R., Jinah, S., Klement, W., & Kaminsky, Z. A. (2020). "A machine learning approach predicts future risk to suicidal ideation from social media data." npj Digital Medicine, 7(1), 1-10.

[14] D. Dataset, Suicide and Depression Detection dataset https://www.kaggle.com/datasets/nikhileswarkomati/suicide-watch

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.479

Selective of IoT Applications for Water Quality Monitoring in Malaysia

Ahmad Anwar Zainuddin, Amir 'Aatief Amir Hussin, Ammar Haziq Annas, Mohamad Syafiq Bharudin, Alin Farhain Abdul Rajat @ Abdul Razak, Muhammad Nur Badri Mahazir, Asmarani Ahmad Puzi, Dini Handayan, and Abdul Rafiez Abdul Raziff
Kulliyyah of ICT, International Islamic University Malaysia, Kuala Lumpur, Malaysia

*Corresponding author anwarzain@iium.edu.my
(Received: 29th May 2024; Accepted: 2nd June 2024; Published on-line: 30th July 2024)

Abstract— The aquaculture industry in Malaysia relies predominantly on Recirculating Aquaculture Systems (RAS), which are susceptible to infections, leading to disease outbreaks and significant economic repercussions. The frequent need for manual interventions makes RAS labor-intensive and inefficient. To address these challenges, this study advocates a shift towards disease prevention and proactive water quality management. The proactive approach entails modern water treatment methods, stringent biosecurity measures, and the integration of IoT (Internet of Things) technology to anticipate and prevent disease outbreaks. Our disease detection system utilizes real-time sensors, machine learning algorithms, and IoT technology to swiftly identify pathogen indicators. Simultaneously, the IoT-enabled water quality monitoring system consistently delivers crucial data, eliminating the need for on-site monitoring. The adoption of disease prevention and control strategies, including probiotics, vaccinations, and biosecurity measures, plays a pivotal role in fostering sustainable advancements within the aquaculture sector. By incorporating effective water quality management, optimizing fish stocking density, ensuring proper nutrition, adhering to hygienic practices, and deploying fish vaccines, with the aim to mitigate the occurrence of fish diseases, ultimately bolstering the resilience and sustainability of Malaysia's aquaculture industry. Overall, this paper proposes a comprehensive overview of IoT-based applications for water quality monitoring in Malaysia's aquaculture with the advancements in IoT technology and its potential impact on improving water quality management practices.

Keywords— Aquaculture, RAS, practices.

I. Introduction

The practice of aquaculture in Malaysia began in the 1920s, employing large polyculture in ex-mining pools with introduced Chinese carps like the bighead, silver, and grass carp [1]. Malaysian aquaculture includes both food and non-food sectors, such as brackish water fish, freshwater fish, seaweed, decorative fish, and aquatic plants. In 2019, Malaysia's fisheries industry contributed about 1.1% to global output, with aquaculture accounting for 0.4% [2]. Recognized as essential for food security in the Seventh Malaysia Plan (1996-2000) and a catalyst for economic growth in the Eighth Malaysia Plan (2001-2005) [1], the industry faces high land costs, feed, labor, and pollution challenges, with land costs posing the most significant obstacle [2].

The fisheries sector is currently confronted with environmental challenges, particularly in relation to water pollution, despite its significant role in driving the country's economic development [3]. The release of untreated effluent from aquaculture ponds into the surrounding environment has the potential to result in water contamination, hence contributing to the deterioration of aquatic ecosystems [4]. Fortunately, the Malaysian government has implemented several policies and plans to address those issues including:

1. National Agrofood Policy 2021-2030 (NAP 2.0): This policy aims to ensure adequate food safety and security, increase the contribution of the agro-food industry, empower human capital, and promote sustainable agriculture [5].
2. Malaysian Aquaculture Farm Certification Scheme (SPLAM): This certification scheme is

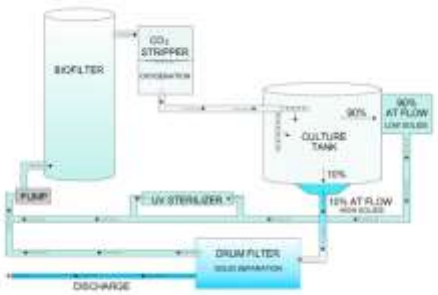

Fig. 1. Recirculating Aquaculture System Components showing the path water takes through major components within one type of a recirculating system [15]

https://doi.org/10.31436/ijpcc.v10i2.479

aimed at promoting sustainable aquaculture practices in Malaysia. It covers areas such as environmental management, animal health, and welfare, and food safety [4].

3. **Good Aquaculture Practices (GAqP)**: This initiative aims to promote sustainable aquaculture practices among Malaysian aquaculture farmers. It covers areas such as site selection, water quality management, and disease control [4].

4. **Technical support services and good regulatory frameworks**: The government provides technical support services and good regulatory frameworks for the industry [4].

5. **Aquaculture Master Plan**: This plan aims to promote the development of the aquaculture industry in Malaysia. It covers areas such as research and development, infrastructure development, and marketing [4].

6. **Effective governance:** Effective governance of modern aquaculture must reconcile ecological and human well-being so that the industry is sustainable over time. The government has implemented policies and plans to ensure effective governance of the aquaculture industry in Malaysia [6].

One solution to the challenges of high land cost and environmental pollution in the aquaculture industry in Malaysia is the use of Recirculating Aquaculture Systems (RAS). RAS is a technology that allows for the efficient use of water and reduces the environmental impact of aquaculture. The system works by recirculating water through a closed system, which reduces the amount of water needed for aquaculture production. RAS also allows for the efficient removal of waste products, which reduces the environmental impact of aquaculture. Figure 1 shows RAS water flow schematic.

Yet RAS offer several advantages, there are also some challenges associated with its use for instance:

1. Poor designs of the systems: Many RAS systems have been modified after a previous approach was unsuitable, leading to poor designs [7].

2. High investment costs: RAS technology is expensive to set up, and the recirculation technology consumes vast amounts of energy, which can be costly [8].

3. Vulnerable to disease: Parasites with direct life cycles are more common and dangerous in an RAS, because RASs used in production tend to have greater fish densities and by definition recycle water, which results in closer fish-to-fish contact and greater buildup of parasite numbers within the system. Once a parasite infects a fish within an RAS, it becomes magnified, and disease can spread rapidly [9].

It can be seen that water quality management is very important in RAS frameworks. The quality of water directly affects the health and well-being of the aquatic organisms being cultivated. Fish, shrimp, and other species are highly sensitive to changes in water parameters such as temperature, pH, dissolved oxygen levels, and ammonia concentration. Maintaining optimal water quality ensures that these organisms thrive, grow, and remain disease-free. Water quality management can be conducted at aquaculture ponds or water tanks by monitoring their inlet water quality, performing on-site monitoring and using biofiltration systems to manage ammonia and nitrite levels in RAS. Monitoring water quality is a continuous process that must adapt to changing conditions. Seasonal variations, weather events, and industrial activities can significantly influence water quality. Timely monitoring and data analysis are essential for early detection of contamination, ensuring the safety of water supplies, and taking appropriate remedial actions. Therefore, determining the optimal frequency and timing of water quality assessments is a critical aspect of effective management.

Integrating the Internet of Things (IoT) with RAS can enhance efficiency and sustainability. IoT sensors provide real-time data on water quality, temperature, and oxygen levels, enabling farmers to monitor and adjust conditions promptly [10, 11].

Section 1 introduces the enhancement of aquaculture practices in Malaysia through RAS and IoT and outlines related work on water quality, environmental factors, IoT technology, and disease prevention as well as the details objectives related to RAS operational efficiency, framework development, and substantiation of RAS efficacy as a sustainable methodology. Section 2 describes the research methodology, Section 3 shows the practical applications and real-world benefits, and Section 4 presents the results. Section 5 includes a Gantt chart of milestones, and Section 6 summarizes and concludes the work.

1.1 RELATED WORK

In this section, a set of questions that drive the investigation into the challenges and possibilities within Malaysia's aquaculture industry. These questions touch on vital topics, such as water quality, environmental factors, IoT technology, and disease prevention. By exploring these questions, the aim is to uncover practical insights and solutions to improve and sustain aquaculture practices in Malaysia.

A. Optimal Water Quality Parameters

What are the species-specific optimal water quality parameters for different aquaculture organisms in Malaysia, and how do these parameters vary across different stages of growth?

B. Impact of Environmental Factors

How do environmental factors, such as climate change and seasonal variations, affect water quality in aquaculture

https://doi.org/10.31436/ijpcc.v10i2.479

systems in Malaysia, and what strategies can be employed to mitigate these impacts?

C. Optimal Water Quality Parameters

What are the species-specific optimal water quality parameters for different aquaculture organisms in Malaysia, and how do these parameters vary across different stages of growth?

D. Optimal Water Quality Parameters

How can the integration of Internet of Things (IoT) technology enhance water quality management in Malaysian aquaculture, and what are the economic and environmental benefits of such integration?

1.2 OBJECTIVE

In this study, there are a few specific goals to tackle the problems in the aquaculture industry, especially in how Recirculating Aquaculture Systems (RAS) are used in Malaysia. These objectives aim to investigate, develop solutions, and confirm improvements that can make RAS more efficient, resilient to diseases, and sustainable. Together, these objectives help to work towards improving aquaculture practices in Malaysia as such:

A. *To investigate Operational Efficiency and Susceptibility of Recirculating Aquaculture Systems (RAS)*

The first objective of this study is to conduct a comprehensive investigation into the operational efficiency and susceptibility of Recirculating Aquaculture Systems (RAS) within the Malaysian aquaculture industry. As previously stated, Malaysia's aquaculture sector heavily relies on RAS as a method of cultivating aquatic species [12]. However, the inherent sensitivity of RAS to diseases and other operational challenges has raised concerns regarding its efficiency and sustainability [13].

B. *To Develop a Comprehensive Framework to Address RAS Weaknesses and Enhance Operational Efficiency*

Building upon the identified vulnerabilities and inefficiencies, the second objective is to develop a robust framework designed to counter these weaknesses and elevate the operational efficiency of RAS. It is necessary to shift from reactive disease management to proactive disease prevention and water quality control.

This objective seeks to address this need by proposing innovative strategies and solutions. It aims to design a comprehensive system that not only mitigates the identified vulnerabilities but also optimizes resource utilization within the aquaculture facilities. This aligns closely with the solution proposed in the abstract, where advanced water treatment processes and stringent biosecurity measures are recommended to prevent disease outbreaks and enhance overall efficiency.

C. *To Substantiating the Enhanced Efficacy of RAS as a Sustainable Aquaculture Methodology*

The final objective is to empirically validate the effectiveness of the proposed enhancements to the RAS methodology. The objective is to demonstrate that the improved RAS approach is more operationally efficient, economically viable, and sustainable compared to its current state [14].

To achieve this, rigorous experimentation and in-depth data analysis will be undertaken. This process aims to provide substantial evidence supporting the benefits of the proposed modifications, reinforcing the idea that RAS can indeed serve as a more efficient and resilient method for sustainable aquaculture in Malaysia.

II. RESEARCH METHODOLOGY

This section touches on the detailed methodology employed in this research endeavor. Figure 2 provides an insightful flowchart that visualizes the step-by-step approach guiding this investigation. This methodology encompasses a multifaceted strategy designed to comprehensively address our research objectives and culminate in meaningful outcomes.

Month 2-4: Work Initiation and Planning

- Define research objectives, questions, and scope.
- Develop a detailed research proposal.
- Identify research team members and assign roles.
- Secure necessary approvals and funding.

Month 6-8: Literature Review and Data Collection

- Conduct an extensive literature review.
- Collect historical data on disease outbreaks in Malaysian aquaculture systems.
- Gather information on water quality parameters during outbreaks.
- Compile data on aquaculture species, stocking density, and environmental factors during outbreaks.

Month 10-12: Data Analysis and Protocol Development

- Analyze historical data to identify patterns and correlations.
- Identify critical factors contributing to disease susceptibility.
- Determine optimal water quality parameters for different aquaculture species.
- Consult with experts and stakeholders to refine protocols.

Month 14-16: Protocol Implementation and Monitoring

- Implement water quality management protocols in selected aquaculture systems.
- Set up on-site testing equipment and IoT technology.
- Establish a routine for proactive monitoring and data collection.

Month 18-20: Response and Mitigation

- Respond to parameter deviations by initiating corrective actions.

https://doi.org/10.31436/ijpcc.v10i2.479

- Implement disease prevention measures (biosecurity, vaccination, probiotics).
- Monitor the effectiveness of these measures.

Month 22-24: Data Analysis, Reporting and Conclusion

- Analyze data collected over the research period.
- Evaluate trends and the effectiveness of disease prevention measures.
- Adjust protocols and strategies as necessary.
- Prepare research paper, including abstract, introduction, methodology, results, discussion, and conclusion.
- Complete final revisions, proofreading, and formatting.

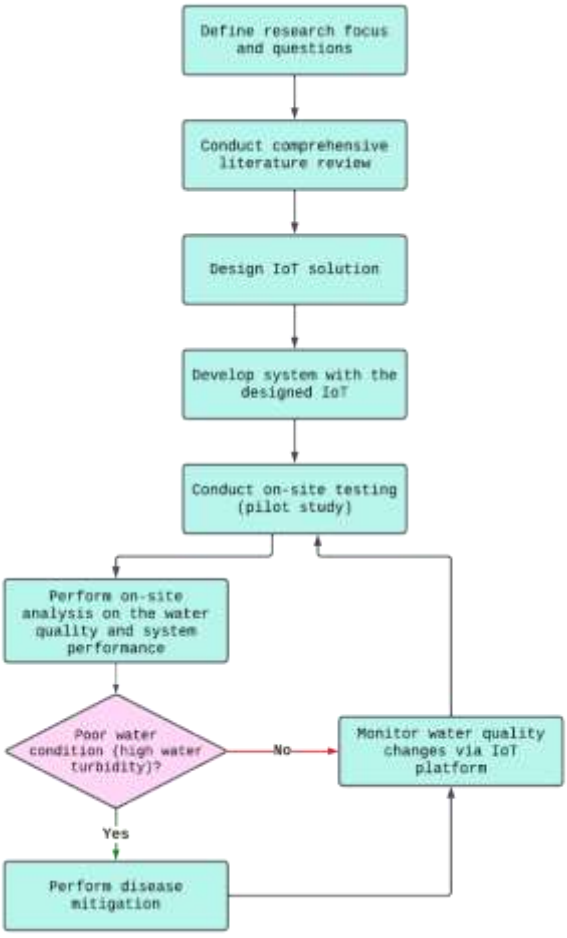

Fig. 2. IoT-integrated aquaculture solution flow

2.1 Description of Methodology

A. *Table Captions*

At an early phase, a comprehensive literature review needs to be conducted. In aquaculture, there are numbers of parameters that should be concerned which can affect the water quality. The variation of water quality parameters across different stages of growth can affect the behaviour, physiology, and cell biology of aquatic organisms [15]. But these three parameters are chosen to be enough for controlling water quality and inexpensive to be applied [16].

TABLE I
WATER QUALITY PARAMETERS

Parameters	Factors that can affect the parameter	Optimal water condition
pH	CO_2 concentration Organic materials	pH 6.5 - pH 8.5
Temperature	Solar radiation Climate Aquaculture system design (eg. exposed piping)	Coldwater species: Coldwater species such as trout and salmon prefer water temperatures between 10-18°C [17] Warmwater species: Warmwater species such as catfish, carp, and tilapia thrive in water temperatures between 22-32°C [17] Tropical species: Tropical species such as shrimp prefer water temperatures between 26-30°C [18] Hard clams: Hard clams prefer water temperatures between 16-27°C [19]
Turbidity	Small floating organisms suspended in the water column (e.g. plankton, algae, cyanobacteria) Pelleted food	Intense culture systems: In intense culture systems such as recirculation systems, it is recommended that suspended solids levels should not go above 15 mg/l (dry weight) [18] Aquaculture systems: The amount of total suspended solids (TSS) in aquaculture systems determines the level of mineral turbidity. If there is less than 25 TSS (mg/l), the mineral turbidity is considered low. The mineral turbidity is medium if it falls between 25-100 TSS (mg/l) [20]

B. *Impact of Environmental Factors*

Obviously, Environmental pollution can affect water quality in aquaculture systems. Malaysian coastal waters are mainly contaminated with oil and grease, faecal matter, and other

https://doi.org/10.31436/ijpcc.v10i2.479

pollutants [21]. The presence of pollutants can affect the health and growth of aquatic organisms, as well as the quality of aquaculture products [21-23]. Climate change can also affect water availability, with changes in precipitation patterns and water flow affecting the amount of water available for aquaculture operations [24].

There are several strategies that can be applied to mitigate environmental impacts in aquaculture. These strategies include:

- Farm design and layout: The design and layout of aquaculture systems can also affect environmental impacts. Factors to consider include the use of recirculating systems, the use of appropriate cage design and orientation, and the control of stocking densities [25]–[27].
- Feeding practices: Managing feeding practices can help to reduce pollution and improve water quality. Overfeeding can lead to excessive waste and pollution, while underfeeding can lead to poor growth rates and weakened immune systems in farmed fish [26].
- Reducing chemical use: Minimizing the use of chemicals and veterinary drugs can help to reduce environmental impacts. Natural alternatives can be used to control diseases and parasites, and careful monitoring can help to prevent the overuse of chemicals [26], [27].

C. *IoT Integration*

Assessing environmental impacts: Assessing the environmental impacts of aquaculture operations can help to identify potential issues and develop appropriate mitigation strategies (see Figure 3 to 6). This can include monitoring water quality, assessing the cumulative impacts of multiple aquaculture farms, and seeking professional advice [25], [28].

Fig. 3. pH Sensor

Fig. 4. Temperature Sensor

Fig. 5. Turbidity Sensor

Moreover, IoT-based systems can collect and analyse large amounts of data on water quality parameters, allowing for more accurate and precise monitoring of water quality. There are many IoT platforms available on the Internet which enable users to monitor and analyse data from IoT sensors remotely like Blynk. Blynk is a comprehensive software suite that enables the prototyping, deployment, and remote management of connected electronic devices at any scale [29]. The integration of IoT technology in water quality management in aquaculture can provide both economic and environmental benefits:

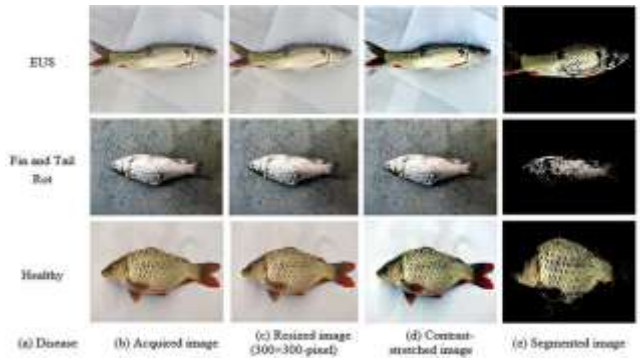

Fig. 6. Classification using multi-SVM's [36]

i. Economic

- Increase in productivity: IoT-based systems can provide aquaculture operators with more accurate and timely information on water quality, allowing for better decision-making and improved management of aquaculture operations [30]–[32]
- Cost savings: IoT-based systems can reduce the need for manual labour and improve efficiency, leading to cost savings for aquaculture operators [32], [33].

ii. Environmental

- Reduced environmental footprint: IoT-based systems can help to reduce the environmental footprint of aquaculture operations by improving water quality management and reducing pollution.

https://doi.org/10.31436/ijpcc.v10i2.479

- Improved sustainability: IoT-based systems can help to improve the sustainability of aquaculture operations by reducing waste and improving resource management [34].

D. *Disease Prevention*

Disease prevention in Malaysia aquaculture is designed to reduce the incidence of diseases and enhance the overall health and sustainability of aquaculture systems. The methodology spans several key phases over the course of the work, aiming to proactively manage water quality parameters and mitigate disease outbreaks.

- **Species-Specific Monitoring:** The early disease detection system is tailored to the specific aquaculture species being cultivated. As seen in Figure 6, different species have varying sensitivities to changes in water quality [35], [36]. Species-specific parameter ranges are defined, ensuring that the system's alerts are customized to the needs and vulnerabilities of the aquatic organisms in question.
- **Internet of Things (IoT) Connectivity:** A robust IoT infrastructure that facilitates the seamless transmission of sensor data to a central monitoring platform is established [37]. Its connectivity allows for remote monitoring and
- **Early Warning Signs and Biomarkers:** The monitoring of early warning signs, such as abrupt shifts in temperature, pH, or dissolved oxygen levels, which are often associated with disease onset are prioritized [38]. The integration of disease-specific biomarkers or genetic markers that can be detected through molecular techniques, providing precise and early indications of disease presence.

2.2 Detailed Implementation Framework

A. Adopting Disease Prevention Methods and Advanced Water Quality Management Practices

To effectively adopt disease prevention methods and advanced water quality management practices in Malaysian aquaculture, the following step-by-step framework is recommended for industry stakeholders:

i. Assessment of Current Practices:
- Conduct a thorough evaluation of existing disease prevention and water quality management practices in the facility.
- Identify gaps and areas for improvement in current methodologies.

ii. Selection of Appropriate Technologies:
- Choose suitable IoT sensors and water treatment technologies based on the specific needs of the aquaculture operation.
- Consider factors such as farm size, species cultivated, and local environmental conditions.

iii. Integration of IoT Technologies:
- Install IoT sensors to monitor key water quality parameters such as temperature, pH, dissolved oxygen, and ammonia levels.
- Ensure real-time data transmission to a centralized monitoring system for continuous oversight.

iv. Implementation of Disease Prevention Protocols:
- Develop and implement standard operating procedures (SOPs) for disease prevention, including regular health checks, vaccination programs, and biosecurity measures.
- Utilize IoT data to predict and prevent outbreaks by identifying early warning signs of disease.

v. Training and Capacity Building:
- Provide comprehensive training for staff on the use of IoT technologies and new water management practices.
- Conduct regular workshops and refresher courses to keep the workforce updated on the latest advancements and protocols.

vi. Continuous Monitoring and Evaluation:
- Establish a continuous monitoring system to track the effectiveness of implemented practices.
- Use collected data to make informed decisions and adjustments to enhance the overall efficiency of the aquaculture operation.

III. Practical Applications and Real-World Benefits

Incorporating advanced technologies such as IoT and RAS in Malaysian aquaculture offers numerous practical applications and real-world benefits, enhancing both efficiency and sustainability.

3.1 Enhancing Aquaculture Efficiency and Sustainability

i. Increased Productivity

Implementing IoT technologies allows for increased productivity by enabling precise monitoring and control of water quality parameters, ensuring optimal conditions for aquaculture. This real-time data facilitates immediate corrective actions, significantly reducing the risk of crop losses due to poor water conditions or disease outbreaks.

ii. Cost-Effective Management

Advanced water quality management practices reduce the need for frequent water changes and chemical treatments, leading to cost savings. Automated monitoring systems further decrease labour costs by reducing the necessity for manual checks.

iii. Improve Fish Health and Yield

Healthier fish populations and higher yields are achieved through early detection and prevention of diseases, made

https://doi.org/10.31436/ijpcc.v10i2.479

possible by IoT sensors. This proactive water quality management results in optimal growth conditions, enhancing the overall quality and market value of the produce.

iv. Sustainability and Environmental Protection

Additionally, adopting RAS and IoT technologies minimizes water usage and waste discharge, contributing to environmental sustainability. Effective governance and adherence to sustainable practices reduce the ecological footprint of aquaculture operations, ensuring long-term viability and environmental protection.

IV. Presentation of the Results

This research work holds substantial significance for the Malaysian Aquaculture sector. These worked outcomes represent pivotal advancements and benefits for the industry, fostering a more efficient, sustainable and environmentally conscious framework such as:

E. *Enhanced Water Quality Management Practices*

The research efforts outlined in this study, encompassing the exploration of optimal water quality parameters and strategies to mitigate environmental impacts, are assured to achieve improved water quality management practices within Malaysian aquaculture systems. The practical implementation of contemporary water treatment methodologies and proactive water quality oversight is anticipated to elevate overall water conditions in these systems.

F. *Increase Operational Efficiency and Effectiveness*

The integration of IoT technology into aquaculture operation is expected to boost the efficiency and effectiveness of water quality management significantly. By providing real-time data and facilitating swift responses to any changes from optimal conditions, IoT technology has the potential to streamline operations and minimize resource wastage, thus optimizing the use of water resources.

G. *Reduced Disease Outbreaks*

One of the paramount objectives of this research is to tailor water quality management practices for disease prevention. Consequently, a reduction in the incidence of disease outbreaks within Malaysian aquaculture systems is a expected outcome. The proactive measures recommended, including stringent biosecurity measures and the early disease detection system, are designed to pre-empt pathogen proliferation, thereby minimizing losses attributed to disease-related incidents.

H. *Economic and Environmental Sustainability*

The adoption of best practices in water quality management is anticipated to bolster both economic and environmental sustainability within Malaysian aquaculture. By optimizing resource utilization and reducing disease-related losses, aquaculture businesses can expect improved profitability and productivity. Simultaneously, the implementation of sustainable practices and the reduction of environmental impacts contribute to a more environmentally friendly industry.

I. *Reinforcement of RAS with IoT*

The integration of IoT technology is poised to bolster the capabilities of Recirculating Aquaculture Systems (RAS). By providing real-time insights into water quality parameters and facilitating immediate responses, IoT technology is set to empower RAS, rendering it more resilient and adaptable to dynamic conditions. This technological fortification holds the potential to transform RAS into a more robust and resource-efficient aquaculture method.

Through the implementation of proactive disease prevention strategies, the seamless integration of IoT technology, and the optimization of water quality management practices, the sector stands to reap the benefits of heightened productivity, profitability, and sustainability. These outcomes collectively contribute to the cultivation of a more prosperous, resilient, and ecologically attuned aquaculture industry that harmonizes with the evolving demands and expectations of the nation.

V. Milestone and Gantt Chart

Phase 1: System Setup and Data Collection

In this initial phase, the focus is on establishing the foundation of the early disease detection system. Key activities include the deployment of specialized sensors designed to monitor critical water quality parameters in selected aquaculture systems. These sensors are strategically placed to ensure comprehensive coverage. Simultaneously, the team acquires and configures data analysis software and tools, laying the groundwork for data processing and interpretation. To facilitate effective operation, research personnel undergo thorough training in sensor operation and data collection techniques. A crucial aspect of this phase is the allocation of the initial budget, which covers sensor procurement, installation, and other essential setup expenses. Additionally, preliminary data collection begins, serving as the baseline for subsequent monitoring and analysis.

Phase 2: System Implementation and Monitoring

With the infrastructure in place, Phase 2 focuses on the full-scale implementation and continuous monitoring of the early disease detection system. Sensors, deployed across aquaculture sites, provide real-time data on water quality parameters. This continuous data stream is subject to real-time analysis, enabling the rapid identification of any deviations from optimal conditions that could signal early

disease indicators. To enhance data transmission and accessibility, an Internet of Things (IoT) infrastructure is developed and seamlessly integrated into the system. Ongoing budget allocation ensures sensor maintenance, data storage, and any necessary adjustments. A critical milestone is the implementation of a real-time alert system, enabling immediate notifications to aquaculture personnel when potential disease indicators are detected. This phase also involves the establishment of response protocols, outlining the actions to be taken in the event of an alert, such as isolation measures and disease mitigation efforts.

Phase 3: Evaluation and Optimization

In the final phase, the research work shifts its focus to evaluation and optimization. Extensive data analysis is conducted, delving into the collected data to refine algorithms and enhance the system's accuracy in detecting early disease indicators. Simultaneously, the response protocols are continually assessed and improved to ensure efficient and effective actions in response to alerts. A critical aspect of this phase is reporting, where research findings are compiled and synthesized into a comprehensive research report. Budget allocation for final evaluations, reporting, and dissemination is essential to ensure the work's outcomes reach relevant stakeholders. The research work also emphasizes a commitment to continuous improvement, maintaining an open dialogue with industry stakeholders to refine the system based on evaluation results and emerging disease patterns.

VI. Conclusion

In conclusion, the imperative for a more efficient, sustainable, and resilient aquaculture industry in Malaysia necessitates the concerted embrace of disease prevention, advanced water quality management, and cutting-edge technologies such as RAS. These concerted efforts bear the potential to significantly contribute to the realms of food security, economic prosperity, and environmental preservation. It suggests a focused approach to exploring specific IoT applications tailored for water quality monitoring in Malaysian aquaculture settings. Furthermore, it underscores the importance of customization and adaptation of IoT solutions to suit the unique needs and challenges of Malaysian aquaculture.

Acknowledgement

AgriNXT, a collaborative initiative involving the Malaysian Communications and Multimedia Commission (MCMC), the Ministry of Agricultural and Food Security, and Bioeconomy Corporation, serves as a platform for young innovators to present their ideas in agricultural technology. This competition seeks to foster innovation and address challenges within the agricultural sector. In the highly anticipated AgriNXT competition 2023, a team of ambitious and creative students from the Department of Computer Science, Kulliyyah of Information Communication and Technology, IIUM, showcased their talent and emerged victorious on 28 December 2023, with their innovative solutions to real-world agricultural challenges.

Conflict of Interest

The authors declare that there is no conflict of interest

References

[1] "FAO Fisheries & Aquaculture - National Aquaculture Sector Overview - Malaysia." Accessed: Oct. 02, 2023. [Online]. Available: https://firms.fao.org/fi/website/FIRetrieveAction.do?dom=countrysector&lang=en&xml=naso_malaysia.xml#tcN90188

[2] A. Chong, "Malaysia's Aquaculture Industry 5 Challenges," Maritime Fairtrade. Accessed: Oct. 02, 2023. [Online]. Available: https://maritimefairtrade.org/aquaculture-industry-malaysia-5-challenges-issues/

[3] S. Fathi, A. N. Harun, S. Rambat, and N. A. Tukiran, "Current Issues in Aquaculture: Lessons from Malaysia," Adv. Sci. Lett., vol. 24, no. 1, pp. 503–505, Jan. 2018, doi: 10.1166/asl.2018.12051.

[4] S. B. Kurniawan et al., "Aquaculture in Malaysia: Water-related environmental challenges and opportunities for cleaner production," Environ. Technol. Innov., vol. 24, p. 101913, Nov. 2021, doi: 10.1016/j.eti.2021.101913.

[5] S.-Y. Tan, S. Sethupathi, K.-H. Leong, and T. Ahmad, "Challenges and opportunities in sustaining aquaculture industry in Malaysia," Aquac. Int., Jun. 2023, doi: 10.1007/s10499-023-01173-w.

[6] N. Hishamunda, N. Ridler, and E. Martone, Policy and governance in aquaculture: lessons learned and way forward: Lessons learned and way forward. Rome, Italy: FAO, 2014. Accessed: Oct. 05, 2023. [Online]. Available: https://www.fao.org/documents/card/fr/c/a6c20b4f-7b92-5da6-b5f8-83bbde723eb6/

[7] M. Badiola, D. Mendiola, and J. Bostock, "Recirculating Aquaculture Systems (RAS) analysis: Main issues on management and future challenges," Aquac. Eng., vol. 51, pp. 26–35, Nov. 2012, doi: 10.1016/j.aquaeng.2012.07.004.

[8] "8. What are the advantages and key challenges of Recirculating Aquaculture Systems (RAS)? | EU Aquaculture Assistance Mechanism." Accessed: Oct. 02, 2023. [Online]. Available: https://aquaculture.ec.europa.eu/faq/8-what-are-advantages-and-key-challenges-recirculating-aquaculture-systems-ras

[9] "Infectious Diseases in Aquaculture - Exotic and Laboratory Animals," Merck Veterinary Manual. Accessed: Oct. 02, 2023. [Online]. Available: https://www.merckvetmanual.com/exotic-and-laboratory-animals/aquaculture/infectious-diseases-in-aquaculture

[10] "Internet of things," Wikipedia. Oct. 01, 2023. Accessed: Oct. 02, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Internet_of_things&oldid=1178081162

[11] C. Pham, T. Le, Y. Lim, and Y. Tan, "An architecture for supporting RAS on Linux-based IoT gateways," in 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), Nagoya: IEEE, Oct. 2017, pp. 1–5. doi: 10.1109/GCCE.2017.8229234.

[12] A. Yusoff, "Status of resource management and aquaculture in Malaysia," 2014.

[13] J. Bregnballe, A guide to recirculation aquaculture: an introduction to the new environmentally friendly and highly productive closed fish

farming systems. Copenhagen: Food and Agriculture Organization of the United Nations: Eurofish, 2015.
[14] A. Midilli, H. Kucuk, and I. Dincer, "Environmental and sustainability aspects of a recirculating aquaculture system," Environ. Prog. Sustain. Energy, vol. 31, no. 4, pp. 604–611, Dec. 2012, doi: 10.1002/ep.10580.
[15] K. Semmens and D. MILLER, "Utilizing Mine Water for Aquaculture," Jan. 2003.
[16] M. Toni, "Variation in Environmental Parameters in Research and Aquaculture: Effects on Behaviour, Physiology and Cell Biology of Teleost Fish," J. Aquac. Mar. Biol., vol. 5, no. 6, Jun. 2017, doi: 10.15406/jamb.2017.05.00137.
[17] University Putra Malaysia (UPM), Malaysia, O. A. Nasir, S. Mumtazah, and University Putra Malaysia (UPM), Malaysia, "IOT-BASED MONITORING OF AQUACULTURE SYSTEM," MATTER Int. J. Sci. Technol., vol. 6, no. 1, pp. 113–137, Jun. 2020, doi: 10.20319/mijst.2020.61.113137.
[18] G. G. Aquaponics, "The Effects of Water Temperature in Aquaponics," Go Green Aquaponics. Accessed: Oct. 04, 2023. [Online]. Available: https://gogreenaquaponics.com/blogs/news/the-effects-of-water-temperature-in-aquaponics
[19] "Site Selection For Aquaculture: Physical features of water." Accessed: Oct. 04, 2023. [Online]. Available: https://www.fao.org/3/ac174e/AC174E02.htm
[20] "FA151/FA151: The Role of Water Temperature in Hard Clam Aquaculture." Accessed: Oct. 04, 2023. [Online]. Available: https://edis.ifas.ufl.edu/publication/FA151
[21] "Factors Affecting Fish Farming: Water Parameters and Pre-Stocking Management." Accessed: Oct. 04, 2023. [Online]. Available: https://bivatec.com/blog/required-parameters-for-water-quality-management
[22] "Report on a Regional Study and Workshop on the Environmental Assessment and Management of Aquaculture Development." Accessed: Oct. 04, 2023. [Online]. Available: https://www.fao.org/3/ac279e/ac279e16.htm
[23] P. Wang and I. Mendes, "Assessment of Changes in Environmental Factors Affecting Aquaculture Production and Fisherfolk Incomes in China between 2010 and 2020," Fishes, vol. 7, no. 4, p. 192, Aug. 2022, doi: 10.3390/fishes7040192.
[24] M. Camara, N. R. Jamil, and A. F. B. Abdullah, "Impact of land uses on water quality in Malaysia: a review," Ecol. Process., vol. 8, no. 1, p. 10, Dec. 2019, doi: 10.1186/s13717-019-0164-x.
[25] R. Hamdan, A. Othman, and F. Kari, "CLIMATE CHANGE EFFECTS ON AQUACULTURE PRODUCTION PERFORMANCE IN MALAYSIA: AN ENVIRONMENTAL PERFORMANCE ANALYSIS," Int. J. Bus. Soc., vol. 16, no. 3, Nov. 2017, doi: 10.33736/ijbs.573.2015.
[26] "Mitigation and best practice options," NIWA. Accessed: Oct. 04, 2023. [Online]. Available: https://niwa.co.nz/freshwater/kaitiaki-tools/what-is-the-proposed-activity-or-industry/aquaculture-and-customary-fisheries/mitigation-and-best-prac
[27] "Six tips to make your fish farm more environmentally sustainable," The Fish Site. Accessed: Oct. 04, 2023. [Online]. Available: https://thefishsite.com/articles/six-tips-to-make-your-fish-farm-more-environmentally-sustainable
[28] R. Waite and M. Phillips (WorldFish), "Sustainable Fish Farming: 5 Strategies to Get Aquaculture Growth Right," Apr. 2014, Accessed: Oct. 04, 2023. [Online]. Available: https://www.wri.org/insights/sustainable-fish-farming-5-strategies-get-aquaculture-growth-right
[29] "Fish Farming Improvements Reduce Environmental Impacts of Aquaculture," NCCOS Coastal Science Website. Accessed: Oct. 04, 2023. [Online]. Available: https://coastalscience.noaa.gov/news/fish-farming-improvements-reduce-environmental-impacts-of-aquaculture/
[30] "Introduction." Accessed: Oct. 04, 2023. [Online]. Available: https://docs.blynk.io/en/
[31] G. Gao, K. Xiao, and M. Chen, "An intelligent IoT-based control and traceability system to forecast and maintain water quality in freshwater fish farms," Comput. Electron. Agric., vol. 166, p. 105013, Nov. 2019, doi: 10.1016/j.compag.2019.105013.
[32] "Internet of things to improve productivity and sustainability of trout aquaculture in Peru | IADB." Accessed: Oct. 04, 2023. [Online]. Available: https://www.iadb.org/en/news/internet-things-improve-productivity-and-sustainability-trout-aquaculture-peru
[33] M.-C. Chiu, W.-M. Yan, S. A. Bhat, and N.-F. Huang, "Development of smart aquaculture farm management system using IoT and AI-based surrogate models," J. Agric. Food Res., vol. 9, p. 100357, Sep. 2022, doi: 10.1016/j.jafr.2022.100357.
[34] R. Ramanathan, Y. Duan, J. Valverde, S. Van Ransbeeck, T. Ajmal, and S. Valverde, "Using IoT Sensor Technologies to Reduce Waste and Improve Sustainability in Artisanal Fish Farming in Southern Brazil," Sustainability, vol. 15, no. 3, p. 2078, Jan. 2023, doi: 10.3390/su15032078.
[35] M. F. Taha et al., "Recent Advances of Smart Systems and Internet of Things (IoT) for Aquaponics Automation: A Comprehensive Overview," Chemosensors, vol. 10, no. 8, p. 303, Aug. 2022, doi: 10.3390/chemosensors10080303.
[36] Md. J. Mia, R. B. Mahmud, Md. S. Sadad, H. A. Asad, and R. Hossain, "An in-depth automated approach for fish disease recognition," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 9, pp. 7174–7183, Oct. 2022, doi: 10.1016/j.jksuci.2022.02.023.
[37] J. Sikder, K. Sarek, and U. Das, "Fish Disease Detection System: A Case Study of Freshwater Fishes of Bangladesh," Int. J. Adv. Comput. Sci. Appl., vol. 12, Jun. 2021, doi: 10.14569/IJACSA.2021.01206100.
[38] N. Darapaneni et al., "AI Based Farm Fish Disease Detection System to Help Micro and Small Fish Farmers," in 2022 Interdisciplinary Research in Technology and Management (IRTM), Feb. 2022, pp. 1–5. doi: 10.1109/IRTM54583.2022.9791553.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.462

NavigateMe:

An in-Building Navigation Application

Siti Asma binti Mohammed*, Nor Asyikin Binti Ahmad Nasaruddin, Nur Airin Faqihah Binti Ruzaidi

Department of Computer Sciences International Islamic University Malaysia, Gombak, Malaysia.

*Corresponding author siti_asma@iium.edu.my
(Received: 20th February2024; Accepted: 8th June 2024; Published on-line: 30th July 2024)

Abstract— For some people to reach their destination and complete their daily tasks, navigation systems serve as an aid, a tool, or an assistance. Currently, International Islamic University Malaysia (IIUM) lacks an in-building navigation system that could assist users, particularly new students, in finding their way to the location of their choice. This paper has two goals. This study first examines the current campus navigation systems and the relevant research article. Second, this work suggests a mobile navigation system that facilitates user navigation within Kuliyyah of Information and Communication Technology (KICT) facilities. Methods used to build the application were according to Software Development Life Cycle (SDLC). The suggested navigation application, NavigateMe, helps users navigate within buildings by providing sequential instructions and images of landmarks along the route. It stands out for being usable even in the event of sporadic internet connectivity. In conclusion, visitors and the IIUM community, particularly the new students of KICT, will benefit from an in-building navigation application like NavigateMe to effortlessly reach their destination.

Keywords— navigation application, mobile application, locations, path finding

I. Introduction

A. *Project Overview*

NavigateMe is a mobile application that helps the user to navigate through the campus (KICT and nearby location). This application benefits the user as it can save time in finding desired destinations on the campus and was created for public use due it not requiring any credentials like ID and password for login except for the staff responsible to update and manage the application so it is usable for IIUM visitors. A few existing systems such as ClassFind.com [1], University of Calgary Interactive Map (UoC) [2] and the USF Interactive Campus Map [3] were referred to research and understand more in how this kind of applications work. They (USF & UoC) assist users to search for their desired location by inputting the keyword of the location. Moreover, the systems (ClassFind, USF & UoC) display the map for clearer view of the campus so they can know the landmarks surrounding the location. Furthermore, it (ClassFind) also provides a navigation function that guides the user to their destination. If the navigation does not work, the system provides an external link for the floor plan, building and department information as an alternative as implemented in the USF & UoC system. Therefore, all the functions which were possible to code are included in the NavigateMe system including the features where the system informs the user of their current location that allows the user to find their destination manually using the provided floor plan in case of unstable internet connection or navigation problem.

B. *Problem Statement*

A navigation system has been used to help the user find their desired location. It cannot be denied that without the system, something cannot be solved or would be difficult to solve, for example business processes where the delivery of goods needs to be done and a good navigation system would reduce a lot of effort and time. Both staff and students can arrive at their workplace and classes faster and easier. For IIUM, which is a large campus with different kinds of department buildings, it would be difficult to find certain places. With the existence of navigation systems like Google Maps, it is indeed beneficial, however some users might have difficulties in using such navigation systems. Research has shown that not everyone is able to easily navigate using the existing navigation system and this is said to be true due to differences in gender, between males and females [4]. Some users, especially females are not able to interpret the map easily and research has shown that it is due to the different visual and spatial capacity of both users [5]. Some of the users, mostly females, depend on the landmark along the way to find their desired location.

https://doi.org/10.31436/ijpcc.v10i2.462

So, with our navigation system, we intend to solve this problem by providing the simplest version of the map so that all users can use it with ease.

C. *Project Objective*

- To investigate the components and current designs of existing navigation systems from the literature
- To design and develop a user friendly and easy to use version of navigation system for all types of users in IIUM.
- To test the developed system within IIUM campus

D. *Significance of Project*

The significance of this project is that users, especially the students and visitors, can use this system to find their desired location in the campus easily. In addition, the system is user-friendly for all generations by having easier features than the existing navigation system. This system shows landmarks, a few icons and steps to navigate through the way to their desired location. Other than that, this system is reliable since it is accessible even during intermittent internet access, which means that the user would only need to know the starting point that is displayed, and the rest of the steps would be shown by the images displayed in the page. Even though other functions cannot be accessed during internet intermittent, in some cases, the page would still be there with all images for navigation to the destination.

II. Related Works

For the first research papers authored by researchers and developers, the problem of where to locate classrooms at Politeknik Kuching Sarawak is discussed [6]. With a focus on user interaction and authored by Helmi Abd Kadir, Muhd Nazmi Ismail and Muhammad Firdaus Aminuddin, the paper covers requirements analysis through evaluation. Real-time maps, comprehensive class information and user notifications were all included in the built program. The study offers insights on user-centric development and the effects of technology integration in educational settings, despite its limitations in terms of scope and technical details. The second case study examined navigational issues on university campuses and suggested a mobile navigation system. It was carried out by Akanbi Caleb, I K Ogundoyin, and A O Lawal [7]. System design, user testing and data collection were all part of the technique. Highlights include turn-by-turn directions and interactive maps. Despite having many useful features, the study lacks technical specifics and considers scalability. Considering this, it encouraged the effective fusion of GPS technology with the ideas of user-centred design.

In the third case study, Susovan Jana and Matangini Chattopadhyay demonstrated an Android-based event-driven navigation system [8]. By integrating with the university's event management system, the method guaranteed precise location, real-time updates, and an intuitive user interface. Reliability, broader application, accessibility, and security issues are among the challenges. The study highlights the value of user feedback for continual improvement and recommends continuing research for testing in real-world settings.

TABLE I
COMPARISON BETWEEN THE EXISTING SYSTEMS AND THE PROPOSED SYSTEM

	USF Interactive Campus Map	**University of Calgary Interactive Map**	**ClassFind.com**	**NavigateMe (Proposed System)**
Choose location	✓	✓	✓	✓
Real life map	✓	✓	✓	✓
Use coordinates	✓	✓	✗	✗
Live location	✗	✗	✗	✗
Starting points	✗	✗	✓	✓
Search location	✓	✓	✓	✓
Layer list	✓	✓	✗	✗
Navigation guide	✗	✗	✓	✓

Table I shows the comparisons between the existing systems. Three existing systems were chosen for this such as the USF Interactive Campus Map, University of Calgary Interactive Map and ClassFind.com. To compare, all three systems have features for the user to choose their desired location and to search it by key in the key word in the search feature available. These systems are also able to display a real live map for the user to use it. But all these systems do not have live location features where it displays the current location of the users. For USF Interactive Campus Map and the University of Calgary Interactive Map, both somehow have almost the similar features. They use coordinates in their system, the real-life map has the layer list functions where the user can choose which layer, they prefer to use. For example, campus planning, parking, and transportation. But these two systems do not have a starting point for the user to start navigating. Other than that, it does not have a navigation guide for the user to use to help them navigate to the location. But it is different for ClassFind.com. In this system, it has a starting point and navigation guide step by step for the user to start navigating. The navigation guide is in the form of pictures with arrows in it which display the landmarks of the route and location. Unfortunately, it does not use coordinates in its system, and it does not have a layer list for the user to use. This study has proposed NavigateMe system, a system that provides clear and real-life visualization of the routes to the desired location for navigation. This system has the location displayed for the user to choose from, for example, the list of room in KICT. Second, the

https://doi.org/10.31436/ijpcc.v10i2.462

system gives the user a list of starting points where the user may use where they want to start navigating. Other than that, NavigateMe displays the images with arrows for the user to use as a navigation guide. This system provides the user the ability to search their desired location and the option to use the real- life map which is linked to the Google Map. NavigateMe does not display real-life maps because this system is meant to help the user that has low visual and spatial capacity, in other words, they have difficulties in using the real-life map. This also means that the system does not have a layer list and live location function since it is an in-building navigation application. The other important feature of the system is the authenticity of the contents shown on the website are provided by only authorized staff and the system.

III. Proposed System

A. Design

In designing the system, a prototype for the system was created using Canva. The design was inspired from the Classfind.com navigation system. The design was done by completing the requirements specification for this system. As shown in Fig 1, there are two systems in the use case which are NavigateMe and Firebase.

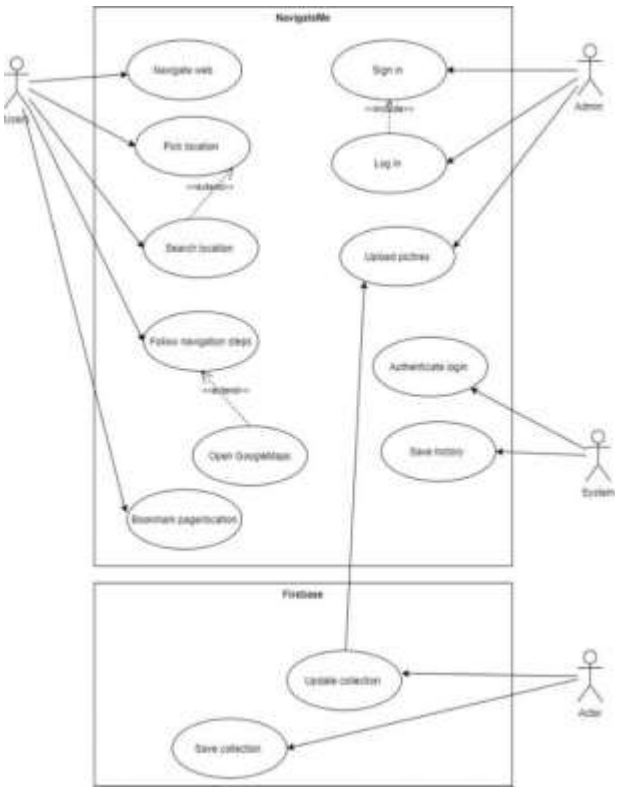

Fig. 1 Use Case Diagram

The actors for the NavigateMe are users that interact with the front-end of the application and the second actor is the admin that manages and updates the contents. The description of the use case is stated in detail in Table II.

TABLE II
DESCRIPTIONS OF USE CASE DIAGRAM

Use Case	Description
Naviagate web	Allow the user to navigate through the web application
Pick location	Allow the user to pick their desired destination
Search location	Allow the user to search their desired location by key in the key word
Follow naviagtion steps	The system display series of images as guide for the user to navigate
Sign up	Admin create account to get authorize permission to manage database
Login	Allow the admin to log in into the web application
Upload pictures	Allow the admin to upload images into the web application
Update collection	Allow the admin to update the images in the database
Save collection	Allow the admin to save changes of collection

The flow of the whole process of using the navigation system is shown in Fig 2 and relationships between the entities is systematically explained in Fig 3.

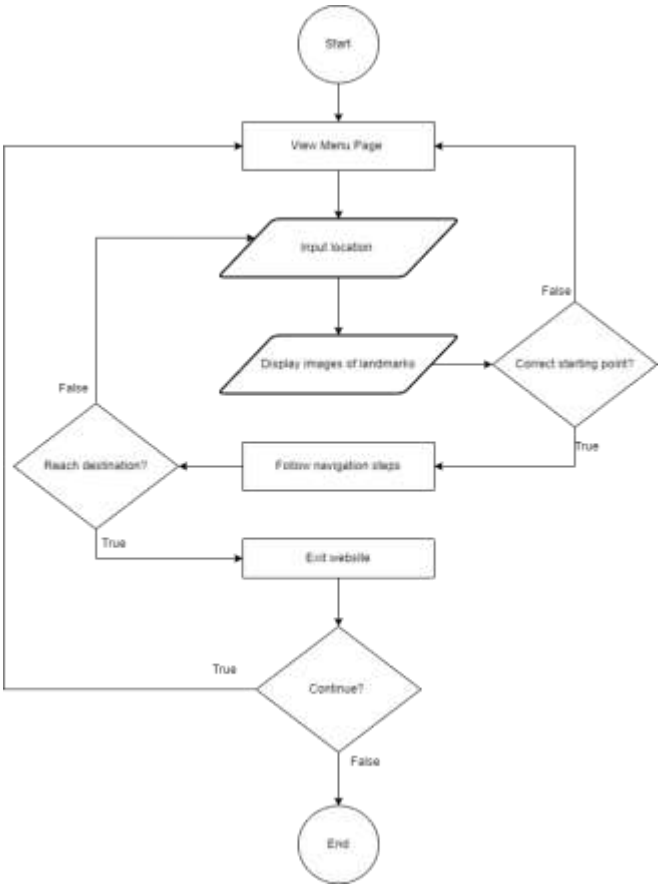

Fig. 2 Flowchart Diagram

https://doi.org/10.31436/ijpcc.v10i2.462

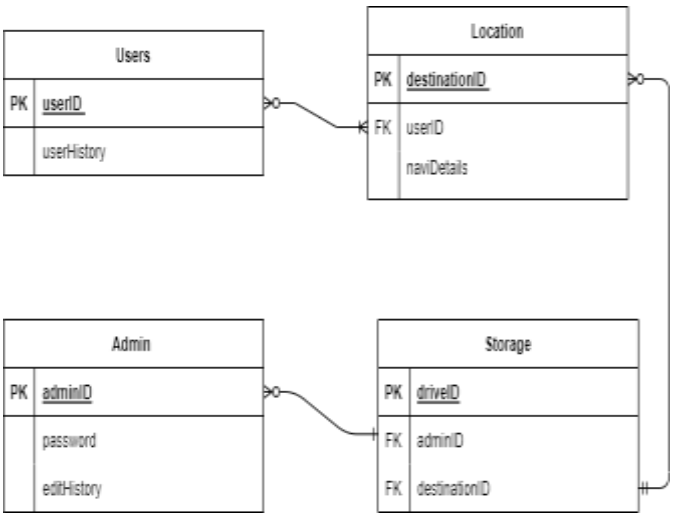

Fig. 3 Entity Relationship Diagram

B. *Implementation*

The data required for the proposed system is collected by capturing pictures of the landmarks within the KICT building and detailed information on every location is taken from the IIUM official website. The programming language used is Dart and the application is connected to the Firebase Realtime Database. The system has two different types of interfaces which are for the user who are the visitors and for the admin who are the authorized personnel that manage the system.

Fig 4 the staring to Fig 5 are all the prototypes of the mobile application opened in a website mode (e.g. Chrome). Fig 4 runs until Figure 5 where the pages displayed to the users after clicking "Start Searching" button in the users' homepage. The homepage has two buttons' options; users click on the "Start Searching' button to use the application while admins click the "Log In" button to log in. The pages shown below is the focus of the navigation application.

Fig. 4 Homepage

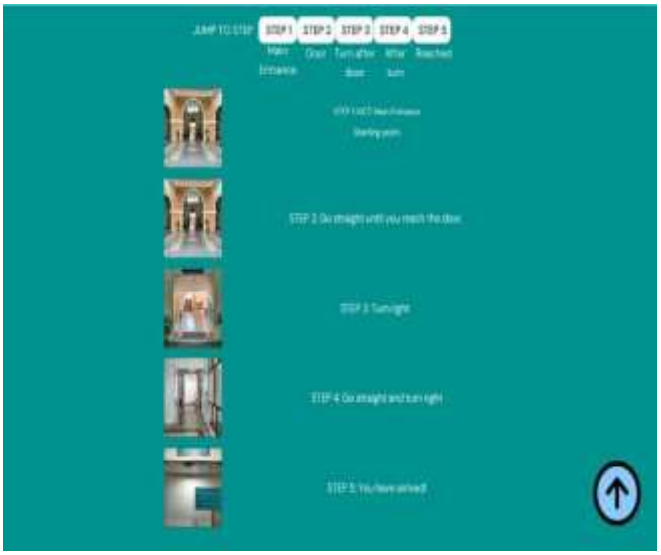

Fig. 5 Navigation steps Page which is for the user

C. *Testing*

Unit testing has been chosen to test the NavigateMe system. Generally, unit testing is where the individual components of the software are tested and validate that each unit of the software works as intended and meets the objective. The primary goal was to ensure that each unit of the system performs as expected in isolation, before integrating them into the overall system. For NavigateMe system, there are 3 modules for the testing and all these modules are decided according to the list of system requirements.

1. User Interface Module

This module tested the responsiveness of interactive elements, such as buttons and forms, was a primary focus. The system was tested to ensure that all interactions, including clicking, hovering, and inputting text, were accurately and quickly registered. This responsiveness is essential for a smooth user experience.

2. Data Display Module

This module is tested on the images displayed in the system. The system was tested to ensure that the data that were stored in the databases were able to be displayed in the system upon user input such as clicking and inputting text.

3. Admin Module

This module tested on the admin side of the system. This system was tested to ensure it can apply changes done by the admin to the user system such as location, images and the navigation steps.

Under these modules are the components of the system. The table below shows the features that were tested according to its module.

TABLE III
TEST MODULES

Modules	Components
User Interface	Navigation bar; Search box; Chatbot; Selecting building of the location; Display details of the destination; Choosing the location; Choosing the starting point; Use indicator to choose steps of the navigation guide
Data Display	Display image Display navigation steps
Admin	Login Input new locations, images, and steps Save updates

The tests were done module by module to ensure all components were working well. Any errors or unsatisfactory output were recorded while doing the tests and it was fixed and improved first before moving on to other modules. Then, the modules were integrated together and tested. During this phase, the system was tested, and errors or issues were recorded and fixed.

IV. Results and Discussion

NavigateMe's objectives are to develop the simplest version of navigation system that is user friendly to all types of users from various backgrounds and ages including those without prior IT knowledge, to guarantee the authenticity of the contents shown in the application that are provided by only authorized staff, to provide a reliable system and to provide clear and real-life visualization of the route to the location for the navigation. Thus, using the test cases in Table IV, unit testing was conducted to test all the modules of the navigation system.

Generally, unit testing is where the individual components of the software are tested and validate that each unit of the software works as intended and meets the objectives. From the testing, it was observed that almost all the test cases being tested passed with a few of them not meeting the requirements (see Appendix 1). For the planned users' interfaces, unit testing allows us to test the navigation within the application from page to page. Clicking on the "Start Searching" button implemented in the home page for the users will lead to the next pages, "Pick Your Destination" pages in which the destinations are sorted in different pages named as level 1, level 2, level 3, level 4 and level 5 following the real layout of the KICT building. The codes also include functions such as URL launcher to navigate external websites.

The links are embedded under each of the images in the form of image description as can be seen in the prototype in the Implementation section. Overall, all the features for the users' interfaces worked fine but the problem was in the limitations in the search function as the system was not implemented with the auto suggest feature or the auto correct feature that could make the usage of the application easier especially when the users want to search something within the application. For the admin interfaces, it was observed that the login functions worked fine but the problem was that the edits made by the admin were not displayed in the users' interfaces. The recommendations and studies on how to resolve each of these issues that arise from the unit testing are covered in the discussion. The user would benefit from the implementation of the auto suggest or auto correct features, which might make using the application easier, particularly when the user wants to search within the application. One possible solution to the issue of photo updates not appearing on the user's end is to thoroughly inspect the connection between the database and navigation system. In addition, a chatbot feature might be included to the navigation system to help users, such as when they have questions about the Kulliyyah or the location

V. Conclusion

This study examined and discussed research articles on navigation systems as well as the current on-campus navigation system. It advances the conversation about contrasting the features of all current navigation systems. All these systems have certain flaws, and NavigateMe was suggested as a solution to address them. NavigateMe only provides navigation within the KICT building, thus it is intended that in the future, its coverage will expand to include buildings from various kuliyyah and benefit the IIUM community members as well as visitors.

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] classfind.com, "classfind.com." Accessed: Dec. 21, 2023. [Online]. Available: https://classfind.com/

[2] ucalgary-gs.maps.arcgis.com, "University of Calgary Interactive Map." Accessed: Dec. 21, 2023. [Online]. Available: https://ucalgary-gs.maps

[3] gis.usf.edu, "USF Interactive Campus Map." Accessed: Dec.21, 2023. [Online]. Available: https://gis.usf.edu/ICM/

[4] P. C. Lin and S. I. Chen, "The effects of gender differences on the usability of automotive on-board navigation systems- A comparison of 2D and 3D display," Transp Res Part F Traffic Psychol Behav, vol. 19, pp. 40–51, 2013, doi: 10.1016/j.trf.2013.03.001.

[5] S. P. Ross, R. W. Skelton, and S. C. Mueller, "Gender differences in spatial navigation in virtual space: Implications when using virtual environments in instruction and assessment," Virtual Real, vol. 10, no. 3–4, pp. 175–184, Dec. 2006, doi: 10.1007/s10055-006-0041-7.

[6] M. Firdaus Aminuddin, A. Helmi, M. Kadir, and I. Nazmi, "The Development of Class Location Finder Application: Case Study of Politeknik Kuching Sarawak (Pembangunan Aplikasi Pencari Lokasi Kelas: Kajian Kes Politeknik Kuching Sarawak),"2022. [Online]. Available:http://myjms.mohe.gov.my/index.php/josstedhttp://myjms.mohe.gov.my/index.php/jossted

[7] A. Caleb, C. O. Akanbi, I. K. Ogundoyin, and A. O. Lawal, "Implementing A University Mobile Navigation System," 2014. [Online].Available: https://www.researchgate.net/publication/353958656.

[8] M. Chattopadhyay, Jadavpur University. School of Mobile Computing and Communication, P. I. India. University Grants Commission. University of Potential Excellence Program, Institute of Electrical and Electronics Engineers, and IEEE Computer Society, International Conference on 2015 Applications and Innovations in Mobile Computing (AIMoC): proceedings: Jadavpur University, Kolkata, India, February 12-14, 2015.

[9] S.A. Mohammed, M.A. Ighe, A. Nordin. Information Quality Requirements for a Nutrition App Based on Experts Interviews. InInternational Conference of Reliable Information and Communication Technology 2021 Dec 22 (pp. 551-558). Cham: Springer International Publishing.

[10] M.A. Ighe, S.A. Mohammed, A. Nordin, N.A. Mohamadali. Improving Information Quality Requirements for Online Health Information Systems: A Review on the Previous Frameworks. Journal of Computational and Theoretical Nanoscience. 2019 Sep 1;16(9):3663-9

Appendix 1

Test Case ID	Objective	Input	Expected Result	Special Procedural Requirements
TC-01-001	Navigate through website	User click on the navigation bar	The desired page is displayed	The link to each page is working and stable internet connection
TC-01-002	Key in location in search box (No auto-correct)	Users type the keyword of the location or the exact name of the location	The navigation steps to the location is displayed	The users have to write the correct name.
TC-01-003	Communi cate with a chatbot on a website.	Users click on the chatbot and write on the message box displayed	Chatbot display an appropriate e reply message	Must have a stable internet connection
TC-01-004	Choose any building of their destinatio n.	Users click on the link (the name) of their desired location (e.g. "Kulliyyah of ICT")	The next page, the page of starting point is displayed	Must have working links and stable internet connection
TC-01-005	View details of location.	Users click on "Details" under the destination link.	IIUM official website containing all the details of the location will be displayed	Must have working links and stable internet connection
TC-01-006	Choose a room in a certain level of the building.	Users click on "FIND" button for any location they want to go to (e.g button under the "CITA")	The next page, the starting point page is displayed	Must have working links and stable internet connection
TC-01-007	Choose starting point	Users click on the "Start" button under the name of any the starting points provided in the page (e.g. button under "Cafeteria ")	The next page, the navigation steps page will be displayed	Must have working links and stable internet connection
TC-01-008	Display navigation n steps for users	Users click on "Start" button	The navigation steps page will be displayed	None
TC-01-009	Choose any steps of navigation	User click on steps button (e.g. "Step 3")	The page will scroll down to that particular step (in case the steps are long)	Must have stable internet connection at that particular time, if not need to just scroll there
TC-01-010	Login (Admin)	Admin key in their username and password in the space provided	The admin can view the next pages that they can do updates on	Authorized account with correct username and password
TC-01-011	Update data on the website (pictures and details)	Admin click on the edit icon	The admin can do updates on the information and upload pictures on the website	Only those who are authorized account can see the edit features
TC-01-012	Update picture collection in database (google drive).	The admin upload more pictures or delete pictures in	The collection is updated	Admin must be authorized and internet connection

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.483

An Empirical Study for the Dynamic and Personalised Learning Experience of the AI Course Generator

Sophian Faza Amal, Ismail Abu Saiid, Hafizah Mansor*
Department of Computer Science, Kulliyyah of ICT, International Islamic University Malaysia, Selangor, Malaysia.

*Corresponding author hafizahmansor@iium.edu
(Received: 13th May 2024; Accepted: 2nd June 2024; Published on-line: 30th July 2024)

Abstract— In a world that is quickly evolving, the demand for continuous learning and upskilling is critical for personal and professional growth. However, many learners struggle to create personalised, efficient learning paths tailored to their unique needs due to the limitations of traditional course creation methods, which require significant human input and expertise. This project aims to address this problem by developing "*modulo*," an innovative platform designed to automate the creation of personalised and structured learning paths. The objectives of "*modulo*" are to leverage artificial intelligence and external APIs to generate customised study plans for any chosen subject, integrate curated YouTube tutorials and supplemental materials, and enhance the learning experience with adaptive quizzes tailored to user progress. The methodology follows an Iterative-Waterfall approach, combining structured phases with iterative cycles to incorporate feedback and adapt to emerging challenges. The system architecture is built on a microservices framework, with a frontend developed using React and Next.js, and a backend supported by Supabase with Prisma for database management, NextAuth for user authentication, and Stripe for payment processing. The result is a scalable and maintainable platform that empowers diverse user groups by enhancing education accessibility. "*modulo*" provides a dynamic and personalised learning experience, making a meaningful impact on self-directed learning.

Keywords— AI, APIs, educational technology, course generation, personalised learning experience.

I. INTRODUCTION

In today's environment of fast change, continuous learning and upskilling are essential for personal and professional growth. While online learning platforms like Udemy, Coursera, and Khan Academy offer extensive resources, many learners struggle to create personalised, efficient learning paths tailored to their unique needs. Traditional course creation methods require significant human input and expertise, making it challenging to meet individual learner requirements effectively. This project introduces "*modulo*", an innovative platform designed to transform the self-study experience by automating the creation of personalised learning paths. Leveraging artificial intelligence (AI) and machine learning, *modulo* generates customised study plans based on user-selected topics, integrating relevant YouTube tutorials and supplemental materials. The platform enhances learning with adaptive quizzes, tailored to user progress, to reinforce understanding of key concepts.

Our project aligns with the Sustainable Development Goal (SDG) 4, which underscores the importance of quality education. SDG 4 aims to ensure inclusive and equitable quality education and promote lifelong learning opportunities for all [1]. By providing a dynamic and personalised learning experience, *modulo* contributes to making education more accessible and tailored to individual needs, supporting lifelong learning and educational equity.

The key objectives of the project are as follows:

- Automating course generation using AI algorithms.
- Curating relevant content through application programming interface (API) integrations.
- Implementing adaptive quizzes to verify and solidify learning.
- Creating an intuitive user interface for seamless interaction.

II. REVIEW OF PREVIOUS WORKS

In recent years, the field of educational technology (EdTech) has experienced rapid growth and innovation, with advancements in various technologies reshaping the landscape of teaching and learning. This review of previous works delves into two key subtopics driving this evolution: Trends and Advancements of Technology in Education, and Integration of AI in Educational Platforms. Through an examination of these subtopics, this review aims to summarise and provide valuable insights into the current state of EdTech and its implications for the future of learning.

https://doi.org/10.31436/ijpcc.v10i2.483

A. *Trends and Advancements of Technology in Education*

Recent advancements in EdTech have significantly impacted teaching and learning. Some of the key trends include:

1) *Artificial Intelligence*

One of the most prominent trends in EdTech is the integration of AI into educational platforms and systems. AI has the power to completely change how we educate, learn, and evaluate the progress of our students [2]. AI-powered tools and applications, such as chatbots, virtual tutors, and personalised learning systems, are revolutionising how educators deliver instruction and how students engage with course materials.

2) *Immersive Technologies*

Another significant trend is the growing use of immersive technologies, including virtual reality (VR) and augmented reality (AR), in education. VR and AR technologies offer immersive, interactive learning experiences that allow students to explore virtual environments, conduct experiments, and engage with complex concepts more tangibly and engagingly. While augmented reality allows teachers to lead their students through 360° views and 3D objects, virtual reality allows the exploration of the complete universe virtually [3].

3) *Gamification*

Saleem, Noori, and Ozdamli [4] highlight in their literature review that gamification can serve as an effective tool for acquiring knowledge and enhancing critical capabilities such as decision-making, cooperation, and communication. Gamified learning platforms achieve this by incorporating game elements, such as points, badges, and leaderboards, into educational activities to incentivise participation and foster a sense of achievement.

It is crucial to remain informed about emerging trends in EdTech, including AI, VR & AR, and gamification, which present fresh possibilities for personalised and immersive learning encounters [5]. Thus, to fully harness the benefits of technology in education, educators, policymakers, and stakeholders must address the challenges and considerations associated with its implementation and ensure that technology-enhanced learning remains inclusive and learner-centred.

B. *Integration of AI in Educational Platforms*

AI integration in educational platforms offers transformative opportunities. Recent developments include:

1) *Automated Course Generation*

AI-driven educational platforms leverage machine learning algorithms, natural language processing (NLP), and other AI technologies to provide personalised learning experiences, automate administrative tasks, and facilitate real-time feedback and support for learners. Wijerathne et al. [6] introduced "Create-My-Course," an automated platform tailored for self-paced programs in asynchronous e-learning. The platform utilises AI algorithms to automate course generation processes, including video segmentation, transcription, lecture note generation, question creation, and past paper suggestions.

2) *Personalised Learning*

It is also valuable to consider any existing platforms that utilise AI technology to automate course generation processes. AI-driven platforms such as Coursebox [7] and Courseau [8] demonstrate the practical applications of AI in course creation, highlighting the potential for personalised and adaptive learning experiences. A comparison of the features of Coursebox, Courseau and our AI Course Generator, *modulo* is shown in Table 1 below.

TABLE 1 COMPARISON OF FEATURES BETWEEN COURSEBOX, COURSEAU AND *MODULO*

Features	Coursebox	Courseau	*modulo*
Personalised course outlines and study plans.	✓	✓	✓
Written material such as essays, summaries, and transcriptions.	✓	✓	✓
Curated video tutorials	✗	✗	✓
Adaptive quizzes	✓	✓	✓

Video tutorials can be viewed as part of a sophisticated electronic teaching strategy, which becomes more effective when combined with other techniques and tools [9]. While Coursebox and Courseau demonstrate the versatility and capabilities of AI technology in automating course creation processes, they lack the integration of video tutorials, which are an important component of modern learning experiences. Our AI Course Generator addresses this gap by incorporating the YouTube API to find and curate the best and most relevant video tutorials for each course. This ensures that learners not only receive structured and personalised content but also benefit from high-quality visual aids that enhance understanding and engagement.

III. METHODOLOGY

A. *Iterative-Waterfall Approach*

We have carefully selected the Iterative-Waterfall technique, which is well known for combining the structured

https://doi.org/10.31436/ijpcc.v10i2.483

aspects of the waterfall approach with the flexibility of iterative cycles. The iterative waterfall model, also known as the mini-waterfall model, addresses the limitations of the traditional waterfall model [10]. This approach allows for continuous refinement and adaptation as we progress through the development lifecycle. The Iterative-Waterfall methodology maintains the organised and sequential phases of the Waterfall model while incorporating feedback loops and iterations to enhance adaptability and efficiency, which can be seen in Figure 1 below.

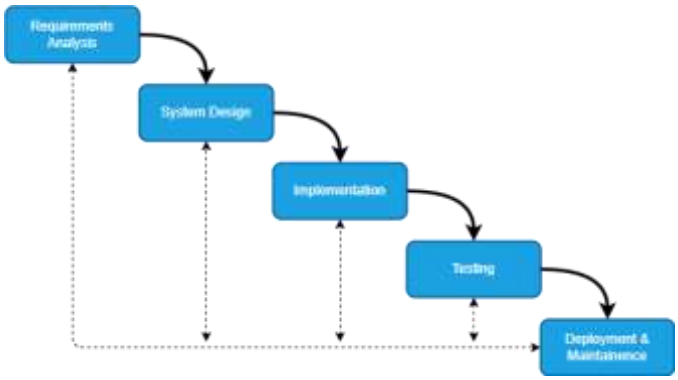

Fig. 1 Iterative-Waterfall Model

The next sections will examine each stage of our Iterative-Waterfall technique as it relates to our project, providing more detail on the particular tasks, approaches, and results included in each phase.

B. Requirements Analysis

The requirements analysis for the AI Course Generator platform was shaped by insights gathered from an online survey involving 50 respondents who were interested in self-directed learning platforms, with the majority being students and some professionals. These respondents expressed a strong inclination towards utilising online platforms dedicated to self-directed learning, underscoring the importance of structured learning paths and personalised study plans. Additionally, we identified the potential for leveraging various APIs to enhance the platform's functionalities, including Pexels for visual resources, OpenAI for intelligent interactions and content development, and YouTube for selected instructional content. These findings, coupled with users' expectations for features like automated course generation and adaptive quizzes, provide valuable guidance for the development of a user-centric and comprehensive learning platform.

Firstly, an online survey conducted with the 50 respondents provided valuable insights into user requirements, revealing a strong interest in self-directed learning activities, with 88% currently engaged in such pursuits. Furthermore, 90% expressed interest in utilising an online platform for self-directed learning, indicating a high demand for such services. The survey highlighted the importance of structured learning paths, with 84% considering it very important to have predefined subtopics and resources. Moreover, 98% of respondents preferred personalised study plans tailored to their interests and learning goals, emphasising the need for adaptive and customisable learning experiences. Essential features such as automated course generation, adaptive quizzes, and a user-friendly interface were prioritised, reflecting users' expectations for a seamless and intuitive learning environment.

The survey results highlighted key user requirements, such as the importance of 1) personalised study plans, 2) automated course generation, and 3) adaptive quizzes. Users also expressed a preference for 4) visually appealing interfaces and access to 5) supplemental materials/ content. The charts of the results of these features can be seen in Figure 2 and Figure 3. This has guided us to incorporate these features as requirements to be developed into the *modulo* platform.

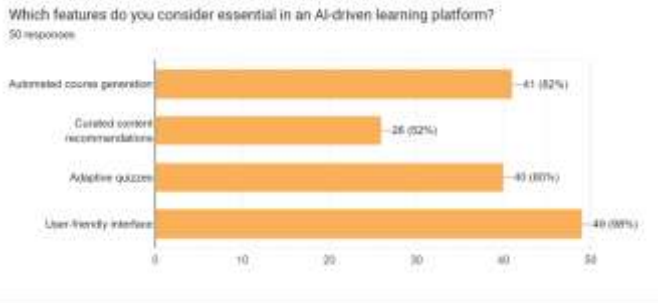

Fig. 2 Essential Features

Fig. 3 Dashboard Features

Moreover, recognising the immense potential of API integrations, our project is poised to leverage these technologies to enhance the AI Course Generator's functionalities. Multiple APIs are integrated to enhance the platform's functionality. These APIs include Pexels for visual resources, OpenAI for intelligent interactions and content development, and YouTube for selected instructional content. These APIs will be essential building blocks for creating a thorough learning ecosystem on our platform.

https://doi.org/10.31436/ijpcc.v10i2.483

The requirements analysis process has provided essential insights into user preferences and technological opportunities. With a clear vision informed by user feedback and technological advancements, the project is poised to deliver a transformative learning experience tailored to the needs of self-directed learners.

C. System Design

Outlining the system architecture, database design, and technological components required for the development and implementation of our website is the focus of our System Design phase.

1) System Architecture

A microservices architecture will be used in the development of our website to ensure scalability, maintainability, and effective performance. The core components include:

- Frontend Framework: Utilising Next.js for client-side rendering, TailwindCSS for styling, and shadcn for component management.
- Backend Infrastructure: Employing Supabase with Prisma for a cloud-hosted SQL managed database, integrated with NextAuth for user authentication and payment via Stripe.
- Deployment & Hosting: Deployment will involve pushing the project to GitHub for version control and deploying on Vercel for seamless integration with Next.js. The GPT API server will be hosted on a dedicated Linux server. Continuous monitoring, regular updates, and user feedback integration will ensure optimal performance and user experience.

2) Component Details

The frontend components of the AI Course Generator platform include several key features. The Sign Up and Login functionality, powered by NextAuth, ensures secure user authentication, allowing users to register and log in. The Dashboard/Library displays curated courses and user-specific recommendations, providing easy navigation for an optimal exploration experience. The Create Course Page would enable users to select topics of interest and generate personalised study plans using AI & API algorithms. Once generated, the Course Page showcases the complete course structure, including all modules and their respective lessons. Finally, the Lesson Page presents the lesson content, such as videos and summaries, and includes adaptive quizzes for each lesson to reinforce learning.

The backend components of the AI Course Generator platform are designed for efficiency and security. Database management is handled using Supabase with Prisma, which ensures secure storage of user data, course structures, and user preferences. NextAuth is integrated with Stripe to provide secure user authentication and manage subscription and payment features. Additionally, the platform leverages external APIs such as Pexels for visual resources, OpenAI for content development, and YouTube for tutorial content, enriching the overall learning experience.

3) Data Flow & Integration

The user flow and interaction sequence for the AI Course Generator platform involves several steps, which are illustrated in a use case diagram (Figure 4) and a flowchart (Figure 5).

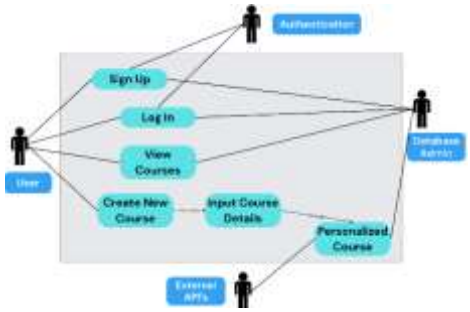

Fig. 4 Use Case Diagram

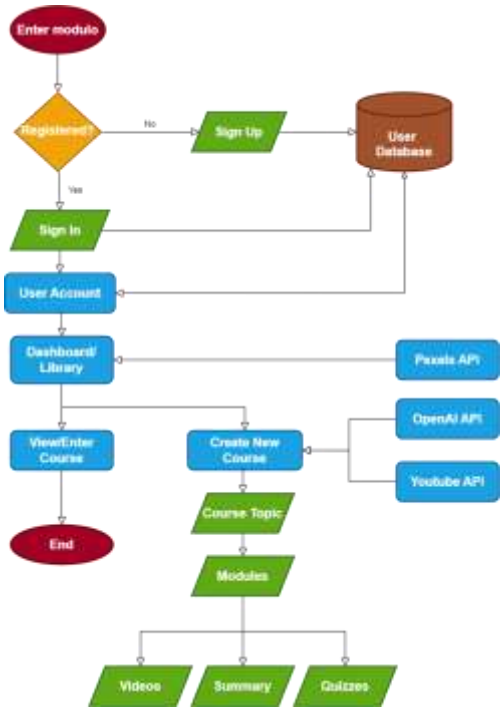

Fig. 5 System Design Flowchart

The sequence begins with user registration and login, followed by browsing and selection of topics. Next, the backend processes these requests, utilising AI algorithms to generate personalised courses and fetch relevant content

https://doi.org/10.31436/ijpcc.v10i2.483

from integrated APIs. Once the course is generated, it is displayed for the user. Finally, users can view the course and interact with quizzes, with the processed data sent back to the front end for display and interaction.

4) High-Fidelity Prototype

A horizontal high-fidelity prototype of the frontend components was created to visualise the user interface, navigation flow, and overall layout of the platform before actual development began. The prototype was fully coded using Next.js for client-side rendering, TailwindCSS for styling, and shadcn for component management.

D. Implementation

The implementation phase of the AI Course Generator project commenced with the development of the backend components, followed by enhancements to the frontend interface based on the high-fidelity prototype.

1) Backend Development

The backend development process utilised Supabase, a fully managed MySQL-compatible database platform that supports the growth of organisations of all sizes in a cloud-based environment. Supabase provided the foundation for storing and managing the project's data securely and efficiently. Additionally, Prisma ORM, a next-generation ORM (Object-Relational Mapping), was employed to facilitate seamless integration with Supabase. Prisma simplifies database interactions and makes working with databases easy for application developers, enhancing productivity in the backend development process.

a) Database Schema:

The database schema was designed to include model-tables such as Account, Session, User, UserSubscription, Course, Module, Unit, and Question, all interconnected to manage user data, course content, and subscriptions effectively. Figure 6 depicts the database schema that was created, illustrating the relationships between different models/tables. This schema outlines the structure of the database.

Fig. 6 Database Schema

b) Integration with External Services:

The Supabase database was also integrated with Stripe, a payments platform that enables businesses to accept credit cards, debit cards, and various popular payment methods globally, all through a single integration. Stripe provided robust payment processing capabilities, allowing the AI Course Generator platform to manage user subscriptions and control the number of course generations allowed per user seamlessly. Table 2 below shows the initial subscription plans that have been incorporated within the platform.

TABLE 2 INITIAL SUBSCRIPTION PLAN

	Free Users	Subscribed Users
Course Generations	Limited (5)	Unlimited

Furthermore, NextAuth, a flexible authentication and authorisation library, was integrated through the database to facilitate user authentication and streamline payment processing. NextAuth simplifies user authentication processes, providing a secure and user-friendly experience for accessing the platform's features and services.

c) Course Generation with APIs:

The course generation process leveraged the YouTube API and OpenAI API in tandem to create personalised courses. Firstly, users provided the topic/title and details of the course they desired, which were then sent to the OpenAI API to generate a study plan based on the input. This study plan encompassed the creation of modules, lessons, and quiz questions tailored to the user's preferences.

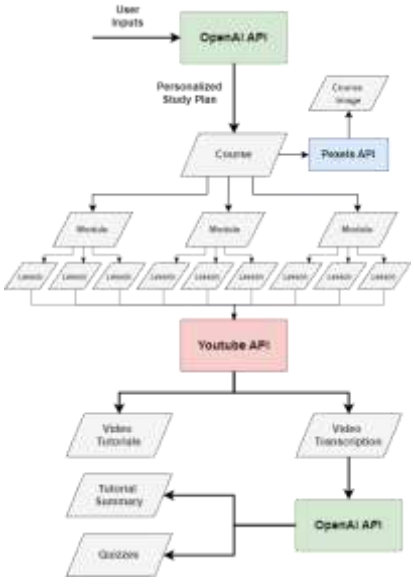

Fig. 7 Integration of All the APIs for the Course Creation Process

https://doi.org/10.31436/ijpcc.v10i2.483

In addition, the YouTube API was utilised to identify relevant videos for each lesson based on their transcription. The OpenAI API received the transcription of each lesson's video to generate summaries and formulate quiz questions and answers based on the video content. These questions and answers were then used to create quizzes in multiple-choice format for user interaction. Lastly, the Pexels API which is a provider of stock photography and stock footage was integrated to procure images for each course, enhancing the visual appeal of the dashboard/library interface. These images provided visual representation for different courses, improving user engagement and navigation. Figure 7 shows the integration of all the different APIs for the course creation process.

2) Frontend Development

Following the completion of backend development, attention was directed towards enhancing the frontend interface, as the core outline was already built as a high-fidelity prototype in the system design phase. Using Next.js with TailwindCSS, the user interface underwent significant improvements to enhance aesthetics, usability, and overall user experience. Screenshots of the revamped interface were captured to showcase the updated look and feel of the platform. Figure 8 to Figure 13 display the screenshots of the main pages of the *modulo* platform.

Fig. 8 Sign-Up Page

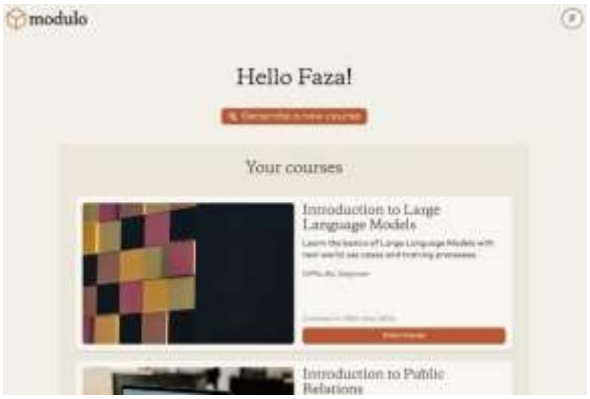

Fig. 9 Dashboard/Library Page

Fig. 10 Create a Course Page

Fig. 11 Course Page

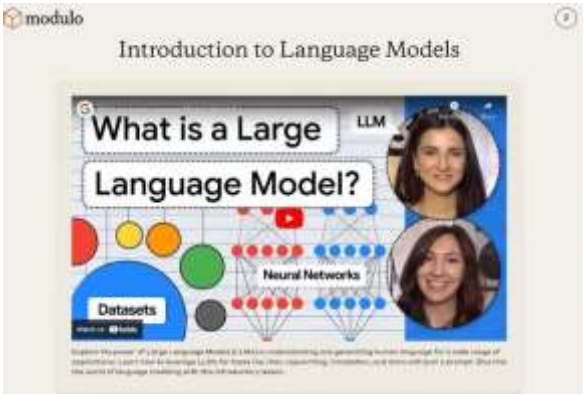

Fig. 12 Lesson Page video tutorials

The backend development focused on establishing a robust infrastructure for managing user data, course content, and subscriptions, while the frontend enhancements aimed to improve the visual appeal and usability of the platform. Together, these efforts contributed to the realisation of the AI Course Generator platform, providing users with a seamless and engaging learning experience.

https://doi.org/10.31436/ijpcc.v10i2.483

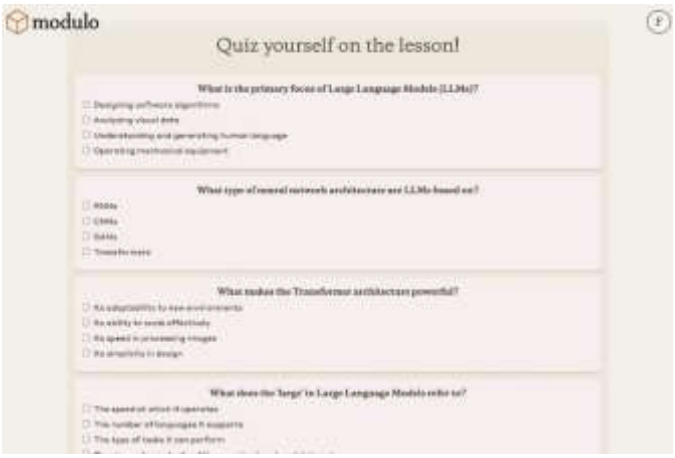

Fig. 13 Lesson Page quizzes

E. System Testing

A User Acceptance Testing (UAT) was performed for the testing of the system and to confirm that the platform worked as intended and that it is usable from an end-user perspective. The UAT was conducted face-to-face in IIUM Gombak Selangor, Kuala Lumpur, Malaysia, on May 18th. It involved 3 participants (students in the Department of Computer Science), who were already aware of our project background as they were already involved in the gathering of the user requirements. The UAT plan involved users performing all possible actions within the system with a record of the results.

1) Test Plan

The UAT test plan was organised to include all the components for comprehensive testing. The test plan was based on various scenarios, where a description of the scenarios is shown in Table 3 and a real example of a scenario is shown in Table 4.

TABLE 3 SCENARIO DESCRIPTIONS

Pages	Each page of the platform tested
Test Data	Specific test data were used to simulate realistic user interactions.
Test Condition	Various conditions under which users might interact with the system were considered.
Expected Result	For each test condition, an expected result was defined to establish the benchmark for successful functionality.
Actual Result	The actual outcomes were recorded to identify any discrepancies between expected and actual system behaviour.
Remarks	Observations and feedback from the users were noted to highlight areas of improvement or additional feature requirements.

TABLE 4 SCENARIO EXAMPLE

Pages	Test Data	Test Condition	Expected Result	Actual Result	Remarks
Course Page	N/A	Selected "Start Lesson" for any of the Lessons within a Module.	Redirected to the respective Lesson Page	☑	Worked as expected

2) Enhancements

The UAT was successfully completed, with all core features functioning as intended. However, based on user feedback and remarks, several areas for enhancement were identified to further improve the platform's usability and functionality. These enhancements included:

a) "Forgot Password" Feature

A new feature was added to the login page, allowing users who forgot their password to reset it easily. This enhancement aimed to provide a straightforward solution for password recovery which was lacking.

b) Additional Modules Post-Course Generation

Users expressed the need for flexibility in adding more modules even after a course had been generated. This feature was implemented to allow continuous course customisation, accommodating evolving learning needs.

F. Deployment & Maintenance

The deployment and maintenance phase ensured that our AI Course Generator platform, *modulo*, was not only successfully launched but also remained functional and up-to-date post-deployment. The first step involved pushing the entire project to a GitHub repository, ensuring that all code was version-controlled and easily accessible for further development and deployment processes. Subsequently, a Vercel account was created and linked to the project's GitHub repository. Vercel was chosen for its coherent integration with Next.js and its capabilities in automatic deployments.

The repository was then deployed on Vercel as a website, with necessary environment variables such as API keys and database connection strings configured to ensure the application could function correctly in the live environment. Following this, the GPT API server, responsible for handling OpenAI API calls, was pushed to a separate GitHub repository. This server forms the backend of our application, processing user requests and generating personalised content. Furthermore, a dedicated Linux server was used, where the latest commits from the GPT API server were

pulled and the server was made to handle API calls, ensuring that the AI functionalities of the platform were operational.

Post-deployment, the platform's maintenance involved continuous monitoring and updates to ensure optimal performance and security. Key maintenance activities included monitoring and logging the application's performance, applying regular updates to software components, libraries, and dependencies, and integrating user feedback into subsequent iterations to enhance functionality and user experience. These steps ensured that *modulo* was successfully deployed and maintained, providing a reliable platform for self-directed learners to generate and follow personalised learning paths.

IV. Conclusions

The development of the AI Course Generator platform, *modulo*, represents a significant advancement in self-directed learning. This project successfully addressed the challenge of creating personalised and structured learning paths by leveraging AI and machine learning technologies. Through the implementation of a microservices architecture, the platform ensured scalability, and efficient performance. The Iterative-Waterfall methodology employed during the development process allowed for continuous refinement and adaptation, ensuring that the final product met the needs and expectations of its users. The thorough requirements analysis, informed by a survey of potential users, guided the design and implementation phases, resulting in a user-centric and feature-rich platform.

Looking ahead, future work should consider the existing limited user testing on a small group of three participants only from the Department of Computer Science in the current study. Although their feedback is essential, conducting a more extensive testing phase with a bigger and more diverse set of users would yield a more comprehensive evaluation of the platform's usability and effectiveness. Increasing the number of users participating in testing could reveal additional insights and identify areas that need improvement. Additionally, future work could explore additional features such as expanding the range of integrated APIs, incorporating more interactive elements like live tutorials or discussion forums, and further enhancing the adaptive capabilities of the platform to provide an even more personalised learning experience. Additionally,

In conclusion, *modulo* stands as an innovative solution for self-directed learners, aligning with Sustainable Development Goal (SDG) 4 by promoting inclusive and equitable quality education and lifelong learning opportunities for all. The successful development and deployment of the platform marks a significant milestone, paving the way for ongoing improvements and greater impact in the field of educational technology.

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] United Nations Development Programme, "Sustainable Development Goals | United Nations Development Programme," www.undp.org, 2023.

[2] V.J. Owan, K.B. Abang, D.M. Idika, E.O. Etta, and B.A. Bassey, "Exploring the potential of artificial intelligence tools in educational measurement and assessment," EURASIA Journal of Mathematics, Science and Technology Education, vol. 19, no. 8, pp. em2307–em2307, Aug. 2023, doi: https://doi.org/10.29333/ejmste/13428.

[3] P. Kuna, A. Hašková, and Ľ. Borza, "Creation of Virtual Reality for Education Purposes," Sustainability, vol. 15, no. 9, p. 7153, Jan. 2023, doi: https://doi.org/10.3390/su15097153

[4] A. N. Saleem, N. M. Noori, and F. Ozdamli, "Gamification Applications in E-learning: A Literature Review," Technology, Knowledge and Learning, vol. 27, no. 1, pp. 139–159, Jan. 2021, doi: https://doi.org/10.1007/s10758-020-09487-x.

[5] M. Jiang, "The Impact and Potential of Educational Technology: A Comprehensive Review", RAE, vol. 2, no. 7, pp. 32–49, Jul. 2023.

[6] A. Wijerathne, B. Sandaruwan, and D. Oddugama, "Create-My-Course: An Automated Course Generator for Self-Paced Programs," International Journal of Innovative Science and Research Technology, vol. 7, no. 11, 2022, Accessed: May 19, 2024.

[7] "AI Course Creator," www.coursebox.ai. https://www.coursebox.ai/ (accessed May 16, 2024).

[8] "Develop engaging courses with the help of AI.," courseau.co. https://courseau.co/ (accessed May 16, 2024).

[9] D. Airinei and D. Homocianu, "The Importance of Video Tutorials for Higher Education - The Example of Business Information Systems," Social Science Research Network, Jan. 2010.

[10] C. Kaur and V. Kumar, "Comparative Analysis of Iterative Waterfall Model and Scrum," International Journal of Computer Science Research (IJCSR), vol. 3, no. 1, pp. 11–14, Mar. 2015

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.478

Analyses of 6G-Network and Blockchain-Network Application Security: Future Research Prospect

Ammar Haziq Annas[1], Ahmad Anwar Zainuddin[1,*], Afnan Wajdi Ramlee[1], Ahmad Solihin Ya Omar[1], Muhammad Hafiz Faruqi Md Saifuddin[2], Nur Fatnin Izzati Sidik[2], Muhamad Syariff Sapuan[3], Amysha Qistina Amerolazuam[2], Muhammad Haziq Zulhazmi Hairul Nizam[2], Farah Mazlan[2], Nur Faizah Omar[2], Nur Alia Alina Abdul Rahman[2], Nur Nisa Humairah Rosdi[2], Nur Zafirah Adira Ahmadzamani[2]

[1]Department of Computer Science, International Islamic University, Malaysia, Kuala Lumpur, Malaysia.
[2]Department of Information Systems, International Islamic University, Malaysia, Kuala Lumpur, Malaysia.
[3]Department of Nuclear Science, Faculty of Science and Technology, Universiti Kebangsaan Malaysia, Selangor, Malaysia

*Corresponding author: anwarzain@iium.edu.my
(Received: 29th May 2024; Accepted: 25th June 2024; Published on-line: 30th July 2024)

Abstract— The evolution from 5G to 6G signifies a monumental progression in wireless communication technology, promising enhanced capabilities and broader applications. Building on the transformative impact of 5G with its high speeds, low latency, and improved connectivity, the transition to 6G aims to overcome the limitations of its predecessor and unlock new potentials. However, this shift is not devoid of challenges, particularly concerning the privacy and security risks inherent in the adoption of 6G networks. Reflecting on the historical trajectory of wireless technologies, from the first 0G to the current 5G networks, each generational leap has brought significant enhancements in design, coverage, speed, quality of service, capacity, and latency rates. The ongoing deployment of 5G is expected to further expand network capacity through innovative architectural advancements, such as the convergence of information and communication technologies and the implementation of heterogeneous networks. These advancements are essential in optimizing energy consumption, enhancing overall performance, and ensuring the sustainability of wireless networks. Furthermore, the convergence of emerging technologies like the Internet of Things (IoT), energy harvesting, and Simultaneous Wireless Information and Power Transfer (SWIPT) is reshaping the landscape of wireless communication. These technologies not only facilitate the deployment of numerous low-power radios but also pave the way for a more interconnected and efficient wireless ecosystem. In this dynamic world of evolving wireless technologies, the concept of mobile edge computing (MEC) emerges as a novel paradigm for providing computing, storage, and networking resources at the edge of mobile networks. By allowing latency-sensitive and context-aware applications near end-users, MEC ensures efficient operations without compromising performance. This integration of edge computing within the Radio Access Network (RAN) architecture signifies a theoretical shift towards more distributed and responsive network infrastructures.

Keywords— 5G, 6G, Computing Architecture,

I. Introduction

The transition from 5G to 6G is a significant advancement in wireless communication technology. While 5G has revolutionized industries with its high speeds, low latency, and connectivity, the limitations of 5G have prompted exploration into the wider application of 6G[1]. The main concerns with 6G usage include privacy and security risks[2]. The development of the sixth generation of cellular technology, or 6G, has started in response to the need for affordable worldwide internet access. Even though it plays a crucial role in the achievement of the Sustainable Development Goals (Target 9. c), widespread and cheap internet connection is still difficult to find. Unfortunately, Mobile Network Operators and governments do not yet have access to impartial analyses of the 4G and 5G cellular technology solutions that are available to assist them reach this goal[3]. This article uses a quantitative evaluation to close this gap by showing how current 5G policies influence universal broadband and by analysing the performance of various 4G and 5G efforts, it is still possible to determine the effect of actions on the development of 6G. Add on, to ensure the uniqueness, this evaluation uses open-source techno-economic codebase that blends remote sensing with better network methods. The analysis is used as an illustration for India, which has the second-largest mobile

https://doi.org/10.31436/ijpcc.v10i2.478

market in the world and very expensive spectrum pricing. The assessment's findings highlight the trade-offs between technical choices and the significance of existing infrastructure policies, especially fibre backhaul, which is crucial for delivering 6G quality of service[4]. According to research, fibre backhaul may effectively achieve 5G population coverage by removing all the expenses related to the spectrum licensing itself. This data maintains the distinctiveness of the conversation while highlighting the possibilities of fibre and enabling complete 5G connection. To lay a solid basis for the transition to future cellular generations, such as 6G, supporting infrastructure policies are crucial[5]. Wireless technology has significantly improved communication and multi-functional gadgets since it was adopted, becoming a pillar of contemporary culture and the digital economy.

Significant improvements in design, coverage, speed, quality of service, capacity, and latency rates occurred when wireless networks transitioned from 0G to 4G[6]. Although the rollout of 5G is still underway, it is anticipated that it will greatly contribute to capacity expansion through network architectural innovations. The 5G system architecture brought a new architecture that worked diligently. Other major strategies include the convergence of information and communication technologies and heterogeneous networks[7]. In order to optimize energy utilization for greater performance and accuracy of technical gadgets and utility items used in daily life, the study provides a For 5G mobile communication, an interference absorber for the sub-6G band that is operating in the broadband range. As wireless technology advanced, 4G networks gained popularity and next generation 5G networks started to take the front stage[8]. Technologies that can transfer huge volumes of data and signals across a variety of distances while minimizing energy loss will be necessary in the future of wireless communication in order to increase the network's overall life span[9]. Furthermore, it is anticipated that widespread The Internet of Things (IoT), energy harvesting, and Simultaneous Wireless Information and Power Transfer (SWIPT) are three crucial technologies that have come together. in the field of wireless communication and at the same time it would be crucial enablers for installing a significant number of low-power radios[10].

A novel method of supplying computing, storage, and networking resources to the mobile RAN's edge is known as mobile edge computing (MEC)[11]. Edge computing deployment allows for running delay-sensitive and context-aware applications in close proximity to end users, ensuring efficient operation without compromising the originality of MEC servers on a general computing platform within the RAN as seen in Figure 1. Integrating edge computing makes it easier to provide a mobile connection with low latency, high bandwidth, and agility. This reduces delays in the backhaul and core network[12]. In essence, MEC improves service quality and user experience by bringing computer power closer to the end customers[11], [12]. The infrastructure for real-time, context-aware collaboration presented in this paper includes diverse edge resources, including MEC servers and mobile devices. Benefits including mobile edge orchestration, cooperative caching and processing, and multi-layer interference cancellation offered by the proposed architecture can aid in the development of 5G networks. To effectively incorporate MEC into the 5G ecosystem, there are still technological obstacles and unresolved research problems to be solved[13]. The importance of determining a location or the location of the assets has long been recognized, and various technologies, such as outdoor global positioning systems (GPS), have proven to be valuable in this regard[14]. Real-time locating inside has been difficult, though. Network-based positioning has gained traction as

5G mobile networks come into being. The 5G network may be used for positioning purposes both inside and outside thanks to new radio technologies, decreased latency, specialized control protocols, and processing power at the network edge[15].

Fig. 1 Mobile edge computing architecture [16]

The foundations of network-based positioning are covered in this paper, along with more sophisticated machine-learning-based approaches. A thorough comparison of the machine learning methods applied to network-based positioning is also included. The article also presents real-world examples from a variety of fields, including industrial and automotive settings. The essay also makes a crucial shift towards placement with these networks as go towards the creation of 6G networks. The article also discusses the difficulties software-defined 5G/6G networks face, such as the use of mm-Wave spectra, the absence of channel models, massive MIMO technology, low latency, and QoE (Quality of Experience), as well as energy efficiency, scalability, mobility, and routing, interoperability,

standardization, and security. The article's main goal is to teach readers about research on SDN-5G and SDN-6G networks, as well as the issues they face from new technology. The article also discusses the difficulties that software-defined 5G/6G networks face, such as the use of mm-Wave spectrums, the absence of channel models, massive MIMO technology, low latency, and QoE (Quality of Experience), energy efficiency, scalability, mobility, and routing, interoperability, standardization, and security. The article's main goal is to teach readers about the research on SDN-5G and SDN-6G networks, as well as the newest developments in these fields and the difficulties they face.

This paper discusses the complex world of 6G-network and Blockchain-network application security, which delves into the nuances of protecting digital ecosystems in a time of rapid technological advancement. In the introduction section, an overview of the development of 6G networks, advances in wireless communication technology, and the importance of tackling security issues in an ever-changing environment is concisely stated. The discussion of the development of security protocols, technologies, and methods used in earlier generations are the main topics of the security evolution of mobile cellular networks section[6]. The vision of the 6G network and essential research works section focuses on the idea of 6G networks and examines the key studies that have prepared the way for the advancement of 6G. The next section is the 6G security requirements and proposed security architecture that addresses the fundamental security needs for 6G networks and describes the particular security criteria that are thought to be necessary for the technology to succeed. It also emphasizes a proactive and overarching approach to security and suggests security architecture to satisfy these criteria. The section on the implementation of promising technologies that are crucial to 6G networks examines potential security issues and threats. It offers perceptions of potential dangers and shortcomings in the context of these cutting-edge technologies[17]. For this paper, an overview of IoT blockchain applications in networking systems shifting the focus to this confluence was discussed in the next section. It provides a thorough grasp of this changing environment by examining how blockchain is used to secure IoT devices within networking infrastructures. This work is finally summarized and concluded in the conclusion section.

II. Security Evolution of Mobile Cellular Networks

This section discusses the security risks and privacy concerns that come with different cellular network generations, including the earliest mobile generations that had to contend with significant security issues like eavesdropping attacks, encryption problems, physical attacks, and authentication problems. These difficulties have exacerbated the threat landscape, which now has more adept and sophisticated attackers and complex attacks. Attacks that eavesdrop or violate privacy can compromise sensitive information, and encryption flaws might make it easier for attackers to decode data. Unauthorised access could occur because of physical assaults on mobile devices and network equipment. Unauthorised access is also facilitated by weak authentication procedures. Continuous research and development activities are essential to handle changing security concerns and proactively minimise potential vulnerabilities.

The 1G network was developed in the 1980s particularly to provide voice communications services. It transfers data using analogue modulation techniques. This generation faces a number of obstacles, including handover issues, a lack of security guarantees, and other transmission concerns. Furthermore, the security and privacy of data transfer cannot be ensured because telephone services are not encrypted. Because of this, the entire network and its users are vulnerable to serious security risks, such as unauthorised access and eavesdropping attacks [18].

For voice and brief message services, the second generation of mobile devices relies on digital modulation technologies such Time Division Multiple Access (TDMA) as seen in Figure 2[19]. A variety of security services, including authentication, information protection, privacy protection, and transmission protection, are provided by the GSM (Global System for Mobile Communications) standard. To identify and authorise users, network providers utilise authentication[20]. The challenges and responses method is the foundation of the 2G authentication process. Through anonymous identifiers that prevent anyone from tracking their true identities, anonymity is established. User data and signalling are protected by encryption, and the SIM generates the encryption keys. Temporary Mobile Subscriber Identity (TMSI) and radio path encryption are used by users to protect their privacy[21]. Unfortunately, despite significant security improvements over the previous generation, 2G security is still very weak. One-way authentication is a security flaw that allows the network to verify the user's identity but prevents the user from verifying their identity with the network. As a result, unapproved base stations masquerade as authorised members in order to steal user data and personal information[22].

https://doi.org/10.31436/ijpcc.v10i2.478

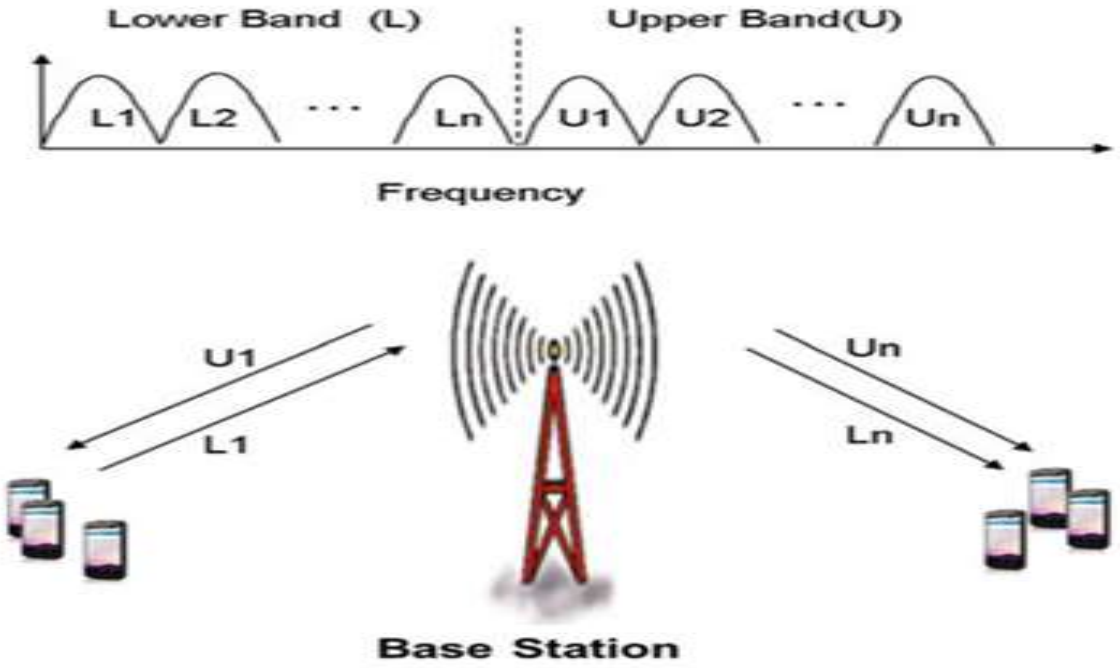

Fig. 2 The 2G cellular TDMA communication system[23]

The end-to-end encryption issue also arises when only a small portion of the communication route is encrypted. The channel is vulnerable to assaults since the other network components are not encrypted at the same time. As a result, the radio path encryption and TMSI privacy solutions outlined above are not sufficient to secure 2G networks and are vulnerable to numerous assaults, including eavesdropping[24].

In order to give internet access and boost the speed of data transfer up to 2 Mbps, the 3G network was first deployed in 2000[25]. However, with this speed, advanced services like TV streaming, internet surfing, and video streaming are available, which were not practical with earlier mobile communication[26]. The security of the 2G networks is applied to the networks of 3G. In addition, third-generation (3G) fixes a number of the security flaws that 2G had. The Authentication and Key Agreement (AKA) and two-way authentication are both included in 3G[27]. A full access control security system is established by the Third Generation Partnership Project (3GPP), which also includes user authentication and air interface security. To safeguard wireless links, users, and communications, air interface security is deployed. In order to increase reliability, it also offers a two-way authentication procedure that may verify users and the network itself on both ends (sender and receiver)[28].

For 3G networks, the 3GPP covers a number of privacy aspects, such as securely locating, recognising, and tracing consumers. 3G networks are thought to be vulnerable to IP attacks and vulnerabilities. 3G network risks are also introduced through channels of communication attacks between end devices and their home networks[29]. The following categories are used to group wireless interface threats: (1) threats to data integrity, (2) unauthorised access to data, (3) DoS attacks, and (4) unauthorised service access. Critical security risks with 3G also include protocol privacy issues connected to sniffing users' private information and identities.

A. *4G and 5G*

The fourth generation of networks provided up to 1 Gbit/s of downlink transmission and 500 Mbit/s of uplink communication in 2009[30]. excellent-definition television (HD TV) and digital video broadcasting (DVB) are two complicated applications that 4G networks can handle thanks to their low latency and excellent spectrum efficiency. IP core networks, backhaul networks, access networks, and a variety of sophisticated mobile terminals are all included in 4G systems[31]. Threats to wireless radio transmission, tampering, eavesdropping, data manipulation, and network authentication are the main 4G security issues.

https://doi.org/10.31436/ijpcc.v10i2.478

The 4G network is more susceptible to security problems than earlier mobile radio networks because of the greater indirect connection between users and mobile terminals. With the storage and computing advancements of mobile terminal devices, several security concerns suffer significant harm[32]. Examples of security issues include viruses, operating system attacks, and tampering with hardware platforms. Various Medium Access Control (MAC) layer problems, which include as eavesdropping and replay attacks, affect 4G standards and crucial management protocols. In addition to data integrity threats, issues with unauthorised clients, and tracking of location utilising MAC layer protocols, 4G networks are also susceptible[33].

As the commercialization of the 5G network approaches, it is expected that the implementation of advanced systems and high-security architectures will lead to enhanced data transfer rates. The novelty of 5G networks lies in their ability to link an ever-increasing number of gadgets while offering greater quality services to every network entity. Examining the network architecture is the most direct way to group security and privacy issues in 5G networks. Access networks, backhaul networks, and core networks are all parts of the 5G architecture. Additional security concerns are presented by several gadgets and network access techniques. Additionally, the likelihood of an assault increases as devices and access technologies are switched between [34].

Between the access and core networks, there are backhaul networks that use regular lines, satellite links, wireless channels, and microwave connections[35]. Backhaul networks don't link to devices, hence they are less private than access networks. By putting the backhaul network into the data plane using methods like Software-Defined Networking (SDN) and Network Functions Virtualization (NFV), security issues are also sent to the core network. Further Enhanced Mobile Broadband (FeMBB)'s high data rates create security issues since they increase the likelihood of DoS or resource assaults[36]. So far, two strategies for coping with signalling overloads have been devised. The first approach uses simple key management and authentication methods to permit communication between several devices, whereas the second approach makes use of protocols that would enable the grouping of devices using numerous group-based AKA protocols[37]. However, the new techniques for speeding up the 5G network can lead to security flaws. Large MIMOs, for instance, are used to conceal both active and passive eavesdropping. Additionally, unauthorised apps or actions offer a hazard to SDN implementation via OpenFlow[38].

Additionally, the migration of NFV features from one location to a different one raises safety concerns. Additional privacy concerns are connected to numerous application situations and services that 5G networks can support. Users' private information is readily leaked to the public due to the open nature of the 5G platform [39, p. 5], [40]. In the coming years, it will likely become necessary to address and resolve the privacy concerns associated with 5G [41]. The 5G CN is made up of various capabilities. NFV, SDN, and cloud technologies have made networks more dynamic than ever, which has led to several risks and vulnerabilities. The requirements for new 6G applications will be higher and the network capacity will be bigger than that of currently operational 5G networks [42] the more devices and services that exceed the signalling load. New 6G applications will have more requirements and require a larger network than the current 5G networks [6]. They also have an important effect on 6G operations. Security measures thereby ensure service reliability and consistency in ERLLC [43]. The latency impact brought on by security processes will also be covered. To guarantee the availability and continuity of resources and services, effective security solutions are regarded as high criteria. The development and security challenges from 1G to 6G are summarised in Figure 3.

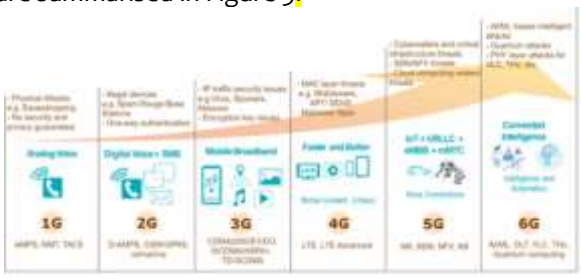

Fig. 3 The security evolution of mobile communications from 1G to the predicted future 6G[44].

B. *Advancements in 5G Security*

While resolving several 4G weaknesses, 5G enhances security architecture and authentication procedures. Unified authentication is being used for the first time in 5G. All networks, including WiFi, cable, and 3GPP, are supported. When moving to a non-3GPP network, a 3GPP-authenticated UE can do so without having to reauthenticate[45]. Subscription Concealed Identifier (SUCI), an encrypted version of Subscription Permanent Identifier (SUPI), is used by 5G for authentication. So, IMSI and other unencrypted data will not be transmitted via 5G networks. The network is more secure because to this feature. It aids in approving interceptions as well. When a judge issues a request for evidence to gather information about a crime, operators may listen in on conversations for authorised law enforcement officials[21], [46]. The message structure and entity role, however, differ. EAP-TLS is specified by RFC 5216 for secure and encrypted Internet of Things (IoT) networks. Previously, laptops and other non-USIM IoT devices were unable to subscribe to or access the 5G core over EAP-TLS.

https://doi.org/10.31436/ijpcc.v10i2.478

The intricacy of 5G and its shortcomings make security issues[47]. AKA falls short of important 5G objectives. The channel that connects hosting and the home network, for instance, is unbounded. This vulnerability could be used by an attacker to charge someone else for access to the network. Even though 5G-AKA defeats IMSI-catcher assaults, users may still be monitored in 5G using synchronisation failure signals. Paging is advised by another study to locate people with less than ten calls. By tricking a UE into disclosing its SUPI, a fake pre-authentication message is sent[48].

C. *Advancements in Legacy Network Security*

Every network generation has its shortcomings. Although there are many ways to lessen exploitation, changing fundamental protocols is challenging, leaving substantial vulnerability. The supported services, features, and known security flaws in the preceding security architecture generations. The signalling DoS (denial of service), DDoS (dispersed denial of service) against authentication servers, energy depletion assaults, and user tracking are examples of attacks on 6G security architecture and applications. Poor authentication and resource limits, for instance, are problematic and affect all network generations. The key lessons from the difficulties and advancements in legacy network security are listed below:

- New applications typically have their security breached. In new applications, contemporary network standards perform better than more dated network standards. However, they could pose further dangers. Numerous research [49], [50] predicted that these new apps would be susceptible to DoS and impersonation assaults.
- Prior to implementation, technology security must be improved. Support for an outdated protocol by a modern one could reveal errors. The primary reason is the conflict between two network security standards.

By asking authentication for an obsolete architecture, compatibility is typically avoided. This kind of access management could make old problems obvious. Unwanted downgrades force 4G-LTE devices onto outdated networks. The attacker can then access the UE's IMSI due to the lack of mutual verification between the UE and authentication servers in 2G/3G standards. Identity management and dual network access authentication are security issues for 6G, it should be noted. More modifications to protocol implementations than to protocol designs help to improve vulnerability fixes while reducing new vulnerabilities.

- For subscriber identity management and AKA, significant equipment changes are required. A lot of operators and customers can suffer financially.
- Before deploying a new architectural or protocol design, extensive security testing is necessary. It is possible to update intrusion prevention systems or implement protocol security patches at endpoints.
- To address the shortcomings and vulnerabilities of the current architecture, a long-term design modification is still required.
- End-to-end encryption and mutual authentication are still open problems. False operators, eavesdropping, and tracing attacks result from the absence of these two characteristics. The enormous processing and transmission requirements of 5G make it unlikely that it will achieve these security requirements. In 6G, mutual authentication and encryption could harm latency-sensitive services.

III. 6G Network Vision and Essential Research Works

The criteria for the initial 6G supported projects are covered in this part along with its vision for the 6G safety structure.

A. *6G Network Vision*

6G networks can still benefit from 5G technologies like Multi-access Edge Computing (MEC), SDN, NFV, and network slicing. Therefore, safety concerns related to them remain. Threats on servers, hypervisors, and virtual network function (VNF) administrators are NFV security hurdles. Finally, because to the massively spread nature of 6G systems and physical dangers, DDoS, and MEC are all threats [51].

Possible network slicing attacks include information theft and denial-of-service attacks using 6G network slices. This network's capacity for attaining significant dynamicness and thorough automation of networking is exposed by threats against networking automation technology[52]. According to 6G, the Internet of Everything will eventually consist of billions of sophisticated connected gadgets. The device's SIM card-based main security is inappropriate for IoE deployment in 6G since 6G devices, like in-body sensors, will be smaller than older devices. In such a vast network, the necessary administration and distribution responsibilities are exceedingly ineffective. IoT devices with limited resources are a major target for attackers since they cannot ensure complex encryption. These tiny gadgets might be attacked using hacking techniques. Furthermore, the information gathered by the Internet of Everything to facilitate 6G applications raises privacy issues[53]. Privacy of information is harmed by data theft from Internet of Things (IoT) gadgets with restricted resources. Installations of local 5G networks tend to focus on specific industries including business, healthcare, and education. These little networks operate independently and connect to big networks[54].

https://doi.org/10.31436/ijpcc.v10i2.478

Many industries' enablers support 6G with varied embedded security levels compared to the networks of 5G. A vulnerable 6G network provides an opportunity for attackers to launch assaults. With the deployment of a high level of technology, 6G cells will shrink from a little to tiny. 6G is a network that is distributed and connected through a mesh has a higher risk of being attacked by malicious devices, increasing the potential for hazard. The massive number of devices inside each sub-network prevents the vast area network from offering security [55].

It would be better in 6G to have a multilayer safety framework (Seen in Figure 4) that recognises communication security at the sub-network level and sub-network to comprehensive area network security. The upper layer RAN services are centralised through convergence of the RAN and core functions, synchronising with dispersed core functions like User Plane Micro Services (UPMS) and Control Plane Micro Services (CPMS). Attackers may target UPMS and CPMS, which would have an effect on many radio units that use microservices. Zero-touch networking and Service Management (ZSM) architecture are features of 6G networks that provide quick services, minimal operational expenses, and reduced human error. In closed-loop systems, attacks might expand thanks to complete automation and self-learning. Due to stringent automation requirements with limited human interaction, data privacy protection in zero-touch networks is hard [56].

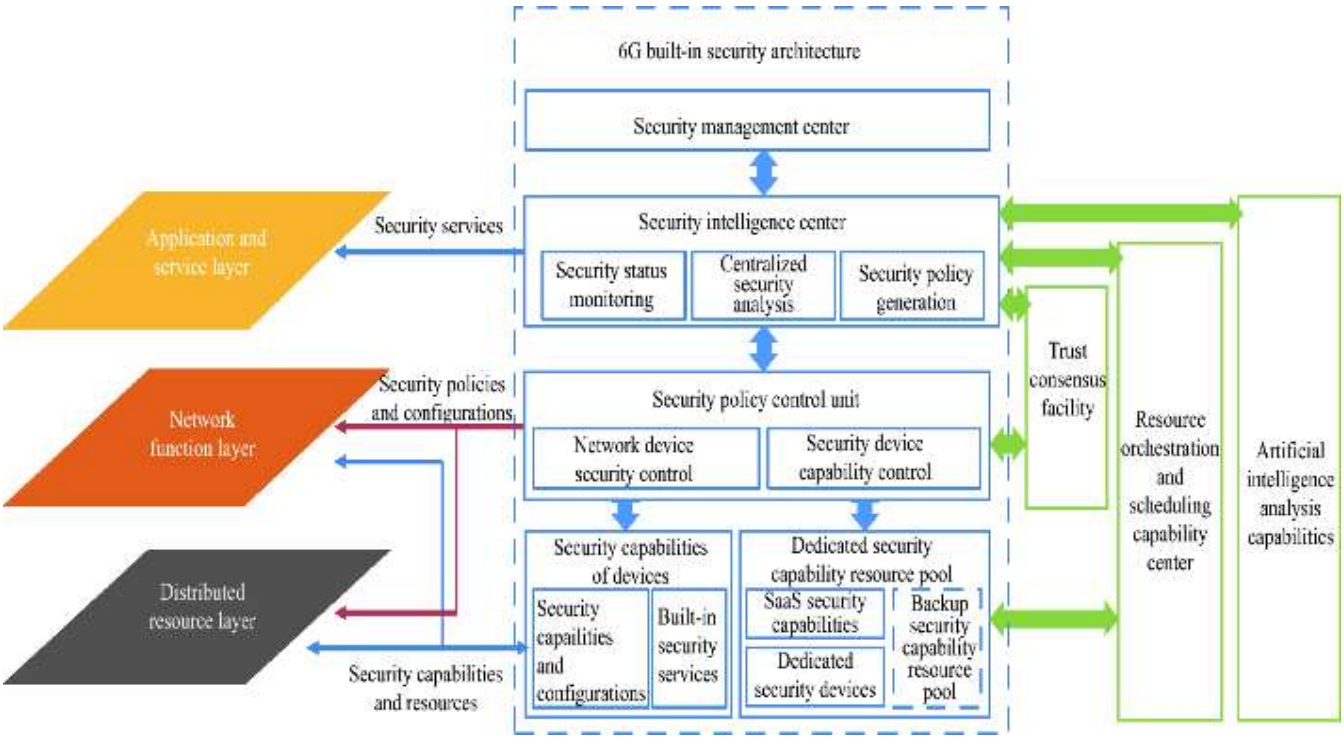

Fig. 4 The security evolution of mobile communications from 1G to the predicted future 6G[57]

B. *6G Essential Projects*

This section focuses on a handful of these trials and the lessons they have taught us about 6G security.

1) Hexa-x

The Hexa-x initiative was introduced by Ericsson in 2021. In this collaboration, various universities and research centres are collaborating to commercialise cutting-edge innovations. The foundation of the 6G networks is what the Hexa-x project wants to do. Additionally, it seeks to guide global research and innovation (R&I) into the following generation. The objective of this project is to enhance the tools required to bring 6G networks to Europe. Hexa-x will create many axes to concentrate on these difficulties[58]. To improve connection quality, new technologies like AI and ML must be used in human-device communication. The creation of a single network of networks is necessary for the global digital ecosystem. This network ought to be intelligent, versatile, and diversified. A sustainable network requires efficient resource exploitation. For the 6G network to offer worldwide and full coverage, viable and affordable solutions must be created[59]. The future generation should ensure data privacy, communication integrity,

https://doi.org/10.31436/ijpcc.v10i2.478

confidentiality, and operational resilience for high security. In order to improve the performance of 6G, further innovations will be developed, including network design, AI-driven air interface, and virtual network design. The project will focus on these ground-breaking communication technologies to improve communication between the human, digital, and physical worlds[60].

2) RISE 6G

One of the important initiatives beginning in 2021 is RISE 6G (Reconfigurable Intelligent Sustainable Environments for 6G wireless networks). Reconfigurable Intelligent Surfaces (RIS) technology is utilised in the project. In the future, RIS will grow to be one of the most potent emerging technologies. RIS works on the dynamic nature of controlling the radio propagation of waves. It enables the wireless environment to be seen as a service. By utilising RIS, enhancement of 6G features for a flexible, intelligent, and sustainable wireless ecosystem will be considered. Four RIS-related issues will be faced by the project[61]. First, the modelling of the real-time Remote Information System, RIS-assisted signal propagation is executed. Secondly, a significant number of Remote Information Systems (RISs) are expected to be integrated into the newly proposed network architecture. Third, a number of use cases will be developed to support quality of service (QoS), including vast capacity in a dynamic portable customizable environment, green communication, power consumption, and precise localization. Fourth, a prototype benchmark for innovation based on two complementing proceedings will be suggested. The initiative contributes to standardization and incorporates its technological vision into the use in industry[62], [63].

3) Next G Alliance

The Next G Alliance was introduced in the US by ATIS (Alliance for Telecommunications Industry Solutions) at the end of 2020. By implementing the fundamentals of 6G in North America, ATIS seeks to promote 6G leadership.
It focuses on the commercialization of technology, which includes R&D, manufacturing, standardisation, and market preparation[64]. The influence of member organisations on significant mobile communication players may be significant for future standards. The Next G Alliance will strategically look at commercial developments and standards. We aim to start a global conversation on standards and how to collaborate between business and government[65].

Mobile technology is essential to the expansion of many significant businesses. The United States depends more and more on a wide range of industries as mobile technology develops, including aerospace, agriculture, defence, education, healthcare, manufacturing, media, and transportation. In these crucial areas, North America has to keep up its position as the global leader in mobile technology[66].

IV. 6G Security Requirements and Proposed Security Architecture

A. *6G Security Architectures Requirements*

The security issue is a major concern for the 6G network, which is currently the subject of extensive study. Globally seamless connections to trillions of people, machines, and objects are expected to be made possible by 6G [67]. Many of these gadgets have weak security features and are easily exploitable for malicious purposes. At the same time, the widespread use of open-source software technologies introduces security risks brought on by software flaws. Even worse, since 6G is an open, integrated space-air-ground network, perimeter-based security measures like firewalls and intrusion detection systems (IDSs) may not provide adequate defense [68]. To meet the needs of 6G, it becomes necessary to construct more elastic security architectures. To convey this problem, the 6G security architecture must follow the basic security principle of ZT (Zero Trust). ZT is a security pattern that places the highest priority on safeguarding system resources. ZT predicts the possibility of an attacker residing on the network as well as the accessibility or unreliability of the network architecture from the outside [44]. The security requirements that the security architecture in the 6G networks must manage and handle are described in the lines that follow.

1) Virtualization Security Solution

In order to address virtualization security concerns, a system with a secure virtualization layer must be used. This layer must include security technology that can detect harmful software that is hidden, like rootkits. Additionally, using secure protocols such as VPN or SSH, the hypervisor must allow complete separation of storage, computing, and the network of various network services [69]. Cloud providers need a heavy detection system to monitor the Virtual Machine at hypervisor layer. Virtual Machine Introspection (VMI) is a technique to achieve the task at hand. There are many approaches proposed to fill in the hole, the biggest hurdle in applicability of VMI. The VMI identifies security threats by checking the IO files, virtual CPU register data of each virtual machine in order to stop intrusion [70].

2) Automated Management System (AMS)

When dealing with open source security issues, managing vulnerabilities brought on by the handling, updating, and discarding of open sources is of utmost importance. This makes an AMS that can find vulnerabilities and patches it for

quick detection of threats. By using secure the OTA technique and making sure that the software is installed securely in a fast matter, another step is necessary. Additionally, a security framework must be set up to deal with

- Deployment of security solutions
- Changes in developer perception
- Long-term open source vulnerability management [44].

3) Data Security using AI

AI systems must be transparent on the way they protect their users and the mobile communication system from Anti-Money Laundering (AML) if they are to guarantee that they are secure from AML. The first step in the process is to build reliable AI models. The AI models operating in radio access networks (RAN), user equipment (UE), and the core must also be checked to see if they have been maliciously updated or otherwise changed by an aggressive attack using a method like digital signatures. A system is required to carry out self-healing or recovery operations when a dangerous AI model is discovered. Additionally, the data collection should be gathered by the system for AI learning to reliable network components [71].

4) Protecting User's Privacy

The Internet provide sensitive information about people such as their lifestyle, demographic and personal information. Suitable information and data management attached to it are the main elements for the development of communication protocols that abide the user's privacy. Therefore, appropriate management of the information must be analysed from both parties of user's privacy and the information control perspective [72]. The 6G system anonymizes or reduces the amount of information that is made publicly available when it is used, keeping personal information secure and safe in a trusted execution environment (TEE) and reliable SW. Before MNO releases personal information, authenticity and authorization must be confirmed. When dealing with user information, an alternative is to use homomorphic encryption for the data to be accessed in an encrypted form. The user's location privacy and usage patterns may also be protected using AI-based solutions [44].

5) Post-Quantum Cryptography

The suggestion of quantum computing for public key cryptography promises to be a one-step-advancement technology when fully realized at scale. Unfortunately, quantum computing also makes it possible to develop a potent new tool for attacking the current cryptography algorithms, even though it introduces a completely new solution for solving complex computing problems. Because of this, it poses a serious threat to current Internet security. To simply put it, public key (asymmetric) cryptography depends on trapdoor mathematical functions that make it easy to calculate a public key from a private key but computationally impossible to calculate a private key from a public key (the inverse). The problem of integer factorization and elliptic curve variants of the discrete logarithm problem, both of which have no known solution for computing an inverse in polynomial time with conventional computing, are the foundations of widely used trapdoor functions [73].

B. *Proposed Security Architecture of 6G*

In this section, the current research being conducted on 6G technology is discussed. The rationale behind the recent modifications and adjustments made towards the implementation of 6G can be understood by examining the changes that have occurred in the three layers. The three main layers of computer communication systems are the physical layer, the network layer, and the application layer. 6G network architecture and design will have a lot of differences from 5G in many aspects. 6G may offer network automation and Network as a Service (NaaS) such as it allows subscribers to customize networks. Internet and information communications technologies (ICTs), robotics and artificial intelligence, neuroscience and cognitive technologies, nanotechnology, biotechnology, intent-based networking, end-to-end software, etc. are among the emerging technologies[52]. Next, the quick implementation of cloud-based networks and open-source software for core/RAN network architectures predicts the flexibility of 6G. It could be the first AI cellular system in entirety. This idea would change 5G's "connected things" into 6G's "connected intelligence," with AI supposedly controlling most of the network operations and nodes [74].

6G security architecture need to familiarized with new applications and integration of space-air-ground-sea integrated network. As seen in Figure 5, the recent 3GPP security architecture might need some big changes. Network operators will be a huge role in upgrading the network access and security design. The service providers provide services and platforms to developers and users. They will improve the application domain and the architecture security. 6G networks can improve the service security by offering many services such as mobile storage[75]. Lastly, users may be unaffected if any modifications or adjustment are made such as swapping to a new device or registering a new SIM card. 6G's security architecture can be split into layers to cover all of the security problems. Back to the 3 layers (physical, network, and application), each layer provides new security features

https://doi.org/10.31436/ijpcc.v10i2.478

that can upgrade and enhance the security of 6G[76]. Figure 5 shows the security improvements of the 6G's architecture.

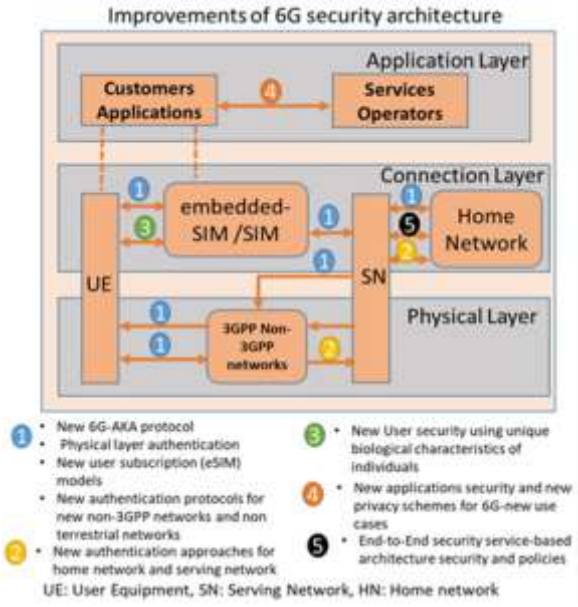

Fig. 5 The new improvements of 6G security architecture[44]

1) Network Access Security

6G needs new authentication and cryptography encryption systems such as quantum-safe cryptography. The need for cloud-based and open-source networking technologies promotes a new authentication so that 5G's security concept can be reused. There are a lot of new functionalities required to implement the system. For example, the authentication systems such as AUSF/SEAF would authenticate in cross-slice communications pattern. Physical layer security can protect IoT networks from threats and improve network access management.

2) Network Domain Security

A requirement will be made for a new open authentication methodology mainly as the factor of the connection of 6G to the space and sea are.

3) User Domain Security

Security authentication using password-less service to access is a top feature in the 6G's security architecture. There are a lot of applications relying on password type of security but evidently there are a lot of vulnerabilities. A few are easy to hack, costly, and difficult for sustainability. A more uniquely designed authentication on password-less method may be more secure in the future.

4) Application Domain Security

Operating 6G trust networks requires both parties to be authenticated. Symmetrical mutual authentication is still being used in 5G security but 6G may bring more advantages from blockchain and DLT.

5) Service-Based Architecture Security

While it's still being used in 5G, this feature towards a more advance level can be transferred. Maybe 6G will use end-to-end architecture or policy-based architecture domain security in all needs of enabling personalisation and flexibility meanwhile supporting a high-level security.

C. Specific Security Measures

Implementing robust security measures is crucial for the success of 6G and blockchain technologies. A detailed framework includes several key components.

1) Multi-Layered Security Approach

Employing advanced encryption techniques, secure authentication mechanisms, and continuous monitoring are vital to the security of 6G networks. Multi-layered security involves the integration of various protective measures across different levels of the network. For example, at the hardware level, Trusted Platform Modules (TPMs) can be used to ensure the integrity of the hardware components. At the software level, Secure Boot and software attestation can prevent unauthorized modifications [77].

AI-driven threat detection systems can identify and mitigate threats in real-time, enhancing the network's ability to respond to emerging threats dynamically. These systems use machine learning algorithms to analyze network traffic patterns and detect anomalies indicative of potential security breaches . Moreover, AI can be used to predict and preemptively block cyber-attacks by identifying suspicious activities before they escalate into full-blown attacks[56] .

2) Technologies

Quantum-resistant cryptographic methods should be adopted to safeguard against emerging threats posed by quantum computing, which has the potential to break traditional encryption methods. Post-quantum cryptographic algorithms, such as lattice-based, hash-based, and multivariate-quadratic-equations-based cryptography, are being developed to secure data against quantum attacks [78].

Blockchain technology can be leveraged to ensure data integrity and secure transactions within the network. By providing a decentralized ledger that is immutable and transparent, blockchain can enhance security in various 6G applications. For instance, blockchain can be used to secure IoT devices by providing a tamper-proof record of all interactions and transactions, thereby preventing unauthorized access and tampering[79] .

Additionally, integrating blockchain with smart contracts can automate security protocols, ensuring that they are executed precisely as programmed. This can be particularly useful in managing access controls and enforcing

https://doi.org/10.31436/ijpcc.v10i2.478

compliance with security policies without human intervention [46].

D. Best Practices:

Regular security audits are essential to identify and rectify vulnerabilities within the network. These audits should include penetration testing, code reviews, and compliance checks against established security standards such as ISO/IEC 27001 and NIST Cybersecurity Framework[80] .

Adherence to international security standards ensures that the security measures implemented are recognized globally and provide a benchmark for best practices. Standards such as the 3GPP security architecture for 5G can be extended and adapted for 6G to ensure consistency and reliability in security protocols[81] .

Comprehensive incident response plans are critical for quickly addressing and mitigating the impact of security breaches. These plans should outline clear procedures for detecting, analyzing, and responding to incidents, as well as for recovering from attacks and restoring normal operations[82]. Training and drills should be conducted regularly to ensure that all stakeholders are prepared to act swiftly and effectively in the event of a security incident[83] .

V. 6G Promising Technologies Security Challenges and Possible Attacks

Some technologies are evidently to be more efficient in a few sectors by using the 6G network as it has advanced high-level security, low latency reliability, and efficient communication services to 6G networks. However, most new 6G technologies have higher security and privacy vulnerabilities [84], [85].

A. *6G Physical Layer Technologies*

The physical layer serves as the basis for wireless communications, therefore securing it could prevent several common radio signal attacks like jamming and eavesdropping that affects the 6G applications. The idea behind physical layer security is to use wireless channel characteristics like noise and fading to increase confidentiality and carry out quick authentication. 6G affordable IoT devices to which sometimes lack the processing power to execute elaborate authentication techniques, would mainly benefit from the physical layer security's low complexity[86]. Physical layer security is strong against cryptanalysis, which has been the main issue of conventional cryptographic methods, in addition to depending on physical laws. Operator base stations and IoT gateways, as well as signal modulation methods, can implement physical layer security[87].

In 6G compatible networks, mmWave MIMO is still an essential physical layer technology. In mmWave MIMO networks, eavesdropping, jamming, and pilot contamination assaults (PCA) are the three typical attacks that are shown in Figure 6. Inferring and wiretapping unsecured wireless communications are used to eavesdrop. Security can be improved by beamforming technology in 6G mmWave MIMO networks[88].

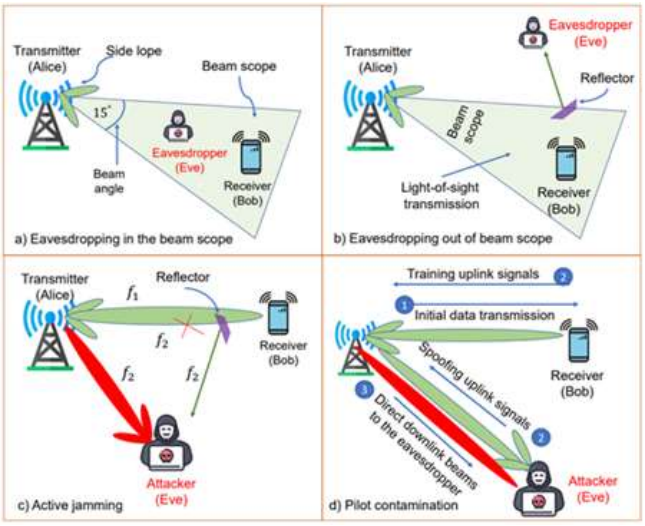

Fig. 6 Illustration of the methods to mitigate eavesdropping/jamming threats for 6G physical layer.

According to Figure 6, to wiretap the channel, from (Figure 6.a), an observer (Eve) must be in the beam scope or employ a reflector. The listener may be a trusted member of the network (internal; for example, an employee) or a third party (external). The eavesdropper can execute two further attacks just from the knowledge of the transmission signals (for example, the frequency f2) between Alice (Transmitter) and Bob (Receiver). In (Figure 6.c), a jamming attack is done, in which a jammer uses radio signals (on the same frequency as Bob's f2) to occupy a wireless channel that is shared with other users. An example of a DoS is when an aggressive injection restricts real users (like Bob) from using a wireless channel for communication.

The second method is called PCA, and it involves the attacker actively transmitting similar signals (spoofing uplink signals) to disrupt the transmitter's user detection and channel estimation phases. In the worst-case possible, the transmitter will send a part of the beam in the attacker's direction in the modified downlink direction, effectively degrading or causing signal leakage from the real user. PCA can affect multi-user and ultra-massive MIMO systems [89]. A cell-free massive MIMO system can also put itself at risk since radio stripes are exposed [90], making dense antennas easier to access during physical threats.

Recently, there has been a lot of focus in preventing the three mentioned attack methods. A primary strategy for preventing eavesdropping and PCA is, in essence, increasing

https://doi.org/10.31436/ijpcc.v10i2.478

signal range between the legal range over an eavesdropper's channels, or maximising the rate of secrecy[91]. The precoding procedure should be equipped with secrecy capacity maximisation as a key strategy of signal strength-based approaches, where the transmitter transmits to the receivers the information signals to the receivers in order to obtain channel state information, or prior knowledge about the communication channel. The most popular approach is to add more randomness to the modulation in order to make it more difficult for an observer to predict the transmitter's next signal sequence or frequency[92].

This approach is used in several current studies [89]. For instance, a research suggests a technique where the transmitter uses many random shifts in frequency or frequency hopping to avoid eavesdroppers. Another option is to generate encrypted communication keys using physical key generation which takes advantage of the entropy of uncertainty in channels like Channel State Information (CSI). To authenticate the broadcast against unreliable partners, [93] suggests an exchange of physical key between the transmitter and the authorised users. Even without the fear of internal attacks, incorporating the transformation (encrypt/decrypt) process into the precoding may be able to affect the operation of the multi-transmission. Although most approaches still have the drawback of high energy consumption, an emerging strategy is to leverage AI/ML techniques (for example, reinforcement learning [94]) to augment CSI knowledge and use effective defence mechanisms such as channel hopping. It should be mentioned that raising the secrecy rate might considerably minimise jamming attacks. Given that overloading all frequencies in modern broadband wireless channels is incredibly expensive, it is difficult for an attacker to attack and jam a communication channel successfully without learning specific information about comm signals between the transmitter and the authorised receiver. Attacking at a given frequency also has no effect on the overall performance of the receiver/transmitter due to the frequent frequency changes (frequency hopping).

Table 1 Comparison of security features across different network generations, from 1G to 6G.

Security Features	1G	2G	3G	4G	5G	6G
Authentication	No	Yes	Yes	Yes	Yes	Yes
Encryption	No	Yes	Yes	Yes	Yes	Yes
Privacy Protection	No	Yes	Yes	Yes	Yes	Yes
Transmission Protection	No	Yes	Yes	Yes	Yes	Yes
Network Security	Low	Moderate	High	High	High	High

In table 1, the security features across different network generations, from 1G to 6G, are evaluated based on authentication, encryption, privacy protection, transmission protection, and overall network security levels. The evolution of security features shows a significant enhancement from 1G to 6G networks, with 6G networks offering advanced security measures to address modern security challenges.

B. Obstacles and Constraints

To comprehensively address the potential challenges, the following obstacles and constraints need to be considered:

1) Technical Challenges:

As the number of connected devices increases, maintaining scalability without compromising performance will be a significant challenge[95]. The sheer volume of devices and the data they generate can overwhelm network resources, leading to congestion and decreased efficiency. Advanced network slicing and resource allocation techniques are required to manage these issues effectively[96].

Ensuring energy-efficient operations, particularly for IoT devices, is critical to sustainable development. Many IoT devices operate on limited battery power and need to function efficiently for extended periods. Techniques such as energy harvesting and efficient power management protocols can help address these concerns[97].

Achieving and maintaining low latency in highly dynamic environments will require innovative solutions. Applications such as autonomous driving and real-time remote surgeries demand near-instantaneous data transmission. Techniques like edge computing and advanced caching mechanisms can help reduce latency by processing data closer to the source[98] .

2) Regulatory Hurdles:

Navigating and complying with international regulations and data privacy laws can be complex and challenging. Different regions have varying standards and legal requirements that must be met to ensure data protection and privacy[99]. Comprehensive compliance frameworks and regular audits are necessary to address these challenges[100] .

Harmonizing standards across different regions to ensure seamless integration and interoperability is essential. The

lack of standardized protocols can hinder the global deployment of 6G and blockchain technologies. Collaborative efforts among international standardization bodies are crucial for achieving this harmonization[101] .

3) Cost Considerations:

The initial costs associated with deploying 6G and blockchain infrastructure can be prohibitive for many organizations. These costs include purchasing new hardware, upgrading existing systems, and training personnel. Financial incentives and funding initiatives can help mitigate these barriers.

Continuous maintenance and upgrades will require substantial financial resources. As technology evolves, regular updates and enhancements are necessary to keep the systems secure and efficient. Budgeting for these ongoing expenses is crucial for sustainable operations [102].

Evaluating the long-term ROI to justify the investments made is crucial for stakeholder buy-in. Organizations need to conduct thorough cost-benefit analyses to understand the potential financial returns from deploying 6G and blockchain technologies [103].

4) Interoperability Concerns:

Ensuring compatibility between new 6G/blockchain systems and existing legacy systems can be challenging. Legacy systems may not support the advanced features of new technologies, leading to integration issues. Developing interoperability protocols and middleware solutions can help bridge these gaps [104].

Developing strategies for seamless integration to provide a smooth transition and enhanced user experience is vital. This includes designing user-friendly interfaces and ensuring that the new systems are backward-compatible with existing technologies .

VI. IOT Blockchain Applications in Networking Systems: An Overview

When discussing the applications of Internet of Things (IoT) in networking systems, it is necessary to provide explanations for certain technical terms. IoT which stands for Internet of things refers to the concept of interoperability between multiple different devices with each other like a watch and phones communicating between each other [105]. Meanwhile for blockchain, it is a bit tricky since this term is used for a wide range of projects, ranging from cryptocurrency to IoT applications. The usefulness of blockchain is due to 3 key elements of it which are immutability, transparency and anonymity [106]. Blockchain is also closely related to bitcoin as blockchain is also used to record transaction without the need of intervention from third party [105].Computer networking system is a system where the 7 layer of open system interconnection (OSI) layer communicate between each other to generate output. Since IoT handles multiple communication between different devices, it might encounter a transaction operation. This is where blockchain can play its part, where can use blockchain to record the transaction data, optimize the performance, provide additional security and automated transactions [107]. Blockchain is not only involved in transactions, but also involved in security. In the modern world where technology, application and communication become super advanced, the security threat has also increased. Not to mention the vast collection of data being stored online pose an additional security threat. Blockchain ensures a significant benefit due to its decentralized, secure, intelligent, and efficient network operation [108].

Since blockchain does not require third person or intermediaries, it emphasizes on logical peer-to-peer(P2P) network, which is a direct communication between 2 organizations or individuals. This has resulted in the birth of P2P platforms for information sharing purposes [109]. The scary thing about blockchain is even though nowadays the functionality of it is nationwide and very useful, experts say that it is yet to reach its full potential, stating that it could get better and reach its peak in five years to come. Blockchain can be applied in ad hoc networks or cloud radio networks. Blockchain not only has been successfully integrated in IoT and security, but also has been in the sectors of healthcare systems, content-centric network, and reputation system. Blockchain systems can be applied in machine learning to tackle problems more effectively. There was a proposal to use blockchain to collect large amounts of sensing data as efficiently as possible to be used in machine learning so it can solve a problem automatically through end devices wirelessly. This blockchain system is called blockchain-based incentive mechanism.

Although blockchain seems to be so capable of many things, there are still challenges that need to be addressed. The challenges include resource management, big data processing, scalability and security and privacy. The issue of scalability presents a significant challenge as it necessitates accommodating both new and legacy systems to ensure seamless integration within a highly intricate system. There exist consensus protocols based on Byzantine Fault Tolerance (BFT), which aim to enhance efficiency. Additionally, Nakamoto's protocols enable consensus to be achieved in permissionless settings, wherein participation in the protocol is open to all individuals, allowing them to join or exit as desired. Nakamoto's protocols have the capability to mitigate security threats such as the sybil attack, wherein entities involved in information processing can be fraudulently replicated multiple times. A researcher has conducted a study on the security concerns associated with a blockchain-based approach. The study focuses on the

areas of authentication, confidentiality, privacy, and access control [110]. Blockchain can also prove to be useful in energy trading market since it can provide detailed data of transactive energy system. The integration of blockchain technology can be advantageous in the development of smart cities due to the anticipated increase in security threats. Consequently, the implementation of a blockchain system becomes essential to enhance security measures. When applied together with machine learning, we can use this combination in AI application where we handle vast amounts of data in the artificial intelligence using the sorting from blockchain.

Blockchain has been applied everywhere, including in network and communication, but it still has some weakness in this sector. As we advance further, the amount of transaction being done daily has caused issues in terms of scalability of the blockchain. Not only that, but every process of transaction also requires a huge amount of energy[111]. To counter this issue, we could increase block size, shading and pruning but this solution is not the absolute answer to our problem since they will also bring their own respective problem. Simply put, applying blockchain in network and communication requires too much amount of time and resources[112]. Another issue within this sector is privacy leakage since some layers of the blockchain is not fully protected. Although there is some issue with blockchain, it does not mean that it should be removed from the talking point completely. We've seen how useful it can be. It can hugely benefit machine learning since blockchain can store a vast amount of data securely, which is needed by machine learning since it will require lots of data to be analysed. The main feature of blockchain is the reason why some are willing to apply it in their system. The features include decentralization, transparency, immutability, security, auditability, autonomy, and pseudonymity[113].

Decentralization is a direct communication between two nodes without the need of intermediaries, where each transaction is generated and recorded without a central controller. Transparency is where transaction that occurred is completely transparent or can be seen by all nodes on public blockchain which makes blockchain more credible. Next is immutability, where once the transaction is done and recorded, is it irreversible, meaning no party can exploit and change the record of transaction for their own benefit. This is thanks to the cryptographic in the blockchain which made immutability possible. After that, have security, where all the transactions done will be checked, verified and even broadcasted and again, thanks to cryptography it is almost impossible to alter the distributed ledger in any way. Next is auditability, which allow nodes that has received permission to audit, trace and verify the transaction through the record stored. After that the autonomy, where each node receives or sends transactions independently without the need of third party or human intervention which most of the time could causes issues. Lastly is pseudonymity, where each node communicates with the pseudonymous address to avoid exposure, which provides high level privacy to users.

Considering the central theme of our discourse pertaining to the sixth generation of wireless technology (6G), it is crucial to examine the interrelationship between blockchain technology and the deployment of 6G. What is the influence of blockchain technology on the implementation of 6G? Can the effective utilization of blockchain technology contribute to the progress of 6G, or does it present potential obstacles to its implementation?[114] Blockchain can be implemented in 6G applications such as industrial application 4.0, seamless environment monitoring and security, smart healthcare, decentralized and trustworthy communication infrastructure and solutions. These are all possible implementations of blockchain in 6G application. It is possible due to the benefit that blockchain brings to 6G applications which are intelligent resources management, elevated security features and again, scalability[115]. Then again, there are still challenges that researchers need to overcome if to yield the 6G application's potential to its fullest. The challenges of having blockchain in 6G application includes massive connectivity to the system since the system becomes more complex, security requirement with scalability which will eventually require huge cost to keep the scalability, high data consumption of future tenants, device resource restriction and finally, interoperability and integration requirement between different device that wants to work together [116]. Even though there are still multiples challenges ahead, this work is worth a shot, since it could open a whole new path to more research opportunities in the future. As an example, work related to internet of things (IoT) will certainly require blockchain to manage data and transaction. Other works related to data storage and analytics will also need the concept of blockchain for data management purpose[117]. As previously stated, the integration of blockchain technology with machine learning has the potential to facilitate the progress of artificial intelligence. Furthermore, it could potentially prove advantageous in the realm of vehicle-to-vehicle communication. Lastly, unmanned aerial vehicles (UAVs) represent a pertinent technology within the domains of geoscience and remote sensing[118].

https://doi.org/10.31436/ijpcc.v10i2.478

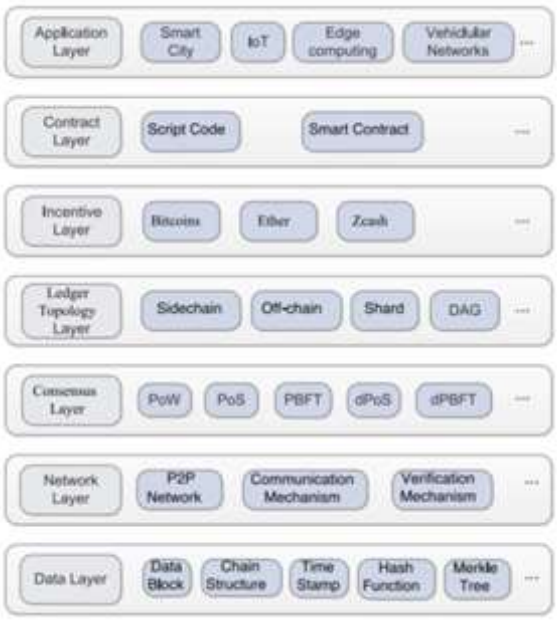

Fig. 7 General Architecture of blockchain

As seen in figure 7, this is the general architecture of blockchain which consists of 7 layers [108]. The data layer purpose is to store data that was generated during any transaction. The network layer uses peer to peer model which is a decentralized node to distribute the transaction. Next the consensus layer which contains consensus algorithms that makes decision whether to accept certain information from a fishy or suspicious party. There are many consensus protocols that exist nowadays, as example proof of work(PoW), Proof of Stake(PoS) and Proof of Authority(PoA) which is just a few examples out of many protocols that exist nowadays. Each of these consensus protocols is selected based on different scenario, meaning each of them has their own role and importance. PoW as an example, is proven to be successfully implemented in bitcoin since bitcoin require complex computational process. Subsequently, the following layer pertains to the incentivization mechanism, wherein the economic incentives are emphasised to ensure the maintenance of decentralisation among the nodes. Following this, there is the contract layer, which serves as the repository for all programme codes. These programme codes facilitate the execution of intricate business transactions. An instance of the contract layer can be observed in the form of a smart contract. The application layer, which is the final layer, is now discussed. The present stratum serves as the point of integration for all underlying strata, facilitating the development of a unified intelligent application. Consequently, the development of various applications, such as smart city initiatives, security systems, and edge computing, will be observed. The primary objective of implementing these applications within specific sectors is to enhance work efficiency. The utilization of big data and the sorting capabilities facilitated by blockchain technology enables these "smart" applications to operate at a significantly faster and more efficient pace. Just as the concept of networks encompasses various types, the realm of blockchain similarly encompasses multiple types. The first type of blockchain is known as a public blockchain, wherein users are not required to obtain permission in order to participate in the network or engage in transactions. This concept bears resemblance to the structure of the internet. The second type of blockchain is known as a private blockchain, which, as the name implies, requires permission to grant access exclusively to a select group of individuals, akin to an intranet. Finally, there exists a consortium blockchain, which refers to a blockchain that is managed and operated by a specific group of nodes that have been carefully chosen.

There exists a curiosity as to why a decentralized model such as blockchain is desired. Has the centralized model ever encountered any issues? Indeed, the response is affirmative. As time progresses, the proliferation of technological advancements in the world will inevitably lead to an increase in the number of devices. The proliferation of devices within a centralised model poses challenges to the management of data traffic within the network. The entirety of the data will ultimately need to traverse through a central point, assuming it is indeed centralised, which inherently exposes the central point to potential malicious attacks [69]. In the event of an attack on the central system, it is possible for the assailant to exert control over the transmitted data that traverses through the central system. The primary rationale behind the extensive research and emphasis on blockchain technology lies in its potential to address the shortcomings inherent in current technological frameworks and models.

The integration of blockchain with the Internet of Things (IoT) involves utilizing gateway devices as endpoints to the blockchain (Figure 8. a), IoT edge devices as transaction issuers to the blockchain (Figure 8. b), interconnected edge devices as endpoints to the blockchain (Figure 8. c), and implementing a hybrid cloud/blockchain approach (Figure 8. d)[119].

https://doi.org/10.31436/ijpcc.v10i2.478

consequently, has the potential to enable significant contributions in the form of feedback and

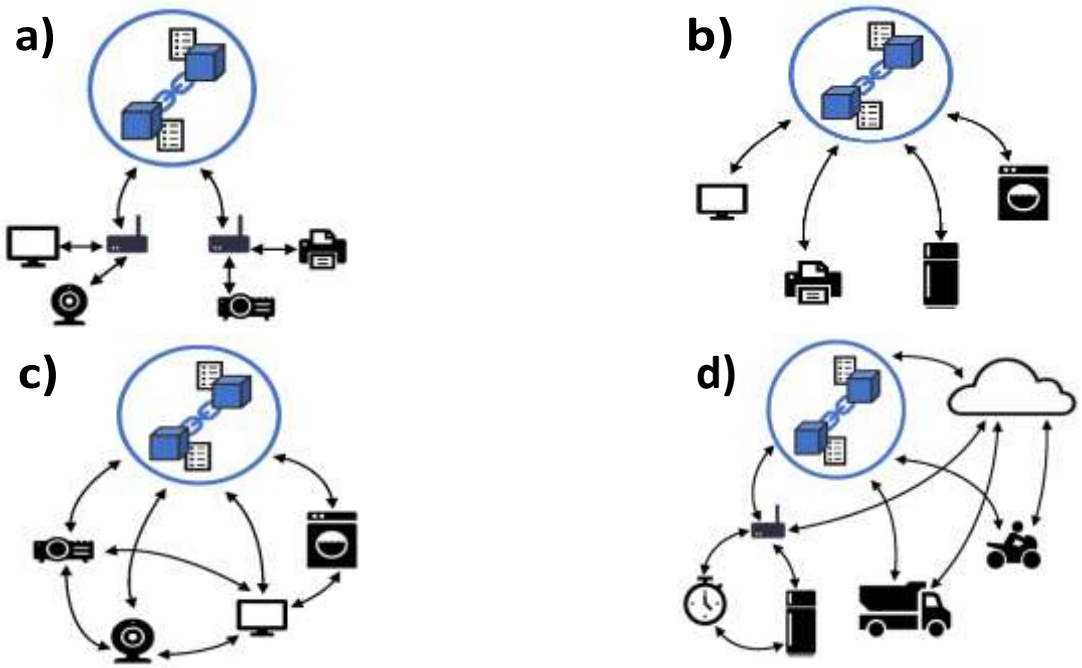

Fig. 8. A Gateway device as end-points to the blockchain, Fig. 8. b IoT edge devices as transaction issuers to the blockchain, Fig. 8.c Interconnected edge devices as end-points to the blockchain and Fig. 8.d A hybrid cloud/blockchain approach.

Gateway devices serve as the bridge between IoT devices and the blockchain network, facilitating secure data transfer and communication. IoT edge devices act as transaction initiators, enabling the seamless recording of IoT data on the blockchain for enhanced security and transparency. Interconnected edge devices establish a decentralized network endpoint, ensuring data integrity and reliability within the blockchain ecosystem. A hybrid cloud/blockchain approach combines the scalability of cloud computing with the security and immutability of blockchain technology, offering a robust framework for IoT data management and secure transactions.

VII. Conclusions

Considering the emerging status of the topics concerning 6G and blockchain, it is justifiable to propose an augmented allocation of funds towards educational endeavors, specifically training programs and workshops aimed at students and individuals interested in attaining a thorough comprehension of this field. Improving the general understanding of this topic is expected to enhance the effectiveness of 6G implementation, as it will cultivate a user base that possesses a thorough comprehension of the fundamental technological principles involved. This, recommendations for future progress. This undertaking could potentially facilitate a rise in the quantity of students who exhibit a keen interest in delving deeper into this discipline and aspire to attain a high level of proficiency in this technological domain. The country of Malaysia is currently facing a significant demand for a larger pool of professionals who possess extensive knowledge and expertise in the domain of 6G technology. The imperative stems from the need to bolster the nation's competitive advantage in comparison to prominent countries such as the United States and China. Furthermore, it is my contention that our government ought to allocate increased financial resources towards sectors affiliated with the development of 6G technology and blockchain. These technologies are anticipated to experience significant demand in the forthcoming 5 to 10 years. In the event of successful technological development, it is conceivable that we could assume the role of a supplier, thereby preserving our position as a leading entity in the production and research of blockchain and 6G. Both technologies have indeed been in existence; however, by harnessing the knowledge and skills of a larger group of experts and obtaining significant financial backing, we can improve the existing technology

and establish our supremacy as the leading nation in the fields of 6G and blockchain research.

This paper has examined the research on 6G and its associated security challenges and requirements. Ongoing research and innovation in the field of wireless networks continue to be pursued to enhance their integrity. The chronology of wireless generations, ranging from 1G to the most recent 6G, has been thoroughly examined in our discussions. The paper has presented a proposed security architecture for 6G and has recommended several security features for implementation within the system. Given the presence of security threats and risks across all layers, we have also examined the measures to counter potential attacks on the 6G network. The implementation of artificial intelligence (AI) technologies in the new 6G network aims to enhance both its structural components and security measures. The literature review for IoT Blockchain Applications in Networking Systems has also been discussed. The integration of IoT blockchain into networking systems has the potential to propel human progress, as blockchain technology emerges as a prominent force in the future. The integration of blockchain technology within networking systems can be observed as we delve into the fundamental aspects of blockchain architecture. Finally, we have discussed the proposal to foster innovation and actualize the development of 6G technology. Given the novelty of 6G and Blockchain, further investigation and scholarly inquiry are necessary to comprehensively understand and explore this subject matter. Consequently, it is imperative to cultivate awareness and enhance familiarity with 6G to facilitate its advancement. The study of 6G is of significant importance for future advancements, making it a crucial area of research.

ACKNOWLEDGMENT

This work is funded by the Ministry of Science and Technology the Malaysia, under of FRGS (FRGS/1/2023/TK07/UIAM/02/2). 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] A. Nasrallah *et al.*, "Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 88–145, 2019, doi: 10.1109/COMST.2018.2869350.

[2] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, Aug. 2020, doi: 10.1016/j.dcan.2020.07.003.

[3] A. Nieto, A. Acien, and G. Fernandez, "Crowdsourcing Analysis in 5G IoT: Cybersecurity Threats and Mitigation," *Mob. Netw. Appl.*, vol. 24, no. 3, pp. 881–889, Jun. 2019, doi: 10.1007/s11036-018-1146-4.

[4] H. Saarnisaari *et al.*, "A 6G White Paper on Connectivity for Remote Areas." arXiv, Apr. 30, 2020. doi: 10.48550/arXiv.2004.14699.

[5] P. P. Ray, "A perspective on 6G: Requirement, technology, enablers, challenges and future road map," *J. Syst. Archit.*, vol. 118, p. 102180, Sep. 2021, doi: 10.1016/j.sysarc.2021.102180.

[6] R. Agrawal, "Comparison of Different Mobile Wireless Technology (From 0G to 6G)," *ECS Trans.*, vol. 107, no. 1, p. 4799, Apr. 2022, doi: 10.1149/10701.4799ecst.

[7] P. K. Agyapong, M. Iwamura, D. Staehle, W. Kiess, and A. Benjebbour, "Design considerations for a 5G network architecture," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 65–75, Nov. 2014, doi: 10.1109/MCOM.2014.6957145.

[8] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015, doi: 10.1109/ACCESS.2015.2461602.

[9] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "Wireless Network Information Flow: A Deterministic Approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1872–1905, Apr. 2011, doi: 10.1109/TIT.2011.2110110.

[10] Z. Zhu *et al.*, "Secrecy Rate Optimization in Nonlinear Energy Harvesting Model-Based mmWave IoT Systems With SWIPT," *IEEE Syst. J.*, vol. 16, no. 4, pp. 5939–5949, Dec. 2022, doi: 10.1109/JSYST.2022.3147889.

[11] D. Sabella, A. Vaillant, P. Kuure, U. Rauschenbach, and F. Giust, "Mobile-Edge Computing Architecture: The role of MEC in the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 5, no. 4, pp. 84–91, Oct. 2016, doi: 10.1109/MCE.2016.2590118.

[12] "MEC Deployments in 4G and Evolution Towards 5G".

[13] L. M. Contreras *et al.*, "Hewlett Packard Enterprise".

[14] M. Patel, D. Sabella, N. Sprecher, and V. Young, "Contributor, Huawei, Vice Chair ETSI MEC ISG, Chair MEC IEG Working Group".

[15] J. Gante, L. Sousa, and G. Falcao, "Dethroning GPS: Low-Power Accurate 5G Positioning Systems Using Machine Learning," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, vol. 10, no. 2, pp. 240–252, Jun. 2020, doi: 10.1109/JETCAS.2020.2991024.

[16] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile Edge Computing: A Survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018, doi: 10.1109/JIOT.2017.2750180.

[17] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 616–621. doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.

[18] N. Kato, B. Mao, F. Tang, Y. Kawamoto, and J. Liu, "Ten Challenges in Advancing Machine Learning Technologies toward 6G," *IEEE Wirel. Commun.*, vol. 27, no. 3, pp. 96–103, Jun. 2020, doi: 10.1109/MWC.001.1900476.

[19] T. Aslanidis and L. Tsepenekas, "Message Routing in Wireless and Mobile Networks using TDMA Technology." arXiv, Jul. 03, 2016. doi: 10.48550/arXiv.1607.00604.

[20] B. Zhang, "Cryptanalysis of GSM Encryption in 2G/3G Networks Without Rainbow Tables," in *Advances in Cryptology – ASIACRYPT 2019*, S. D. Galbraith and S. Moriai, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019, pp. 428–456. doi: 10.1007/978-3-030-34618-8_15.

[21] S. F. Mjolsnes and R. F. Olimid, "Private Identification of Subscribers in Mobile Networks: Status and Challenges," *IEEE Commun. Mag.*, vol. 57, no. 9, pp. 138–144, Sep. 2019, doi: 10.1109/MCOM.2019.1800511.

[22] P. Gope and T. Hwang, "An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in

global mobility networks," *J. Netw. Comput. Appl.*, vol. 62, pp. 1–8, Feb. 2016, doi: 10.1016/j.jnca.2015.12.003.

[23] S. Faruque, "Time Division Multiple Access (TDMA)," in *Radio Frequency Multiple Access Techniques Made Easy*, in SpringerBriefs in Electrical and Computer Engineering. , Cham: Springer International Publishing, 2019, pp. 35–43. doi: 10.1007/978-3-319-91651-4_4.

[24] K. Cohn-Gordon, C. Cremers, L. Garratt, J. Millican, and K. Milner, "On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, in CCS '18. New York, NY, USA: Association for Computing Machinery, Oct. 2018, pp. 1802–1819. doi: 10.1145/3243734.3243747.

[25] N. Niebert *et al.*, "Ambient networks: an architecture for communication networks beyond 3G," *IEEE Wirel. Commun.*, vol. 11, no. 2, pp. 14–22, Apr. 2004, doi: 10.1109/MWC.2004.1295733.

[26] X. Liu, A. Sridharan, S. Machiraju, M. Seshadri, and H. Zang, "Experiences in a 3G network: interplay between the wireless channel and applications," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, in MobiCom '08. New York, NY, USA: Association for Computing Machinery, Sep. 2008, pp. 211–222. doi: 10.1145/1409944.1409969.

[27] S. Putz and R. Schmitz, "Secure interoperation between 2G and 3G mobile radio networks," pp. 28–32, Jan. 2000, doi: 10.1049/cp:20000007.

[28] C. B. Sankaran, "Network access security in next- generation 3GPP systems: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 84–91, Feb. 2009, doi: 10.1109/MCOM.2009.4785384.

[29] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Trans. Wirel. Commun.*, vol. 4, no. 2, pp. 734–742, Mar. 2005, doi: 10.1109/TWC.2004.842941.

[30] S. Frattasi, H. Fathi, F. H. P. Fitzek, R. Prasad, and M. D. Katz, "Defining 4G technology from the users perspective," *IEEE Netw.*, vol. 20, no. 1, pp. 35–41, Jan. 2006, doi: 10.1109/MNET.2006.1580917.

[31] H.-S. Liu, C.-H. Wang, and R.-I. Chang, "The design and implementation of a future Internet live TV system over 4G networks," *Telecommun. Syst.*, vol. 54, no. 3, pp. 203–214, Nov. 2013, doi: 10.1007/s11235-013-9728-8.

[32] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks," in *2007 IEEE Globecom Workshops*, Nov. 2007, pp. 1–6. doi: 10.1109/GLOCOMW.2007.4437813.

[33] A. Singla, S. R. Hussain, O. Chowdhury, E. Bertino, and N. Li, "Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks," *Proc. Priv. Enhancing Technol.*, vol. 2020, no. 1, Jan. 2020, doi: 10.2478/popets-2020-0008.

[34] M. A. Imran, Y. Abdulrahman Sambo, and Q. H. Abbasi, *enabling 5G Communication Systems to Support Vertical Industries*, 1st ed. Wiley, 2019. doi: 10.1002/9781119515579.

[35] T. Sato, "Modeling and Simulation on Securing of Software Defined Network Overlays," *Int. J. Intell. Inf. Syst.*, vol. 8, no. 4, p. 65, 2019, doi: 10.11648/j.ijiis.20190804.11.

[36] A. A. Ajani, V. K. Oduol, and Z. K. Adeyemo, "GPON and V-band mmWave in green backhaul solution for 5G ultra-dense network," *Int. J. Electr. Comput. Eng. IJECE*, vol. 11, no. 1, p. 390, Feb. 2021, doi: 10.11591/ijece.v11i1.pp390-401.

[37] D. P., M. Karuppiah, S. H. Islam, and M. S. Obaidat (Fellow Of Ieee And Fellow Of Scs), "Secure cognitive radio-based synchronized transmission of 5G signals using massive MIMO-OFDM-ES," *Int. J. Commun. Syst.*, vol. 31, no. 17, p. e3805, Nov. 2018, doi: 10.1002/dac.3805.

[38] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 3, pp. 1657–1681, 2017, doi: 10.1109/COMST.2017.2705720.

[39] S. Sridharan, "A Literature Review of Network Function Virtualization (NFV) in 5G Networks," *Int. J. Comput. Trends Technol.*, vol. 68, no. 10, pp. 49–55, Oct. 2020, doi: 10.14445/22312803/IJCTT-V68I10P109.

[40] S. A. Abdel Hakeem, A. A. Hady, and H. Kim, "5G-V2X: standardization, architecture, use cases, network-slicing, and edge-computing," *Wirel. Netw.*, vol. 26, no. 8, pp. 6015–6041, Nov. 2020, doi: 10.1007/s11276-020-02419-8.

[41] S. A. Abdel Hakeem, A. A. Hady, and H. Kim, "Current and future developments to improve 5G-NewRadio performance in vehicle-to-everything communications," *Telecommun. Syst.*, vol. 75, no. 3, pp. 331–353, Nov. 2020, doi: 10.1007/s11235-020-00704-7.

[42] W. Mazurczyk, P. Bisson, R. P. Jover, K. Nakao, and K. Cabaj, "Challenges and Novel Solutions for 5G Network Security, Privacy and Trust," *IEEE Wirel. Commun.*, vol. 27, no. 4, pp. 6–7, Aug. 2020, doi: 10.1109/MWC.2020.9170261.

[43] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, "A Survey on 5G Usage Scenarios and Traffic Models," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 905–929, 2020, doi: 10.1109/COMST.2020.2971781.

[44] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," *Sensors*, vol. 22, no. 5, p. 1969, Mar. 2022, doi: 10.3390/s22051969.

[45] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A Formal Analysis of 5G Authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Toronto Canada: ACM, Oct. 2018, pp. 1383–1396. doi: 10.1145/3243734.3243846.

[46] M. C. Chow and M. Ma, "A Secure Blockchain-Based Authentication and Key Agreement Scheme for 3GPP 5G Networks," *Sensors*, vol. 22, no. 12, p. 4525, Jun. 2022, doi: 10.3390/s22124525.

[47] A. C. Jiménez and J. P. Martínez, "Remote Patient Monitoring Systems with 5G Networks," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 6, no. 4, pp. 44–51, Jul. 2021, doi: 10.25046/aj060406.

[48] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols," *Proc. Priv. Enhancing Technol.*, vol. 2019, no. 3, pp. 108–127, Jul. 2019, doi: 10.2478/popets-2019-0039.

[49] H. H. Hussein, H. A. Elsayed, and S. M. Abd El-kader, "Intensive Benchmarking of D2D communication over 5G cellular networks: prototype, integrated features, challenges, and main applications," *Wirel. Netw.*, vol. 26, no. 5, pp. 3183–3202, Jul. 2020, doi: 10.1007/s11276-019-02131-2.

[50] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information," in *Proceedings 2019 Network and Distributed System Security Symposium*, San Diego, CA: Internet Society, 2019. doi: 10.14722/ndss.2019.23442.

[51] M. Pawlicki, M. Choraś, and R. Kozik, "Defending network intrusion detection systems against adversarial evasion attacks," *Future Gener. Comput. Syst.*, vol. 110, pp. 148–154, Sep. 2020, doi: 10.1016/j.future.2020.04.013.

[52] W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May 2020, doi: 10.1109/MNET.001.1900287.

[53] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The Roadmap to 6G Security and Privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[54] P. Padhi and F. Charrua-Santos, "6G Enabled Industrial Internet of Everything: Towards a Theoretical Framework," *Appl. Syst. Innov.*, vol. 4, no. 1, p. 11, Feb. 2021, doi: 10.3390/asi4010011.

[55] C. Benzaid and T. Taleb, "ZSM Security: Threat Surface and Best Practices," *IEEE Netw.*, vol. 34, no. 3, pp. 124–133, May 2020, doi: 10.1109/MNET.001.1900273.

[56] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G Networks: Use Cases and Technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, Mar. 2020, doi: 10.1109/MCOM.001.1900411.

[57] 粟栗, 庄小君, 杜海涛, 冉鹏, 黄晓婷, and 杨朋霖, "Built-in security framework research for 6G network," *Sci. Sin. Informationis*, vol. 52, no. 2, p. 205, Jan. 2022, doi: 10.1360/SSI-2021-0257.

[58] M. A. Uusitalo *et al.*, "Hexa-X The European 6G flagship project," Jun. 2021, doi: 10.5281/ZENODO.5070052.

[59] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening New Horizons for Integration of Comfort, Security, and Intelligence," *IEEE Wirel. Commun.*, vol. 27, no. 5, pp. 126–132, Oct. 2020, doi: 10.1109/MWC.001.1900516.

[60] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A Speculative Study on 6G," *IEEE Wirel. Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020, doi: 10.1109/MWC.001.1900488.

[61] W. Tang *et al.*, "Wireless Communications With Reconfigurable Intelligent Surface: Path Loss Modeling and Experimental Measurement," *IEEE Trans. Wirel. Commun.*, vol. 20, no. 1, pp. 421–439, Jan. 2021, doi: 10.1109/TWC.2020.3024887.

[62] S. Basharat, S. A. Hassan, H. Pervaiz, A. Mahmood, Z. Ding, and M. Gidlund, "Reconfigurable Intelligent Surfaces: Potentials, Applications, and Challenges for 6G Wireless Networks," *IEEE Wirel. Commun.*, vol. 28, no. 6, pp. 184–191, Dec. 2021, doi: 10.1109/MWC.011.2100016.

[63] D. Kitayama, Y. Hama, K. Goto, K. Miyachi, T. Motegi, and O. Kagaya, "Transparent dynamic metasurface for a visually unaffected reconfigurable intelligent surface: controlling transmission/reflection and making a window into an RF lens," *Opt. Express*, vol. 29, no. 18, p. 29292, Aug. 2021, doi: 10.1364/OE.435648.

[64] A. Dogra, R. K. Jha, and S. Jain, "A Survey on Beyond 5G Network With the Advent of 6G: Architecture and Emerging Technologies," *IEEE Access*, vol. 9, pp. 67512–67547, 2021, doi: 10.1109/ACCESS.2020.3031234.

[65] M. Z. Chowdhury, Md. Shahjalal, S. Ahmed, and Y. M. Jang, "6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, 2020, doi: 10.1109/OJCOMS.2020.3010270.

[66] E. C. Strinati *et al.*, "Reconfigurable, Intelligent, and Sustainable Wireless Environments for 6G Smart Connectivity," *IEEE Commun. Mag.*, vol. 59, no. 10, pp. 99–105, Oct. 2021, doi: 10.1109/MCOM.001.2100070.

[67] X. Fang, W. Feng, T. Wei, Y. Chen, N. Ge, and C.-X. Wang, "5G Embraces Satellites for 6G Ubiquitous IoT: Basic Models for Integrated Satellite Terrestrial Networks," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14399–14417, Sep. 2021, doi: 10.1109/JIOT.2021.3068596.

[68] D. Je, J. Jung, and S. Choi, "Toward 6G Security: Technology Trends, Threats, and Solutions," *IEEE Commun. Stand. Mag.*, vol. 5, no. 3, pp. 64–71, Sep. 2021, doi: 10.1109/MCOMSTD.011.2000065.

[69] A. Agache *et al.*, "Firecracker: Lightweight Virtualization for Serverless Applications," in *Proceedings of the 17th Usenix Conference on Networked Systems Design and Implementation*, in NSDI'20. USA: USENIX Association, 2020, pp. 419–434.

[70] B. Borisaniya and D. Patel, "Towards virtual machine introspection based security framework for cloud," *Sādhanā*, vol. 44, no. 2, p. 34, Feb. 2019, doi: 10.1007/s12046-018-1016-6.

[71] N. R. Sai, G. S. C. Kumar, M. A. Safali, and B. S. Chandana, "Detection System for the Network Data Security with a profound Deep learning approach," in *2021 6th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatre, India: IEEE, Jul. 2021, pp. 1026–1031. doi: 10.1109/ICCES51350.2021.9488967.

[72] S. Ribeiro-Navarrete, J. R. Saura, and D. Palacios-Marqués, "Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy," *Technol. Forecast. Soc. Change*, vol. 167, p. 120681, Jun. 2021, doi: 10.1016/j.techfore.2021.120681.

[73] D. Ott, C. Peikert, and other workshop participants, "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility," 2019, doi: 10.48550/ARXIV.1909.07353.

[74] J. T. J. Penttinen, "On 6G Visions and Requirements," *J. ICT Stand.*, Dec. 2021, doi: 10.13052/jicts2245-800X.931.

[75] K. B. Letaief, Y. Shi, J. Lu, and J. Lu, "Edge Artificial Intelligence for 6G: Vision, Enabling Technologies, and Applications," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 5–36, Jan. 2022, doi: 10.1109/JSAC.2021.3126076.

[76] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and Trust in the 6G Era," *IEEE Access*, vol. 9, pp. 142314–142327, 2021, doi: 10.1109/ACCESS.2021.3120143.

[77] P. Sonwane, V. Shirsath, H. Sharma, and G. Jain, "Failure Analysis of 30 Bus System by Capacitor Sizing and Placement," in *2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Dec. 2020, pp. 1–6. doi: 10.1109/ICRAIE51050.2020.9358282.

[78] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017, doi: 10.1038/nature23461.

[79] M. H. Miraz and M. Ali, "Applications of Blockchain Technology beyond Cryptocurrency," *Ann. Emerg. Technol. Comput.*, vol. 2, no. 1, pp. 1–6, Jan. 2018, doi: 10.33166/AETiC.2018.01.001.

[80] briasmitatms, "ISO/IEC 27001:2013 Information Security Management Standards - Microsoft Compliance." Accessed: Jun. 23, 2024. [Online]. Available: https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

[81] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[82] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains".

[83] R. H. Weber, "Internet of Things – New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010, doi: 10.1016/j.clsr.2009.11.008.

[84] R. P. Jover, "The current state of affairs in 5G security and the main remaining security challenges," 2019, doi: 10.48550/ARXIV.1904.08394.

[85] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The Road Towards 6G: A Comprehensive Survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 334–366, 2021, doi: 10.1109/OJCOMS.2021.3057679.

[86] W. Long, R. Chen, M. Moretti, W. Zhang, and J. Li, "A Promising Technology for 6G Wireless Networks: Intelligent Reflecting Surface," *J. Commun. Inf. Netw.*, vol. 6, no. 1, pp. 1–16, Mar. 2021, doi: 10.23919/JCIN.2021.9387701.

[87] S. Xu, C. Liu, H. Wang, M. Qian, and J. Li, "STAR-RIS-assisted scheme for enhancing physical layer security in NOMA systems," *IET Commun.*, vol. 16, no. 19, pp. 2328–2342, Dec. 2022, doi: 10.1049/cmu2.12486.

[88] Y. Yang, B. Zheng, S. Zhang, and R. Zhang, "Intelligent Reflecting Surface Meets OFDM: Protocol Design and Rate Maximization," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4522–4535, Jul. 2020, doi: 10.1109/TCOMM.2020.2981458.

[89] N. Wang, W. Li, A. Alipour-Fanid, L. Jiao, M. Dabaghchian, and K. Zeng, "Pilot Contamination Attack Detection for 5G MmWave Grant-Free IoT Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 658–670, 2021, doi: 10.1109/TIFS.2020.3017932.

[90] M. Ylianttila *et al.*, "6G White paper: Research challenges for Trust, Security and Privacy," 2020, doi: 10.48550/ARXIV.2004.11665.

[91] L. Bariah *et al.*, "A Prospective Look: Key Enabling Technologies, Applications and Open Research Topics in 6G Networks," *IEEE Access*, vol. 8, pp. 174792–174820, 2020, doi: 10.1109/ACCESS.2020.3019590.

[92] R. Alghamdi *et al.*, "Intelligent Surfaces for 6G Wireless Networks: A Survey of Optimization and Performance Analysis Techniques," *IEEE Access*, vol. 8, pp. 202795–202818, 2020, doi: 10.1109/ACCESS.2020.3031959.

[93] J. Tang, L. Chen, H. Wen, X. Xu, H. SONG, and K. Qin, "Physical layer secure communication against an eavesdropper with arbitrary number of eavesdropping antennas," US 11,483,704 B2 [Online]. Available: https://patents.google.com/patent/US11483704B2/en

[94] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA: IEEE, Jan. 2020, pp. 1010–1015. doi: 10.1109/CCWC47524.2020.9031175.

[95] W. Ejaz, M. Naeem, A. Shahid, A. Anpalagan, and M. Jo, "Efficient Energy Management for the Internet of Things in Smart Cities," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 84–91, Jan. 2017, doi: 10.1109/MCOM.2017.1600218CM.

[96] Y. Li, H. Lin, H. Huang, C. Chen, and H. Yang, "Analysis and Performance Evaluation of an Efficient Power-Fed Permanent Magnet Adjustable Speed Drive," *IEEE Trans. Ind. Electron.*, vol. 66, no. 1, pp. 784–794, Jan. 2019, doi: 10.1109/TIE.2018.2832018.

[97] N. Bandara, K. Gunawardane, and N. Kularatna, "Exprimental verification of Supercapacitor Assisted Sub Module Inverter (SCASMI) Technique," in *2020 2nd IEEE International Conference on Industrial Electronics for Sustainable Energy Systems (IESES)*, Sep. 2020, pp. 176–181. doi: 10.1109/IESES45645.2020.9210666.

[98] L. Zeng, Y. Wang, X. Fan, and C. Xu, "Raccoon: A Novel Network I/O Allocation Framework for Workload-Aware VM Scheduling in Virtual Environments," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 9, pp. 2651–2662, Sep. 2017, doi: 10.1109/TPDS.2017.2685386.

[99] E. Politou, A. Michota, E. Alepis, M. Pocs, and C. Patsakis, "Backups and the right to be forgotten in the GDPR: An uneasy relationship," *Comput. Law Secur. Rev.*, vol. 34, no. 6, pp. 1247–1257, Dec. 2018, doi: 10.1016/j.clsr.2018.08.006.

[100] A. Cavoukian, "Privacy by Design The 7 Foundational Principles".

[101] D. Marsh-Hunn, S. Trilles Oliver, A. González-Pérez, J. Torres-Sospedra, and J. F. Ramos, "A Comparative Study in the Standardization of IoT Devices Using Geospatial Web Standards," *IEEE Sens. J.*, vol. PP, Oct. 2020, doi: 10.1109/JSEN.2020.3031315.

[102] "Sustainability | Free Full-Text | Role of Digital Transformation for Achieving Sustainability: Mediated Role of Stakeholders, Key Capabilities, and Technology." Accessed: Jun. 24, 2024. [Online]. Available: https://www.mdpi.com/2071-1050/15/14/11221

[103] "Achieving ROI with Blockchain in the Enterprise: A Cost-Benefit Analysis." Accessed: Jun. 24, 2024. [Online]. Available: https://www.zeeve.io/blog/achieving-roi-with-blockchain-in-the-enterprise-a-cost-benefit-analysis/

[104] A. Al-Ansi, A. Al-Ansi, A. Muthanna, and A. Koucheryavy, "Blockchain technology integration in service migration to 6G communication networks: a comprehensive review," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 34, pp. 1654–1664, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1654-1664.

[105] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet Things*, vol. 10, p. 100081, Jun. 2020, doi: 10.1016/j.iot.2019.100081.

[106] L. Ghiro *et al.*, "What is a Blockchain? A Definition to Clarify the Role of the Blockchain in the Internet of Things." arXiv, Feb. 07, 2021. Accessed: Sep. 01, 2023. [Online]. Available: http://arxiv.org/abs/2102.03750

[107] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–32, Jan. 2021, doi: 10.1145/3372136.

[108] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and Machine Learning for Communications and Networking Systems," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1392–1431, 2020, doi: 10.1109/COMST.2020.2975911.

[109] Z. Ding, S. Liu, M. Li, Z. Lian, and H. Xu, "A Blockchain-Enabled Multiple Object Tracking for Unmanned System With Deep Hash Appearance Feature," *IEEE Access*, vol. 9, pp. 1116–1123, 2021, doi: 10.1109/ACCESS.2020.3046243.

[110] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.

[111] B. Cao *et al.*, "Blockchain Systems, Technologies, and Applications: A Methodology Perspective," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 1, pp. 353–385, 2023, doi: 10.1109/COMST.2022.3204702.

[112] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in Blockchains," *IEEE Access*, vol. 8, pp. 14155–14181, 2020, doi: 10.1109/ACCESS.2020.2965147.

[113] H. Jebamikyous, M. Li, Y. Suhas, and R. Kashef, "Leveraging machine learning and blockchain in E-commerce and beyond: benefits, models, and application," *Discov. Artif. Intell.*, vol. 3, no. 1, p. 3, Jan. 2023, doi: 10.1007/s44163-022-00046-0.

[114] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019, doi: 10.3390/s19020326.

[115] H. Srikanth Kamath, A. Bhandari, S. Shekhar, and S. Ghosh, "A Survey on Enabling Technologies and Recent Advancements in 6G Communication," *J. Phys. Conf. Ser.*, vol. 2466, no. 1, p. 012005, Mar. 2023, doi: 10.1088/1742-6596/2466/1/012005.

[116] T. Hewa, G. Gur, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, Levi, Finland: IEEE, Mar. 2020, pp. 1–5. doi: 10.1109/6GSUMMIT49458.2020.9083784.

[117] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: a new paradigm towards 6G," *Natl. Sci. Rev.*, vol. 8, no. 9, p. nwab069, Sep. 2021, doi: 10.1093/nsr/nwab069.

[118] T. Noreen, Q. Xia, and M. Zeeshan Haider, "Advanced DAG-Based Ranking (ADR) Protocol for Blockchain Scalability," *Comput. Mater. Contin.*, vol. 75, no. 2, pp. 2593–2613, 2023, doi: 10.32604/cmc.2023.036139.

[119] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 2, pp. 1676–1717, 2019, doi: 10.1109/COMST.2018.2886932.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.484

Analyzing Threat Level of the Backdoor Attack Method for an Organization's Operation

Muhammad Zafran Syahmi Mohd Nasharuddin, Adamu Abubakar*
Dept. of Computer Science, KICT, International Islamic University Malaysia, 53100 Kuala Lumpur, Malaysia.

*Corresponding author: adamu@iium.edu.my
(Received: 4th June 2024; Accepted: 25th June 2024; Published on-line: 30th July 2024)

Abstract— Backdoor attacks played a critical part in the catastrophe, as well as the overall impact of cyberattacks. Backdoor assaults are additionally influencing the landscape of malware and threats, forcing companies to concentrate more on detecting and establishing vulnerability tactics in order to avoid hostile backdoor threats. Despite advances in cybersecurity systems, backdoor assaults remain a source of concern because of their propensity to remain undetected long after the attack vector has been started. This research is aimed to examine the threats of backdoor attack methods in an organization's operational network, provide a full-scale review, and serve as direction for training and defensive measures. The fundamental inspiration was drawn from the alarming and involving threat in cybersecurity, which necessitates a better awareness of the level of risk and the concurrent requirement for increased security measures. Most traditional security solutions usually fail to detect harmful backdoors due to the stealthy nature of backdoor code within the system, necessitating a unique approach to full-scale threat analysis. A multi-phase approach that begins with considerable reading and examination of existing literature to get insight into typical backdoor attack methodologies and application methods. Following analysis, testing was carried out in a virtual lab in a controlled environment because thorough malware analysis testing must adhere to ethical and legal cyber testing laws to avoid any penalties or foolish breaches. This methodology also included testing on numerous attack channels combined with backdoor attacks, such as detecting software vulnerabilities, phishing emails, and direct payload injection, to determine the complexity of the different attack vectors. Each of the collected data is utilized to create a threat model that predicts the amount of risk associated with the backdoor attack approach. The finding contributes to the development of more resilient defence mechanisms, while also strengthening the overall organization's security architecture and protocols.

Keywords— Cybersecurity, Backdoor attack, Malware, Jitter, Direct payload injection

I. INTRODUCTION

In this modernization century, current technologies are heavily relied on efficiency, innovation, and competitive benefits for either the enterprise or the individual. However, when it comes to security issues in computing, modernization generates an entry point and significant vulnerabilities in computing system. Specifically, a security system that can exploit any weakness in system. One such issue is a "backdoor attack". This is a scenario where in system code that was implemented or existed during the implementation process can be potentially exploited [1]. The backdoor attack provides one of the most serious forms of infiltration because it could supply multiple attack paths from a single entry point. That is why, a backdoor attack is an approach of introducing a vulnerability in the system that allows other types of malicious attacks to enter or acquire unauthorized access to the system silently [2]. The backdoor's invisibility allows the attacker to move undetected by the detection system while targeting the victims and jeopardizing the confidentiality, integrity, and availability of the organization's operational systems and services, in particular.

The primary goal of this research is to offer a thorough analysis of the cyber threat level posed by the backdoor payload. The attack's developments and innovations complicate backdoor malicious attacks, making it more difficult for security measures in the business to keep up with the latest and sophisticated attacks in order to avoid disruptions in network system services. The fact that a backdoor is a means of breaking into a system by exploiting an existing or future implementation of malware to gain unauthorized access. This means that backdoors can easily bypass traditional security protections and authentication procedures due to their discrete character and ability to remain hidden in the absence of appropriate security monitoring or assessment [3]. The problem comes when a user's conducts a security evaluation but unable to finds

backdoor codes since they are hiding in the system. Even if current security measures have improved, backdoor attacks remain a significant issue. The fundamental reason advanced security technology cannot deal with current cyber threats is a lack of knowledge in security defensive measures, which makes them difficult to implement a proper degree of defence comply with the attacks [4].

In general, majority of backdoor research focuses on evaluating malware analysis to identify between different levels of a backdoor attack in order to correctly strategy mitigation and security assessments [5]. Most existing security mechanisms frequently fail to detect the backdoor due to its ability to move silently throughout network networks, leaving the organization's system open to unauthorized access and possible exploit. Extensive testing and analysis of the threat level of a backdoor attack were carried out to provide a comprehensive risk assessment, a mitigation strategy, and insightful knowledge about the particular attack to improve the organization's framework and defensive measures [6]. Other issues encountered were the integration of new technologies such as multi-source transfer learning, machine learning, and artificial intelligence into the current system, which made it more vulnerable and created a lot of new loopholes in the system, requiring more advanced and up-to-date information about current cyber-attacks [7].

The final motivation of this study lies within "Attackers framework". It was determined that there were frequently among the internal workforce, as it is quite easy to compromise critical data and spy on the organization's network [1]. Considering that backdoor attack allows the attacker to conduct a threatening attack by exploiting software vulnerabilities or transmitting a malicious payload and easily manipulating system information [8]. This significantly increases the frequency of cyberattacks, particularly within the corporation.

In light of the present circumstances, it is imperative for companies to carry out security evaluations and testing in order to identify any abnormal or detrimental activity. In order to carry out a comprehensive examination, it is crucial to have access to rules that ensure adherence to corporate standards and the complete utilisation of defence and prevention systems. This research is valuable because it offers extensive guidance and understanding of the seriousness of backdoor attack approaches. This enables the adoption of appropriate preventive and security measures. Hence, this ongoing investigation is of utmost importance.

The remaining sections of this work is organized as follows: Section 2 discuss the related work, Section 3 provide the research methodology, and Section 4 presented the analysis and results. Section 5 discuss the conclusions of the study.

II. Literature Review

There are many previous research studies on backdoor attacks. Crucial to these is the work of Hashemi and Zarei [9] which purpose to investigate backdoor attacks in Internet of Things (IoT) environments, with a particular focus on issues of resource management and security. A number of different detection methods and recommendations for improving the security of Internet of Things devices against backdoor attacks has been presented in the paper. Finally, the paper concluded that vulnerabilities that are associated with Internet of Things systems that need security solutions.

Qiu et al. [10] presents "Deepsweep," a framework specifically developed to counteract backdoor attack on deep neural networks (DNNs) by employing data augmentation techniques. The paper illustrates that through the diversification of the training data, Deepsweep can significantly diminish the success rate of backdoor attacks, hence bolstering the resilience of DNNs against these types of threats.

Liu et al. [11] examine backdoor attack that utilise the process of machine unlearning, a technique designed to exclude specific input from models. The paper demonstrates the ability of intentionally designed unlearning requests to introduce backdoors into the model. Finally, the study advocates for the implementation of stronger unlearning techniques in order to mitigate these weaknesses.

Chen et al. [12] research presents a technique for identifying backdoor attacks on DNN by utilising activation clustering. The approach detects clusters that exhibit abnormal behaviour by analysing the activations of neurons in response to inputs, hence identifying potential backdoor attacks. The efficacy of the technique is demonstrated in several attack scenarios, offering a means to detect corrupted models.

Al Kader et al. [13] research investigates the phenomenon of backdoor attacks on video action recognition systems. The method presents a new approach to launching attacks by utilising both visual and audio signals to embed and activate backdoors concurrently. The results emphasise the necessity for implementing more extensive safeguards in multimodal video action recognition systems.

Dong et al. [14] work introduces a technique for identifying backdoor attack using a black-box approach, even when there is a scarcity of information and data available. The paper utilises an innovative testing approach to detect anomalous model behaviours that suggest the presence of backdoors. The approach exhibits resilience and

https://doi.org/10.31436/ijpcc.v10i2.484

efficacy, even in the absence of knowledge regarding the attack specifics and model structure.

Wan et al. [15] examines the occurrence of data and model poisoning backdoor attacks in wireless federated learning. The findings identify crucial obstacles and suggests future research paths to enhance the security of wireless federated learning systems.

Goldblum et al. [16] provides a thorough examination of dataset security in the context of machine learning, with a specific emphasis on the topics of data poisoning and backdoor attacks. The paper classifies different attack techniques and defence mechanisms, highlighting the significance of safe data management practices. The paper put out recommendations for improving the security of datasets and reducing possible risks.

Nguyen et al. [17] introduces a method for executing irreversible backdoor attacks in federated learning settings. Unlike conventional backdoors that may be perhaps reduced or eliminated, the proposed system guarantees the persistence of the backdoor even after substantial model changes and retraining, thereby presenting a considerable risk to the security of federated learning.

The evaluated publications collectively examine several aspects of backdoor attacks in machine learning models, with a particular emphasis on deep neural networks (DNNs) and other advanced architectures like vision transformers and LSTMs. The approaches presented aim to identify and reduce the impact of backdoor attacks through techniques such as data augmentation, activation clustering, and black-box testing. Thorough surveys and evaluations emphasise the difficulties in ensuring the security of datasets, the risks associated with backdoor learning, and the vulnerabilities present in IoT contexts. These findings underscore the importance of implementing strong defence mechanisms. The papers also explore innovative attack techniques such as switchable backdoors and irreversible backdoor attacks in federated learning, demonstrating the dynamic nature of risks and the significance of adaptable security mechanisms.

Although there have been significant improvements, there are still some areas of research that have not been fully explored. First and foremost, there is a requirement for stronger and more scalable defence systems that can adjust to different methods of assault and model structures. Existing techniques frequently depend on particular assumptions or restricted data, hence diminishing their capacity for generalisation. Moreover, the interaction between various forms of attacks, such as data poisoning and backdoor attacks, has not been well investigated, hence neglecting possible vulnerabilities. Further work is needed to understand the impact of backdoor assaults on new technologies, such multimodal learning and IoT systems. Furthermore, there is a deficiency in the establishment of standardised evaluation frameworks and standards to measure the efficiency of defence methods.

Future research should prioritise the development of comprehensive defence frameworks that incorporate various detection and mitigation strategies, hence improving their resilience and scalability. Investigating the interconnections between various forms of attacks and defences could yield a more holistic comprehension of security weaknesses. Researchers should give priority to developing standardised benchmarks and evaluation criteria to simplify the comparison and enhancement of defence mechanisms. Examining the consequences of backdoor assaults on emerging technologies like edge computing and quantum machine learning can reveal innovative risks and countermeasures. Furthermore, the development of more sophisticated methods for securely managing data and protecting privacy in federated and distributed learning settings will be essential in addressing the changing nature of backdoor attacks.

III. Research Methodology

In the methodology section, a proper assessment and penetration testing were performed on the level of effect of a backdoor attack on organization network system administration. This test is necessary to analyse the behaviour of the backdoor payload to estimate the degree of threat posed by the backdoor. This methodology outlines a step-by-step approach to properly conducting penetration testing on advanced backdoor attacks, particularly on organization operations utilizing the Kali Linux penetration operating system. The algorithms employed in this methodology are replications of actual cyber-attacks. The testing will help an organization to understand the backdoor attack mechanism, and a comprehensive insight to prepare for cyber-attacks and system exploitation.

First, due to the risk of handling the backdoor during malware analysis, a proper virtual lab is required during the environment setting-up phases. The virtual environment allows the tester to be more flexible and independent during the penetration testing because the virtual machine is a separate network environment, so it will not affect the local machine or network system from any unintended breach or unexpected attack from the malicious software. then create the representation of organization network architecture to be able to assess the backdoor attack and analyse the level of the attack vector and also to look out if there is the possibility of system vulnerabilities that might occur. This allows for a close comparison of the findings to real-world attack scenarios.

A. Architectural Framework

The architectural framework of this current study lies with the general computer network security issues. For the

https://doi.org/10.31436/ijpcc.v10i2.484

purpose of this specific research, the architectural framework is based on a traditional network environment. Consequently, the architecture that has been suggested is shown in Figure 1. What follows is a condensed version of it: An attack that occurs outside of the network, which is the presence of the attacker, is characterised by the attacker's ability to rely on an open port, where it searches for and eventually locates one. By the "listening port" is where you will find acquire.

Following the acquisition of knowledge regarding both the opening and listening port, the attacker proceeded to create a connection of its own. It is possible that the connection is with a "Internet of Things device," a "control server," or a "Network that remain undetectable" in the system, but this cannot be determined without doing an inspection. In both of these open instances, the attacker has the potential to get root privileges of the control server as well as remote access to the "Internet of Things device." When taking into consideration the scenarios that have been provided thus far, the most important and core aspect of the backdoor attack is the capability to enter the network zones without going via the door that is expected, despite the fact that it is not permitted to go through the door that everyone is familiar with. The term "Backdoor" refers to the fact that attackers have the potential to establish another door, which is why it is an attack mechanism. In light of this, the purpose of this research is to investigate the potential backdoor that the attackers utilised, as well as to assess the possibilities of accessing these doors and the ways in which they might be presented.

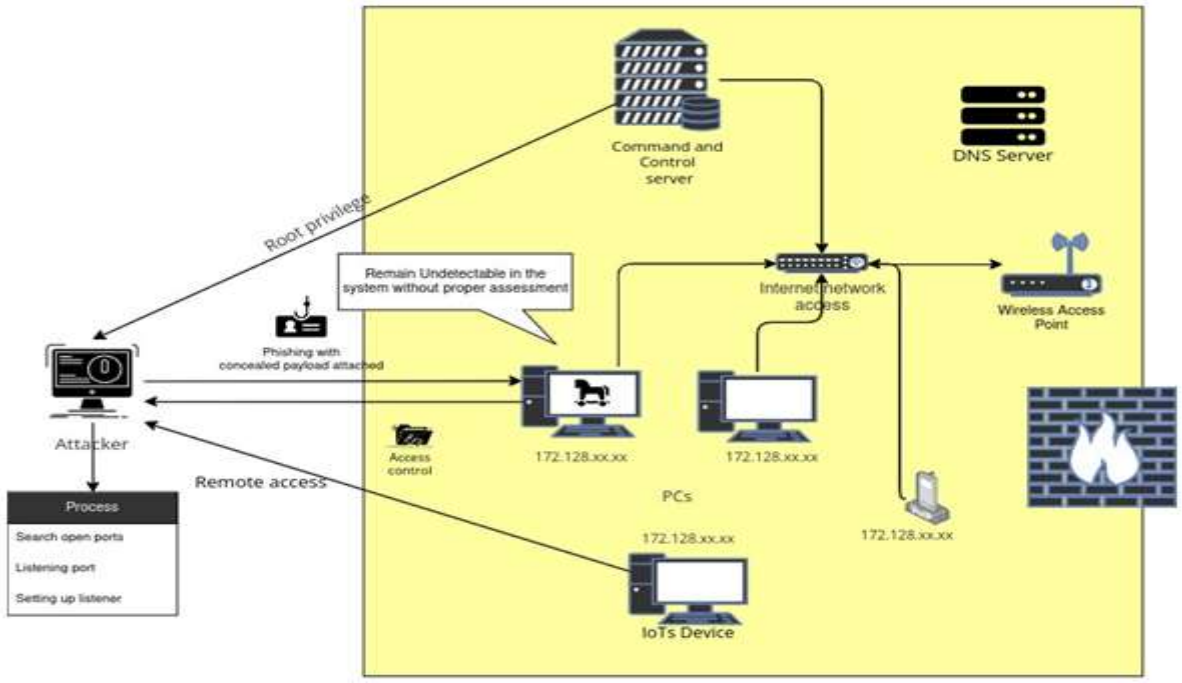

Fig. 1 The Research Architectural Framework

B. Experimental Simulation

The experimental simulation focuses on accurately created simulation approaches to estimate the threat level of backdoor attacks. This technique was implemented in a controlled environment, where all possible scenarios were thoroughly analysed and experimented with. In order to guarantee the effectiveness of the methodological approach, it is crucial to include the requirement for testing. The simulation requirement includes the necessary system specifications for evaluating the extent of the backdoor attack approach. The "Attack Simulation on the Kali Linux" was conducted with the "Metasploit Framework" serving as the listener and for deploying the backdoor. The simulation framework includes Test Servers that utilise a "Kali Linux" operating system, which is installed on a virtual machine. The "msfvenom" tool is employed to generate payloads, while specialised Python scripts were created to target certain attack situations and targets.

An experimental setup was created using a network environment that replicated the organization's network architecture and important systems. A test environment was employed within the Virtual Machine to guarantee the isolation of the network from the production network, thereby avoiding any unwanted repercussions. A strategic plan for launching an assault and a technique for delivering

https://doi.org/10.31436/ijpcc.v10i2.484

hidden malicious software using msfvenom were devised in response to the given circumstances. The covert malicious software was successfully executed. Execution and monitoring are responsible for initiating the connection session between the system and the target in order to get access. After obtaining access, an assault was initiated utilising the Metasploit framework. A thorough examination and assessment of the functionalities of the backdoor, together with the system's.

After clearly outlining the simulation objective, the testing then began with building an isolated environment by configuring the virtual system to minimize any unwanted breaches and effects while also ensuring a safe testing environment.

Then, mimic the organization's network system architecture for exploitation testing. In this situation, the research will use Kali Linux technologies such as msfvenom, metasploit framework, custom Python script, veil framework, and MulVal. The purpose of msfvenom is to construct a backdoor payload containing malicious code that will be sent to the target machine.

While the use of the Metasploit framework is to listen to the victim's machine via a connected backdoor payload that was delivered, the Python script used was to construct a specific malware payload to exploit the specific target within the system. Other than analysing the capability of the monitoring tools to detect backdoor payloads, detecting any intrusion within the system is critical when utilizing the Windows Defender system.

Next, create possible scenarios for the simulation that closely reflect the actual cyberattack.

- Scenario 1: Phishing attack using the delivery emails method
- Scenario 2: Search for any vulnerabilities in outdated software
- Scenario 3: Manually installing backdoor payload in the victim's machine

Further the simulation process by defining the entry point of each scenario above to completely compromise the system and gain full control to enable the remote access control. after the acknowledgment of the entry point, then by using the created payload to deliver to the target system. After delivery is successful, establish the session to connect the victim's machine via the delivered backdoor. The attack can only be delivered if the backdoor is triggered even after the session is established. Select the attack vector method offered by the Metasploit framework, for example accessing command prompt, network monitoring, activity logs and control remotely, then observe the system activity and the interaction between backdoor and detection system. Is the backdoor visible by the intrusion detection system even after launching an attack?

Following the penetration, to avoid leaving a visible footprint or traceable artifact, clean the activity by ending the session and erase all the data artifacts and residual malware to remain hidden in the system. Collect all the information gained and start analyzing the capability of the backdoor payload and detection system towards the integration of the current security technologies. Document all the findings, including timestamp, simulation process, backdoor, and detection system capabilities. All the insight collected can be used for training, assessing software vulnerability, and estimating the degree of threat related to backdoor attacks. To ensure the effectiveness of the testing, schedule the continuous testing within the organization to effectively respond to the attack, and strategize the mitigation plans.

C. Experimental Setup

The experiment setup for this research is presented in Figure 2. The flowchart provides an overview of all of the procedures that are involved in the experimental scenarios. It also illustrates how a traditional backdoor functions by utilising particular tools such as Msfvenom and the Metasploit framework. In order to gain a deeper comprehension of the manner in which backdoor attack operate in a variety of contexts, the experimental scenarios were designed for that. Furthermore, the purpose of this experiment was to repeat the various attack scenarios that were discussed before, as well as to investigate how the backdoor evolved within the context of the incorporation of new technologies.

The first approach involves updating to the most recent version of Kali Linux. This version is required to obtain cutting-edge tools and security patches if the operating system was installed.

Next, launch the terminal and begin the process. Make use of msfvenom in order to create the payload. An application that can construct pre-created payloads is called Msfvenom. As an illustration, in order to develop a payload that employs reverse TCP as a type of attack that is tailored exclusively for Windows operating systems, Msfvenom was used.

As we move further, we begin the exploitation session by opening a listener, which is a component of the Metasploit framework. This allow us to link the payload to the host system and the listener port. In order to configure the Listener, start the msfconsole application and use the (multi/handler) command. After that, enable the remote exploit module. Take advantage of the exploit known as (multi/handler) and set the payload to the one that was generated by msfvenom in order to handle the reverse connection.

https://doi.org/10.31436/ijpcc.v10i2.484

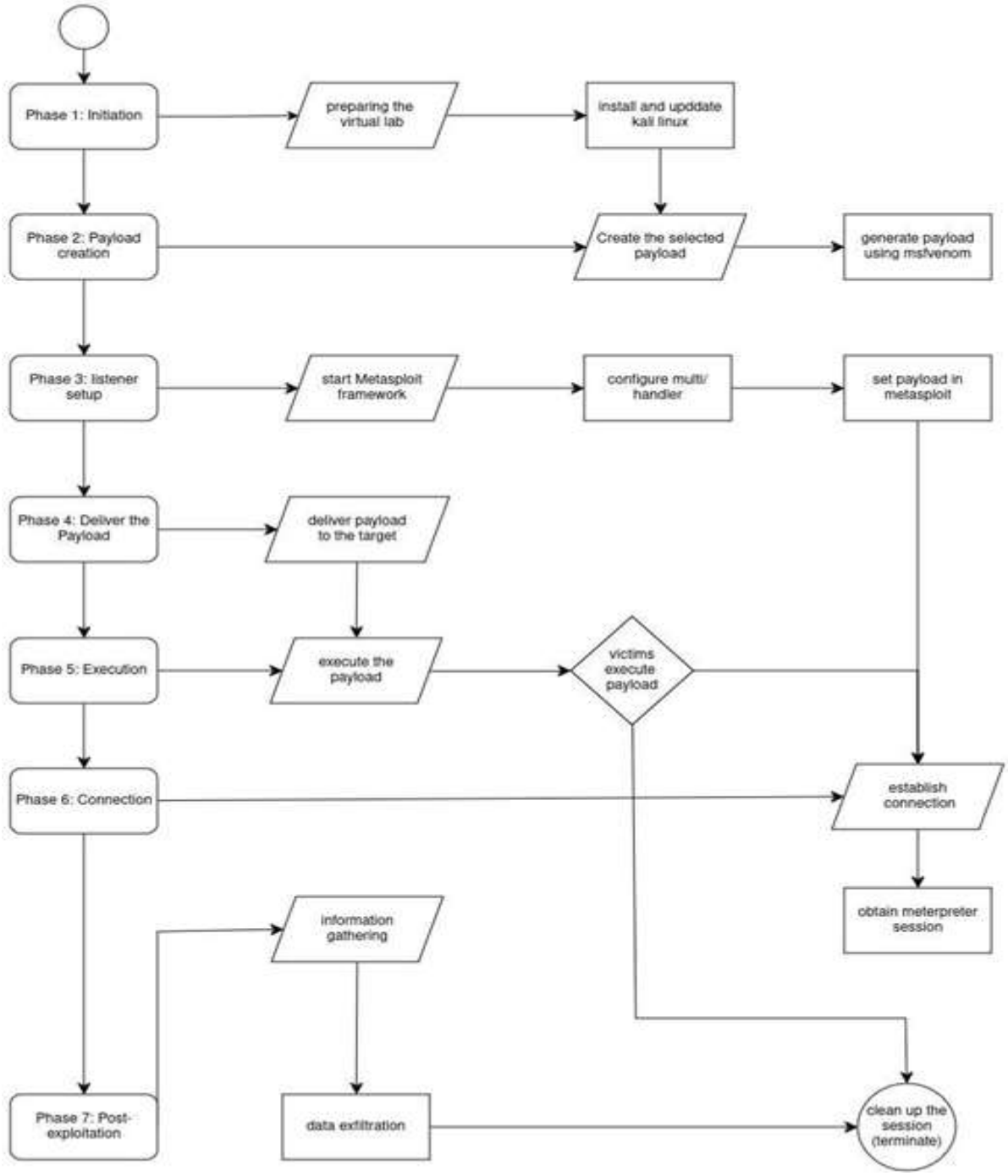

Fig. 2. The Research Methodological Flow

Next, in order to configure the listener, you will need to ensure that the values of LHOST (the attacker host) and LPORT (the listening port) are identical to those of the payload. You can start the listener by using the exploit command, and you can view the several attack routes by using the help/options command afterwards. When everything is ready, the next step is to hand over the payload to the victim. While there are a variety of approaches to delivering the payload in this experiment, we make use of two approaches: "Social engineering" and "Direct Transfer". The social engineering involves manipulating the victim in order to deliver the payload to the target. Sending an email that contains a malicious file attached to it or hosting it on a website that has been infiltrated is what this entails.

https://doi.org/10.31436/ijpcc.v10i2.484

Whereas the "Direct Transfer" deals with providing the payload in a direct manner. In the event that physical access was available or a pre-existing network connection was obtained, the payload may be sent immediately through the use of any storage devices.

After the payload has been properly delivered, the victim or the machine must activate the backdoor in order to create a successful connection in Msfconsole. Only then will the payload be executed. Following the establishment of a session in Metasploit, the listener should be able to detect the reverse connection, which will provide you with a Meterpreter session. This allow obtaining access to the victim system or machine. Several post-exploitation actions can be carried out once access has been gained. These operations include "Privilege Manipulation", "Data Exfiltration", "Installing Malware/Trojans," and "eavesdropping network".

Last but not least, the session is terminated by removing any leftover files that have been created. Once the testing phase is finished, it is imperative to verify that the session is terminated correctly in order to eliminate all traces of the footprint and conceal the backdoor. Erase any artefacts that may be present on the target system, such as any files that are still open or system logs, in order to prevent detection and guarantee the test's dependability

IV. Results

The experimental result of this study is presented in this section. Following extensive testing conducted under conditions mirroring real-world settings, we can now share the initial findings of the penetration testing. The research primarily aimed to assess the level of harm posed by backdoor attack methods to the organization's operations. The testing involved replicating different backdoor attack paths with a single payload development, interpreting software vulnerabilities, and analysing rogue websites in a controlled setting to prevent any unwanted consequences.

The effects of the breach were primarily focused on identifying vulnerabilities and assessing the organization's ability to recognise and respond to them. During the testing, the attack scenario was carried out. The first scenario involves a phishing attempt that aims to deliver a backdoor payload. The objective is to assess the effectiveness of email filters and user knowledge in preventing this type of attack. The method employed entailed dispatching phishing emails to targeted people, which included a malevolent attachment. A total of twenty employees were specifically selected as targets, leading to a 10% chance of successfully opening the payload and a 5% probability of successfully executing it (see Figure 3). The SIEM system identified 2 out of 5 instances where the payload was successfully executed, while the remaining 3 instances were spotted by EDR tools. The mean duration from detection to initial response was 15 minutes. The attack's impact was mitigated by achieving isolation before any important data was accessed.

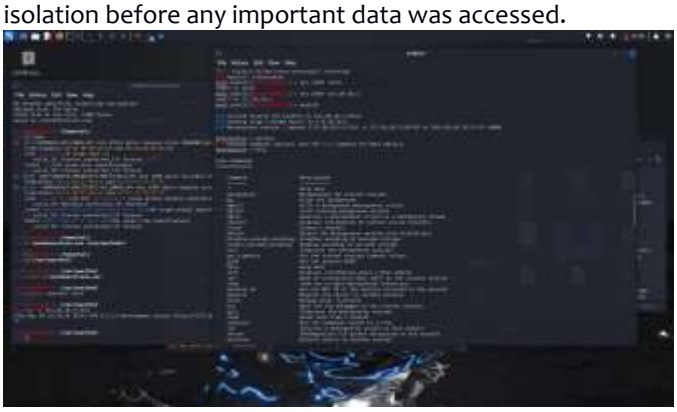

Fig 3. The first Scenario Attack Vector

Scenario 2: Exploiting Software Vulnerability: This scenario examines the impact of a backdoor on old software. The software is susceptible to exploitation due to identified flaws, such as inadequate security patches. The backdoor payload can readily infiltrate the system via the susceptible software. Thankfully, the Intrusion Detection System (IDS) promptly detected the abnormal behavior within the software at an early stage. Nevertheless, the system's average reaction time for isolating the affected software was 10 minutes, a somewhat sluggish performance for response isolation (see Figure 4). During the time it took for a response to be initiated, the attackers were able to effectively steal and remove half of the essential data and monitor network logs. This has had a substantial impact on the organization's operations, which could be further disrupted if an appropriate strategy to mitigate the situation is not implemented.

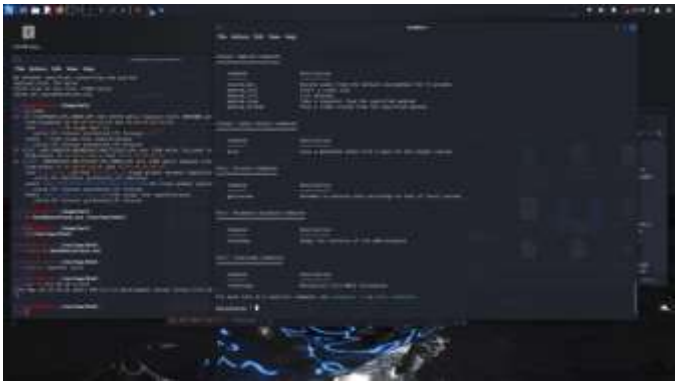

Fig 4. The Second Scenario Attack Vector

This research emphasizes the suggestions and recommendations for enhancing overall security management, such as the integration of sophisticated email filtering. Technologies and methods used to detect unauthorized access or intrusion. Enhancing phishing

awareness is crucial for mitigating the majority of phishing-related attacks. Furthermore, in order to minimize software vulnerabilities and maintain high levels of security, it is imperative to regularly perform data backups, manage patches, and update software. Regular testing is necessary to prevent potential "zero-day" malware. Enhancing security information and event management, intrusion detection systems (IDS), and intrusion prevention systems (IPS), along with adopting strong authentication and access control, can bolster security measures by enabling staff training, continuous monitoring, and authentication.

Finally, . A phishing assault has a 5% success rate in delivering a backdoor payload. This attack method involves using phishing emails to transfer the backdoor payloads, which has led to successful executions. Although SIEM and EDR systems detected most occurrences, a few initially went unnoticed. During the test, once the machine system was compromised, it required an average of 7 minutes to completely gain control. The testing yielded restricted horizontal movement and no essential data retrieval before confinement. Exploiting software flaws, particularly a known weakness in an outdated software program, is the most effective method of breaching security in this test, when compared to other types of attacks. The Intrusion detected the anomalous behavior within a span of 3 minutes by utilizing Intrusion Detection Systems (IDS). The system response involves the isolation of affected data or software within a time frame of ten minutes. Exploiting software vulnerabilities can result in the partial exfiltration of data before the machine is isolated. Insiders executing insider threats may employ a USB device to install harmful or backdoor malware, either acquiring unauthorized access or detecting vulnerabilities in the code. The endpoint protection system recognized it within a span of two minutes. The system will be quarantined within an average duration of 5 minutes. The intrusion detection system, also known as SIEM, has a little impact due to its rapid and efficient detection and response capabilities.

V. Conclusions

The primary objective of this study's penetration testing was to analyses and evaluate the level of risk posed by backdoor attack techniques, specifically within organizational operations, in order to quantify the extent of the backdoor threat. The test involved many attacks, which yielded valuable data on the detection capability, response time to backdoor attacks, stealthiest of the backdoor attack, and effectiveness of mitigation measures. The vulnerabilities revealed encompass a deficiency in email security, leading to a significant rate of success for phishing emails in circumventing the organization's current safeguards. Moreover, the high occurrence of crucial vulnerabilities in obsolete software programs presents a substantial danger as security threats and attacks persistently develop. Insider threats are a worry because of the insufficient monitoring and access controls for personnel within an organization, which can make them potentially dangerous. Ultimately, this study emphasizes the significance of regularly conducting testing, monitoring systems, and upgrading Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) inside an organization. This ensures that vulnerabilities can be quickly identified and backdoor assaults may be prevented in their early phases. As advanced technology becomes more integrated, security measures must enhance defensive strategies to keep up with the quickly growing cyber threats. This abstract provides a concise overview of the research results, presenting thorough and unambiguous recommendations for organizations to enhance their defensive strategies and offering guidelines for penetration testers conducting assessments on backdoor Attack.

Acknowledgment

This research is made possible and supported by UMP-IIUM Sustainable Research Collaboration 2022 Research Grant (IUMP-SRCG22-014-0014).

Conflict of Interest

The authors declare that there is no conflict of interest.

References

[1] H. Yang, K. Xiang, M. Ge, H. Li, Lu R, S. Yu. A comprehensive overview of backdoor attacks in large language models within communication networks. IEEE Network. 2024 Feb 20.

[2] J. Dai, C. Chen, Y. Li. A backdoor attack against lstm-based text classification systems. IEEE Access. 2019 Sep 13; 7:138872-8.

[3] S. Yang, J. Bai, K. Gao, Y. Yang, Y. Li, S.T. Xia. Not all prompts are secure: A switchable backdoor attack against pre-trained vision transfomers. InProceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition 2024 (pp. 24431-24441).

[4] Y. Li, Y. Jiang, Z. Li, S.T. Xia. Backdoor learning: A survey. IEEE Transactions on Neural Networks and Learning Systems. 2022 Jun 22;35(1):5-22.

[5] S. Liang, M. Zhu, A. Liu, B. Wu, X. Cao, E.C. Chang. Badclip: Dual-embedding guided backdoor attack on multimodal contrastive learning. InProceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition 2024 (pp. 24645-24654).

[6] S. Seo, Kim. D. Study on inside threats based on analytic hierarchy process. Symmetry. 2020 Jul 29;12(8):1255.

[7] Y. Gao, B.G. Doan, Z. Zhang, S. Ma, J. Zhang, A. Fu, S. Nepal, H. Kim. Backdoor attacks and countermeasures on deep learning: A comprehensive review. arXiv preprint arXiv:2007.10760. 2020 Jul 21.

[8] B. Li, Y. Cai, H. Li, F. Xue, Z. Li, Y. Li. Nearest is not dearest: Towards practical defense against quantization-conditioned backdoor attacks. InProceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition 2024 (pp. 24523-24533).

[9] S. Hashemi, M. Zarei. Internet of Things backdoors: Resource management issues, security challenges, and detection methods.

Transactions on Emerging Telecommunications Technologies. 2021 Feb;32(2):e4142.

[10] H. Qiu, Y. Zeng, S. Guo, T. Zhang, M. Qiu, Thuraisingham B. Deepsweep: An evaluation framework for mitigating DNN backdoor attacks using data augmentation. InProceedings of the 2021 ACM Asia Conference on Computer and Communications Security 2021 May 24 (pp. 363-377).

[11] Z. Liu, T. Wang, Huai M. Miao C. Backdoor attacks via machine unlearning. InProceedings of the AAAI Conference on Artificial Intelligence 2024 Mar 24 (Vol. 38, No. 13, pp. 14115-14123).

[12] B. Chen B, Carvalho W, Baracaldo N, Ludwig H, Edwards B, Lee T, Molloy I, Srivastava B. Detecting backdoor attacks on deep neural networks by activation clustering. arXiv preprint arXiv:1811.03728. 2018 Nov 9.

[13] A.l. Kader H.A. Hammoud, S. Liu, M. Alkhrashi, F. Albalawi, Ghanem B. Look Listen and Attack: Backdoor Attacks Against Video Action Recognition. InProceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition 2024 (pp. 3439-3450).

[14] Y. Dong, X. Yang, Z. Deng, T. Pang, Z. Xiao, H. Su, J. Zhu. Black-box detection of backdoor attacks with limited information and data. InProceedings of the IEEE/CVF International Conference on Computer Vision 2021 (pp. 16482-16491).

[15] Y. Wan, Y. Qu, W. Ni, Y. Xiang, L. Gao, Hossain E. Data and model poisoning backdoor attacks on wireless federated learning, and the defense mechanisms: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2024 Feb 7.

[16] M. Goldblum, D. Tsipras, Xie C, Chen X, Schwarzschild A, Song D, Mądry A, Li B, Goldstein T. Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2022 Mar 25;45(2):1563-80.

[17] T.D. Nguyen, Nguyen T.A, Tran A, Doan K.D, Wong K.S. Iba: Towards irreversible backdoor attacks in federated learning. Advances in Neural Information Processing Systems. 2024 Feb 13;36.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.466

A Mapping Study of Intrusion Detection System

Wan Ahmad Safwan Wan Umar, Norsaremah Salleh*
Computer Science Department, Kulliyyah of ICT, Malaysia

*Corresponding author norsaremah@iium.edu.my
(Received: 28th March 2024; Accepted: 4th April 2024; Published on-line: 30th July 2024)

Abstract—The Network Security Monitoring System has been widely used to check many systems that supply services. A lot of monitoring tools have been developed to facilitate the monitoring of the network security. Since there are a lot of options to cater to our needs, this will cause a lot of time and resources to try each tool that is suitable with the system. In this research, we conducted a comparative analysis to analyse each tool presenting their advantages, disadvantages and the method used. The main objective of this research is to perform a systematic mapping study for the purpose to identify research topics related to network intrusion detection system, to assess the most frequently applied method of intrusion detection system, and to verify the types of cyber-attack that currently exist. Based on the 30 primary studies included in this mapping study, the findings indicated that the most intrusion detection system commonly used is the hybrid method and Data Injection has been the primary attack type in the existing system.

Keywords—Intrusion detection, attack detection, mapping study, types of attack

I. Introduction

Attack detection systems or Intrusion detection systems (IDS) are a vital component of cybersecurity, as they help organizations identify and respond to threats in their networks and systems [1]. An IDS focuses on traffic that is on the internal network to identify any suspicious or malicious behavior, in contrast to a firewall, which is at the perimeter and serves as a gatekeeper to monitor network traffic and assess if it should be allowed into the network or endpoint at all. As a result, the IDS is able to identify attacks that bypass the firewall as well as those that come from within the network. Most IDS solutions combine anomaly-based detection, which simply searches for suspicious activity or behavior that is strange or significantly different from the established norm, with signature-based detection, which compares traffic against a database of known attacks or attack techniques, to detect threats [1].

Why do we need IDS when we already have firewall? Mihret et al. [1] mentioned, "*No network is impermeable, and no firewall is error-proof. Attackers often create new vulnerabilities and attack methods intended to get past your security*". For many attacks, obtaining user credentials that give them access to the network and data requires the deployment of other malware or social engineering. Network security requires a network intrusion detection system (NIDS) since it makes it possible to identify and react to hostile traffic. However, the landscape of attack detection systems is vast and varied, with numerous approaches, techniques, and technologies available. As a result, it can be difficult for organizations to determine which attack detection system is the most appropriate for their needs [2].

The main objectives of this study are: i) to investigate the publication fora on the network intrusion detection system; ii) to identify the most frequently applied method of intrusion detection system, and iii) to verify the existing types of cyber-attack. This mapping study aims to provide a comprehensive overview of the current state of the field of attack detection systems, including the various approaches, techniques, and technologies that are used, as well as their strengths and limitations. The goal of this research is to help organizations make informed decisions about which attack detection system is the most suitable for their needs, based on a thorough understanding of the available options. In this study, the research was conducted to explore existing research on attack and intrusion detection systems. In addition, the research was conducted by producing a research question to guide to search for the sources of academic literature that relate to the subject matter.

This paper is organized as follows: Section 2 describes the related work available in relation to intrusion detection system. Section 3 describes the research methodology whereas Section 4 presented the analysis of results. Section 5 presented discussion of the findings in terms of research trends and gaps. Finally, Section 6 concludes this study.

II. Related Work

This Section describes the existing research works related to intrusion detection system. Vuong et al. (2015) studied a decision tree-based approach to generate basic detection criteria that are tested against denial of service and command injection attacks [3]. They discovered that adding physical input features could significantly minimize false positives and improve overall detection accuracy. They also developed an intrusion detection system that considers not

https://doi.org/10.31436/ijpcc.v10i2.466

only cyber inputs like network traffic and disc data, but also physical inputs like speed, physical jittering, and power consumption.

Wu et al. (2021) presents a unified method, in the sense of sharing the DDAE models, to provide simultaneous eavesdropping defense and detection of three common CPS attacks [4]. The simulation resulted the IEEE bus-57 system that demonstrates the proposed encryption-decryption strategy. It helps to accomplish secure transmission while maintaining acceptable reconstruction errors.

An et al. (2022) investigated the attack strategy against the power grid's dynamic state estimation, which is first presented from the adversary's point of view. The authors also identified the problem of detecting data integrity attacks, which is formulated as a partially observable Markov decision process with the feature of sequential decision-making. In the same study, a deep reinforcement learning-based method is also suggested for detecting data integrity attacks, which makes use of the Long Short-Term Memory layer to extract the state features from earlier time steps to determine whether the system is currently under attack [2].

Based on the review of related literature, we did not find any similar study that has performed review of related primary studies on the topic of intrusion detection system. Hence, this mapping study serves as a secondary study that will focus on empirical or primary studies looking at solutions on the intrusion detection.

III. Research Methodology

Systematic Mapping Study (SMS) methodology was utilized to identify and synthesize the studies found in the area of intrusion detection system. SMS method will help us to carry out a thorough, in-depth systematic method in performing the study. We refer to the mapping study guidelines by Petersen et al. 2008 [5]. SMS is described as the process of identifying and classifying existing literature publications that are pertinent to the research objective. This research major objective is to gain a thorough understanding of a certain study issue by evaluating recent and related work, identifying and analyzing research gaps and trends of intrusion detection system. The process involved in conducting the mapping study is shown in Fig. 1.

In the planning phase we formulated the research questions in order to provide an overview of the research field. Then in the second phase we started with searching the relevant primary studies. There are a few steps to conduct the searching of studies, such as specifying search string, list down online databases, manual hand searching and lastly snowballing technique. After conducting the search of relevant resources, we performed screening of all studies that have been retrieved using the inclusion and exclusion criteria. Then the classification of all the collected studies, general classification, and topic dependent classification were identified. Finally, relevant data from selected primary studies were extracted for analysis.

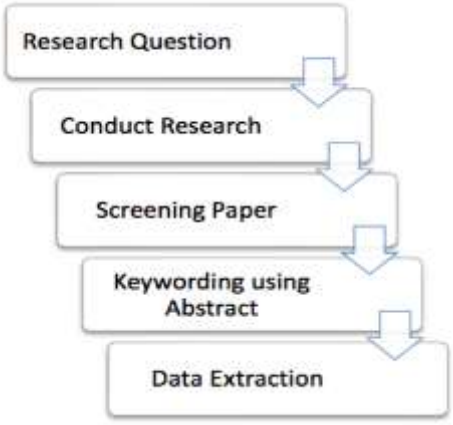

Fig. 1 Systematic Mapping Process

The first crucial stage in developing a structure for categorizing all relevant evidence obtained is the formulation of research questions (RQs). Since this study is designed to draw on empirical data to comprehend the research issue, a PICOC framework has been used to help us frame the research questions [6]. The PICOC that stands for Population, Intervention, Comparison, Outcomes, and Context, has been identified as can be seen in Table 1.

TABLE I
PICOC

Population	IT/SE companies
Intervention	Intrusion Detection System (IDS)
Comparison	Types of attack
Outcomes	Trends and gaps of the research studies
Context	Network security empirical studies

Based on the PICOC structure, we developed the following research questions (RQs) together with their accompanying justifications:

Research Question 1: What are the research topics that have been discussed in the studies of intrusion detection system?

Rationale: Since our focus is on the Attack detection system used in network security, it has required us to focus onto investigating what are available topics that have been written so far in the academic literature. The studies must clearly clarify on the attack detection system technologies used in their system. From this question, it gives an outline for us to analyze the IDS founds.

Research Question 2: What is the most frequently applied method of intrusion detection system?

https://doi.org/10.31436/ijpcc.v10i2.466

Rationale: The purpose of this question is to look into the publication patterns that can be inferred from publication information, such as the journal where the studies were published, the publication venue where we can determine who the research papers' intended audiences are, and the publication year where we can determine when academic researchers first began to study this particular subject and how it relates to current trends of network security.

Research Question 3: What are the types of attack that IDS are dealing with?

Rationale: This sub-RQ gives us an extra edge on what type of situation relates in the paper and how it gives better understanding in this certain area.

A. Study Procedures

The second stage of the SMS research methodology involved conducting a search of primary studies. The two main tasks required are defining search strings and applying them to the chosen online databases. Based on the specific terms and their comparable or synonym words identified from the study questions, we created the search string. We have used the following search string: network detection AND security AND (IDS OR system)

In order to identify additional publications from the original research discovered, we also used the backward snowballing technique through this process, which entails inspecting the references of all retrieved papers that are available. There are seven (7) papers retrieved through this technique based on the references list. In terms of the available online databases, we have used IEEEXplore and Scopus as our main resources to perform the search process in order to discover primary studies. The search string created earlier for the database search was used to carry out this action.

B. Screening of Papers

The next step is to screen the papers obtained from the searching of studies. The process of selecting papers that address the relevant parts of the subject is known as screening paper, and it is used to further filter out the papers that will be used in answering the RQs.

Additionally, SMS has defined goals and questions, and inclusion and exclusion are essential components that serve as criteria for choosing the right materials to be included or excluded. Both of the requirements should be considered based on the following categories, in accordance with "study population, nature of the intervention, outcome variables, time period, cultural and linguistic range, and methodological quality" **Error! Reference source not found.**.

We selected articles for inclusion based on the following selection criteria:

1. Studies must directly relate to intrusion detection system in a cyber security network.
2. Studies must provide adequate supporting details on how the attack was carried out and what system was affected.
3. Studies must be written in English.

In order to further filter the studies, the papers were removed based on the following exclusion criterion:

1. Studies focus on the attack instead of the detection system.
2. Studies that do not provide any empirical data.
3. Studies that are too short or brief such as abstract, poster etc. that did not provide any significant evidence.

C. Keywording of Abstracts

A step in categorizing the plan to produce the categories is known as keywording of abstracts. The purpose of this process is to provide information that supports studies resulting from the categorization activity. There are two approaches known as general classification and topic-specific classification.

The selected studies are categorized according to publication venues and publication years under general classification, often known as topic independence. In addition to the general classification, the topic-specific classification is also utilized, in which the articles are divided into groups according to the types of application. The classification, which is referenced in Table 2, can also be referred to as topic-dependent because it is associated with and dependent on a specific goal of categorization based on the topic matter.

TABLE II
Classification Scheme

General Classification	Topic-dependent Classification
Publication venue Publication year	Method of IDS Types of attack Study method

D. Data Extraction

As the last step, the classification system is used to map all of the primary studies to extract the data that is related to the research questions. To manage citations and determine publication frequencies to aid in identifying the most recent study topic, all data are organized into tabular form and stored in an Excel spreadsheet. We have extracted the following types of data: a) author(s) name, b) the year the work was published, c) paper title, d) research topic, and e) research method. Data extraction also covers IDS mechanism and the form of attack while mirroring the study questions.

https://doi.org/10.31436/ijpcc.v10i2.466

IV. Analysis of Results

We discovered 29 publications as a consequence of the search string procedure, of which 25 papers were retrieved from IEEE Explore and 5 from Scopus. The snowballing process further identified 7 papers. Finally, when applying the inclusion and exclusion criteria, we selected only 30 studies for data extraction process. Fig. 2 illustrated the selection process of the studies based on the inclusion and exclusion criteria identified in this study.

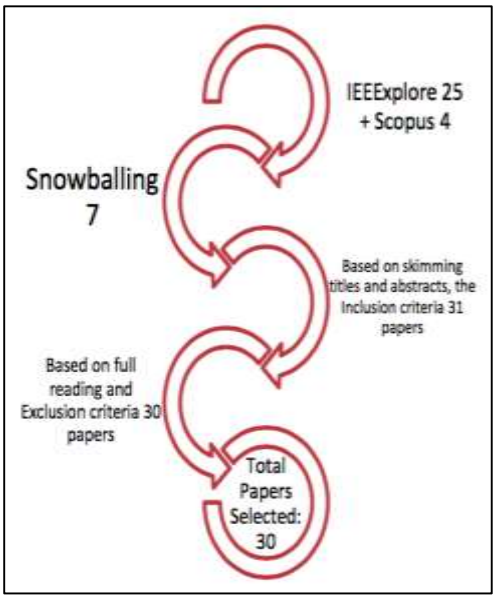

Fig. 2 Papers Screening

A. *Answering Research Question 1 (RQ1)*

This question allows us to have an overview of the current subject that has been covered between 2015 and 2022. This mapping study yielded a total of 20 topic subjects related to IDS, demonstrating the broad range of topics that an intrusion detection system ought to cover. Table 3 provides the topic discussed in the selected studies. We found that most of the studies (11 papers) fall under the topic of cyber physical systems.

TABLE III
Topic Discussed

Topic discussed	Study(s)
Cyber physical system	[7], [17], [20], [21], [23], [25], [26], [27], [30], [31], [35]
Smart Grid system	[8]
Power system	[9], [24]
Unmanned Aerial Vehicles UAVs	[10]
Delay Tolerance System	[10]
Factory Interface Network	[11]
Dynamic Watermarking	[12]
Close loop Robotic system	[13], [15], [19]
Actuator Deception	[14]
Neural Network	[18]
Networked Control System	[19]
Automatic Generation Control	[20]
Nonlinear System	[21]
Blockchain	[24]
Web Application	[28]
Smart Island	[29]
Data Driven Security	[32]
Multi Area Power System	[33]
Mobile Cyber physical system	[34]
Deep Learning	[36]

B. *Answering Research Question 2 (RQ2)*

From the mapping study we have acquired a total of 30 papers that mentioned all the methods they used in intrusion detection system. Table 4 shows the results of the analysis. Anomaly-based IDS capable to detect intrusion in both network and computer via monitoring of system's activity and then classify them as either normal or anomalous. The signature-based IDS examines the network traffic and compares it with known signatures, while hybrid method combines both the anomaly and signature-based approaches to enhance the effectiveness of intrusion detection. The hybrid method appeared to be the most used method in the IDS study, followed by anomaly-based IDS.

TABLE IV
Methods of IDS

Method of IDS	Study(s)
Anomaly Based IDS	[7], [13], [16], [18], [19], [20], [22], [30]
Signature Based IDS	[8], [14], [21], [23]
Hybrid	[9], [10], [11], [12], [17], [25], [28], [31], [34], [35], [36]

Figure 3 shows the number of IDS methods used throughout the papers acquired. Based on the figure we can see that hybrid method has the highest number that is 11 studies compared to the other method. Although the number of signatures based has the lowest which is 4 papers, the studies that report this type of method presented detail study explaining how this method helps them get through their problems.

https://doi.org/10.31436/ijpcc.v10i2.466

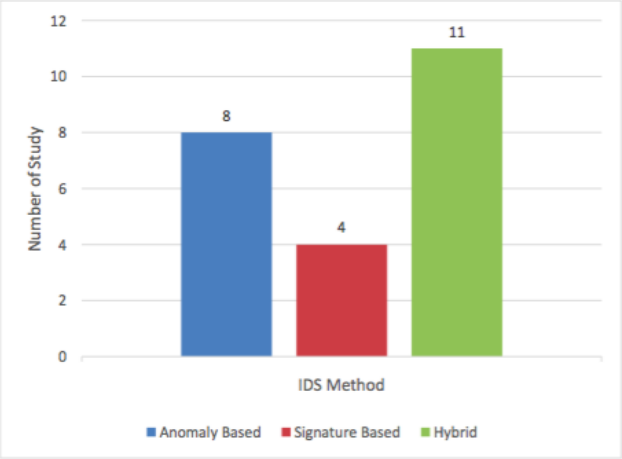

Fig. 3 Types of IDS method used

There are not many usages on the signature based because of a certain reason. Based on our analysis, we found that signature based method has weakness that is it only focused on specific attacks and it can only deal with known attacks [8]. A signature is essentially the attack's unique fingerprint. The action is captured by the signature, which is exclusive to a given attack. This practical technique is targeted at certain attacks and particularly effective at reducing the number of false positives.

On the other hand, a behavioral approach or anomaly-based method places less emphasis on a specific attack pattern and more on user or application behavior. Differentiating between harmful and non-malicious behaviors is the aim. Such systems have enormous promise: This kind of defense can theoretically counteract any attacks, both known and undiscovered. Since there are no attack signatures used, it also claims to relieve the user of the need to keep the system updated.

The finest features of both protection approaches are combined in a hybrid approach, which is the most effective defense against attacks. By offering protection against both known and unknown assaults and suppressing false-positive rates, these hybrids overcome the basic trade-off. Managers must ultimately choose what is the most crucial method to safeguarding the servers, data, and files in their settings. A hybrid strategy calls for protection at all tiers to guarantee that sensitive data is not jeopardized.

C. *Answering Research Question 3 (RQ3)*

Table 5 shows the list of attacks and Figure 4 shows the frequency of the attack from the data we extracted from the selected studies. We can see that there are a total of 11 types of attack (see Table 5). The most frequent attack is the data injection with the total number of 8, followed by the general attack with a number slightly lower than data injection, which are 7 studies. All other types of attack are significantly smaller number with 1 study mention each except for the denial of service with 4 studies mentioned by the research paper.

TABLE V
Types of Attack

No.	Type of attack	Study(s)
1	Data Injection	[7], [8], [20], [25], [27], [29], [31], [33]
2	Advance Persistence Threat	[9]
3	Switching Attack	[11]
4	Denial of Service (DOS)	[15], [19], [21], [23]
5	Distributed Denial of Service	[30]
6	Host based Attack	[16]
7	Replay Attack	[17]
8	Bias Injection	[22]
9	Random Attack	[23]
10	Cross-Site Scripting	[28]
11	General	[12], [13], [14], [18], [26], [32], [36]

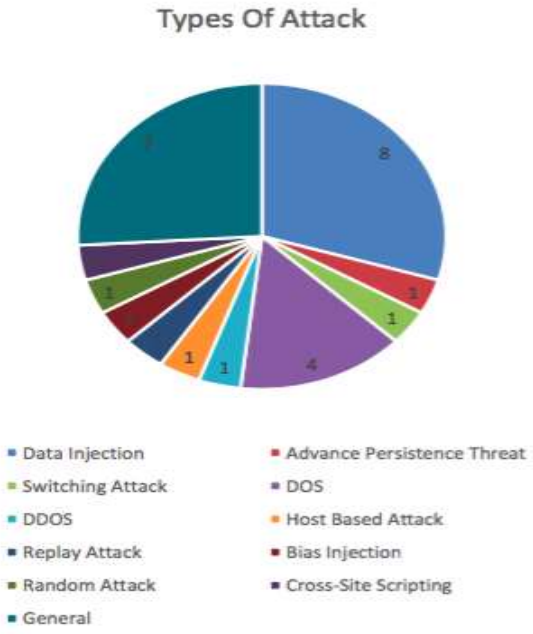

Fig. 4 Types of Attack

V. Discussion

In this section, we aimed to discover the patterns of the studies included in this SMS based on the year of publication. From Figure 5 we can see that interest in intrusion detection system is initially decreased and started to increase only after 2017. From 2018 to 2020 it shows a fluctuating pattern. This research topic reached its peak in 2021 with the number of 7 publications in that year.

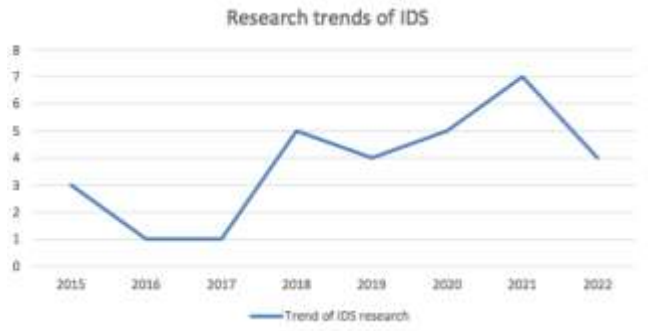

Fig. 5 Trends of IDS Research

Based on our examination of the empirical evidence we had gathered, we found that the absence of empirical evidence had a significant impact on the way we extracted data, resulting in some publications having less information presented in fewer than three pages. For this reason, a lot of data for the classification scheme is incomplete because some studies did not state them clearly. Due to the fact that a mapping study requires empirical research evidence, many of the studies retrieved from the online databases that appeared in the search results had to be disregarded. We argue that reliable findings need to be demonstrated in published studies in order to ensure selection of good quality primary studies.

VI. Conclusions

In this study, we included 30 primary studies that have been located through our SMS. This number suggests a considerably small number of studies that have been done thus far related to the intrusion detection topic. Examining the publication year, we found that this research topic has been studied since 2015.

Our research questions (RQs) assisted in the identification of issues that need to be addressed because the purpose of this study was to provide an overview of the current literature on this research topic. Through our SMS, we also learned that, in contrast to other methods, most intrusion detection system commonly used the hybrid method. The results demonstrated that Data Injection has been the primary attack type in the system on a regular basis, and this resulted in the detection of several research gaps.

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. Estifanos S. Tilahun. n.d. # Intrusion Detection System-IDS-Journal-by Sci-Tech with Estif Intrusion Detection System-IDS.

[2] A. Dou, F. Zhang, Q. Yang, and C.J. Zhang. 2022. "Data Integrity Attack in Dynamic State Estimation of Smart Grid: Attack Model and Countermeasures." *IEEE Transactions on Automation Science and Engineering* 19(3):1631–44. doi: 10.1109/TASE.2022.3149764.

[3] V.T. Phan, G. Loukas, Diane Gan, and A. Bezemskij. 2015. "Decision Tree-Based Detection of Denial of Service and Command Injection Attacks on Robotic Vehicles." in *2015 IEEE International Workshop on Information Forensics and Security, WIFS 2015 - Proceedings*. Institute of Electrical and Electronics Engineers Inc.

[4] W. Shimeng, Yuchen J., Hao L., and Xianling Li. 2021. "Deep Learning-Based Defense and Detection Scheme against Eavesdropping and Typical Cyber- Physical Attacks." in *2021 CAA Symposium on Fault Detection, Supervision, and Safety for Technical Processes, SAFEPROCESS 2021*. Institute of Electrical and Electronics Engineers Inc.

[5] K. Petersen, Hochschule Fl. Robert F. Michael M. and Shahid M.. 2008. *Systematic Mapping Studies in Software Engineering*.

[6] W. Scott, and Robert S. A. n.d. The Well-Built Clinical Question: A Key to Evidence- Based Decisions. Vol. 123.

[7] M. P1 --- M. Ghaderi, K. Gheitasi and W. Lucia, "A Blended Active Detection Strategy for False Data Injection Attacks in Cyber-Physical Systems," in IEEE Transactions on Control of Network Systems, vol. 8, no. 1, pp. 168-176, March 2021

[8] J. Wei, "A data-driven cyber-physical detection and defense strategy against data integrity attacks in smart grid systems,"2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Orlando, FL, USA, 2015, pp. 667-671.

[9] J. Yang, L. Zhou, L. Wang, S. Li, Z. Lin and Z. Gu, "A Multi-step Attack Detection Framework for the Power System Network,"2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), Guilin, China, 2022, pp. 1-8.

[10] H. Sedjelmaci, S. M. Senouci and N. Ansari, "A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1594-1606, Sept. 2018.

[11] J. Gao, J. Li, H. Jiang, Y. Li and H. Quan, "A new Detection Approach against attack/intrusion in Measurement and Control System with Fins protocol," 2020 Chinese Automation Congress (CAC), Shanghai, China, 2020, pp. 3691-3696.

[12] C. Zhang, D. Du, J. Zhang, M. Fei and A. Rakic, "A Novel Dynamic Watermarking-Based Attack Detection Method for Uncertain Networked Control Systems," 2021 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE), Shanghai, China, 2021, pp. 1- 8.

[13] A. Gorbenko, & V. Popo. Abnormal behavioral pattern detection in closed-loop robotic systems for zero-day deceptive threats. In 2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) (pp. 1-6). 2020 IEEE.

[14] K. Han, S. Li, Z. Wang and X. Yang, "Actuator deception attack detection and estimation for a class of nonlinear systems," 2018 37th Chinese Control Conference (CCC), Wuhan, China, 2018, pp. 5675-5680.

[15] A. W. Al-Dabbagh, Y. Li and T. Chen, "An Intrusion Detection System for Cyber Attacks in Wireless Networked Control Systems," inIEEE Transactions on Circuits and Systems II: Express Briefs, vol. 65, no. 8, pp. 1049-1053, Aug. 2018.

[16] T. Badgujar and P. More, "An Intrusion Detection System implementing Host based attacks using Layered Framework," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 2015, pp. 1-4.

[17] H. Guo, Z. -H. Pang, J. Sun and J. Li, "An Output-Coding-Based Detection Scheme Against Replay Attacks in Cyber-Physical Systems," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 68, no. 10, pp. 3306-3310, Oct. 2021.

[18] B. Tulkun and B. Fayzullajon, "Analysis of Integrated Neural Network Attack Detection System and User Behavior Models," 2019 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2019, pp. 1-4.

[19] H. Niu, C. Bhowmick and S. Jagannathan, "Attack Detection and Approximation in Nonlinear Networked Control Systems Using Neural Networks," in IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 1, pp. 235-245, Jan. 2020.

[20] A. Ameli, A. Hooshyar, E. F. El-Saadany and A. M. Youssef, "Attack Detection and Identification for Automatic Generation Control Systems," in IEEE Transactions on Power Systems, vol. 33, no. 5, pp. 4760-4774, Sept. 2018.

[21] Z. Tahir, A. Q. Khan and M. Asad, "Attack Detection and Identification in Cyber Physical Systems: An example on Three Tank System," 2019 15th International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, 2019, pp. 1-6.

[22] L. Kang and H. Shen, "Attack Detection and Mitigation for Sensor and CAN Bus Attacks in Vehicle Anti-lock Braking Systems,"2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 2020, pp. 1-9.

[23] H. Li, X. He, Y. Zhang and W. Guan, "Attack Detection in Cyber- Physical Systems Using Particle Filter: An Illustration on Three-Tank System,"2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Tianjin, China, 2018, pp. 504-509.

[24] P. Ramanan, D. Li and N. Gebraeel, "Blockchain-Based Decentralized Replay Attack Detection for Large-Scale Power Systems," inIEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 8, pp. 4727-4739, Aug. 2022.

[25] S. Tan, J. M. Guerrero, P. Xie, R. Han and J. C. Vasquez, "Brief Survey on Attack Detection Methods for Cyber-Physical Systems," in IEEE Systems Journal, vol. 14, no. 4, pp. 5329-5339, Dec. 2020.

[26] R. Anguluri, V. Katewa and F. Pasqualetti, "Centralized Versus Decentralized Detection of Attacks in Stochastic Interconnected Systems,"in IEEE Transactions on Automatic Control, vol. 65, no. 9, pp. 3903-3910, Sept. 2020.

[27] M. Xiao, J. Wu, C. Long and S. Li, "Construction of false sequence attack against PLC based power control system," 2016 35th Chinese Control Conference (CCC), Chengdu, China, 2016, pp. 10090-10095.

[28] K. Gupta, R. Ranjan Singh and M. Dixit, "Cross site scripting (XSS) attack detection using intrusion detection system,"2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 199-203.

[29] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, E. Tajik,S. Padmanaban, and H. Aliev , "Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack," in IEEE Access, vol. 9, pp. 16488-16507, 2021.

[30] A. Shi, "Cyber Attacks Detection Based on Generative Adversarial Networks," 2021 2nd Asia Conference on Computers and Communications (ACCC), Singapore, 2021, pp. 111-114.

[31] D. An, F. Zhang, Q. Yang and C. Zhang, "Data Integrity Attack in Dynamic State Estimation of Smart Grid: Attack Model and Countermeasures," inIEEE Transactions on Automation Science and Engineering, vol. 19, no. 3, pp. 1631-1644, July 2022.

[32] V. Krishnan and F. Pasqualetti, "Data-Driven Attack Detection for Linear Systems," in IEEE Control Systems Letters, vol. 5, no. 2, pp. 671-676, April 2021.

[33] K. Xiahou, Y. Liu and Q. H. Wu, "Decentralized Detection and Mitigation of Multiple False Data Injection Attacks in Multiarea Power Systems," in IEEE Journal of Emerging and Selected Topics in Industrial Electronics, vol. 3, no. 1, pp. 101-112, Jan. 2022.

[34] T. P. g, G. Loukas, D. Gan and A. Bezemskij, "Decision tree- based detection of denial of service and command injection attacks on robotic vehicles," 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 2015, pp. 1-6.

[35] S. Wu, Y. Jiang, H. Luo and X. Li, "Deep learning-based defense and detection scheme against eavesdropping and typical cyber-physical attacks," 2021 CAA Symposium on Fault Detection, Supervision, and Safety for Technical Processes (SAFEPROCESS), Chengdu, China, 2021, pp. 1-6.

[36] H. Yang, L. Cheng and M. C. Chuah, "Deep-Learning-Based Network Intrusion Detection for SCADA Systems,"2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 2019, pp. 1-7.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.486

EEG-based Sleep Deprivation Classification: A Performance Analysis of Channel Selection on Classifier Accuracy

Wan Nurshafiqah Nabila binti Wan Masri, Nor Zuhayra Amalin binti Zulkifli, Muhammad Afiq Ammar bin Kamaruzzaman, Nurul Liyana binti Mohamad Zulkufli*

Dept. of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia.

*Corresponding author: liyanazulkufli@iium.edu.my
(Received: 9th June 2024; Accepted: 25th June 2024; Published on-line: 30th July 2024)

Abstract—This study analyses the effect of electroencephalogram (EEG) channel selection on the classification accuracy of sleep deprivation using four distinct classifiers: Random Forest (RF), k-Nearest Neighbours (k-NN), Support Vector Machine (SVM), and Artificial Neural Network (ANN). In this study, the EEG data from ten male individuals in good health were collected. Two distinct sets of EEG channels—a limited frontal channel set (Fp1, Fp2) and a thorough 19-channel set—were used to compare the performance of the classifiers. According to our findings, the k-NN classifier produced the greatest classification accuracy of 99.7% when applied to the 19-channel EEG signals. In contrast, both SVM and ANN classifiers were able to obtain the greatest accuracy of 94% with the frontal channels. Though there are not many gaps, these results imply that employing a larger range of EEG channels greatly improves the classification accuracy of sleep deprivation. The present study emphasizes the significance of channel selection in EEG-based sleep deprivation investigations by showcasing the significant advantages of full EEG signal capture over minimum channel configurations.

Keywords—electroencephalogram (EEG), classification, sleep deprivation

I. Introduction

Sleep deprivation is a growing public health concern with significant consequences for cognitive function, physical activity, and overall well-being. Lo et al. [1] emphasizes successive nights of sleep restriction cumulatively impair diverse cognitive functions, including memory, attention, and executive control. Early detection of sleep deprivation is crucial for promoting healthy sleep habits and mitigating its negative effects.

Electroencephalograpy (EEG) offers a non-invasive method for measuring brain activity and has shown promise in classifying sleep states, including identifying sleep deprivation. Khoo et. al. in their research research showed that there are notable changes in EEG microstates for subjects with even mild sleep deprivation [2].

In previous research in automatic sleep staging and classification using EEG signals, Jeon et al. [3] demonstrated the effectiveness of machine learning for sleep stage classification using multiple EEG channels. Their study highlighted the potential for accurate sleep state identification even with a reduced number of channels.

Our research extends this work by specifically focusing on sleep deprivation classification and investigating the trade-off between using a comprehensive set of channels and a minimal frontal channel configuration. Several studies explored channel selection algorithms for EEG signal processing, achieving high classification accuracy with a subset of channels compared to using all available channels [4-6]. This suggests that specific channels may hold more valuable information for sleep deprivation classification. Furthermore, Sen et al. [7] compared the performance of various classifiers for sleep stage classification using feature selection techniques. Their findings emphasize the importance of selecting informative features, which can be linked to choosing informative channels in our context.

In regards to the analysis methods, there are various techniques to analyse EEG data for classification, such as Support Vector Machine (SVM), Artificial Neural Network (ANN), Random Forest (RF), and so on. SVM was incorporated by Sase et. al. in their proposed adaptive feature extraction approach based on EEG theta/beta ratio [8], while Upadhyay et. al. studied the effect of heat stress on sleep stages using wavelet-based analysis of SVM and radial basis function neural network [9]. Other than that, an algorithm to automatically classify sleep stages from EEG data was proposed by Liu et. al. based on RF and hidden Markov model [10].

This research focuses on studying suitable EEG-based sleep deprivation classification by evaluating the performance of four common machine learning classifiers (SVM, ANN, k-NN, and RF) with varying channel configurations, using resting state EEG. The finding might be valuable for researchers and developers working on

https://doi.org/10.31436/ijpcc.v10i2.486

portable and user-friendly EEG devices for sleep monitoring and sleep deprivation detection.

Moreover, in this paper we investigate the effectiveness of channel selection in EEG-based sleep deprivation classification using machine learning algorithms. We analyse the impact of channel number on classifier accuracy by comparing performance between using all 19 available channels and a limited selection of frontal channels (Fp1 and Fp2).

II. METHODOLOGY

The methodological approach used to categorize sleep deprivation using EEG signals is described in this chapter. Using a large dataset of EEG recordings from ten healthy male students, the study focuses on the phases of preprocessing, feature extraction, and classification. In addition to a comprehensive 19-channel set, special attention is paid to the examination of frontal EEG channels because of their increased susceptibility to alterations associated with sleep.

A. Participants

Ten healthy male students' resting-state EEG recordings from an existing dataset were used in the investigation. This dataset is based on the experiment by Kamaruzzaman et. al. who studied the effect of sleep deprivation on driver's mental fatigue [11]. To guarantee a homogeneous and controlled sample and to make it easier to assess the effects of sleep deprivation on EEG signals, these people were chosen. Two sleep conditions were used to gather the EEG recordings: regular sleep and sleep deprivation. The dataset offered a wide range of EEG signals from several channels. This dataset is

B. Methodology Flow

Four main steps make up the methodological framework for this study as shown in Fig. 1 below: data acquisition, data preprocessing, feature extraction, and classification.

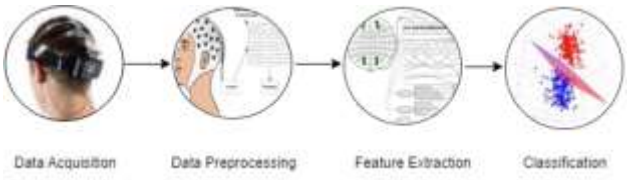

Fig. 1 The methodology flow for the EEG analysis

C. Data Acquisition

The existing EEG data was recorded using a DABO machine following the international 10-20 system for electrode placement. A total of 19 channels (Set 1) were used, and for this study, two EEG channels of interest (Set 2) were selected which is Fp1-Cz and Fp2-Cz, representing the voltage difference between the frontal. This selection was based on the suggestion by Fu et al. that the effectiveness of sleep scoring is influenced by the choice of EEG channel, with derivations from the frontal region being the optimal choice due to the voltage difference between the frontal areas [12]. The positions of the channels are shown in Fig. 2.

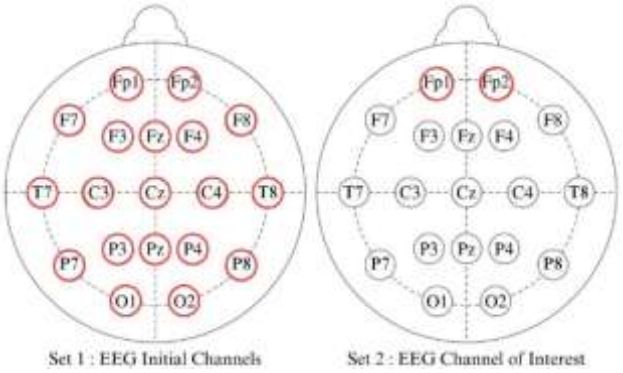

Fig. 2 The selected sets of EEG channels

D. Data preprocessing

EEG signal preprocessing is essential to eliminate artifacts and noise, guaranteeing that the analysis that follows is founded on accurate and clean data.

Detrending the EEG signals to eliminate slow drifts was the first stage in the preprocessing pipeline. By removing low-frequency trends that can mask the real-signal, this procedure improves the EEG data's clarity for additional analysis. Removing these trends makes the underlying brain activity more visible, which makes feature extraction more precise.

Next, a Butterworth low-pass filter with a 30Hz cutoff frequency was used to filter out high-frequency noise. 30Hz was selected because it is good at keeping the key EEG components that are important for sleep research while removing higher-frequency noise that could deteriorate signal quality. Because of its smooth frequency response, which prevents the signal from becoming distorted, the Butterworth filter is very well-liked. The transfer function of the filter can be expressed as follows:

$$|H(jw)| = \frac{1}{\sqrt{1 + \left(\frac{w}{w_c}\right)^{2n}}}$$

where w_c symbolizes the frequency cutoff, and the filter's order is denoted by n. The substantial attenuation of frequencies above 30Hz is guaranteed by this mathematical representation.

https://doi.org/10.31436/ijpcc.v10i2.486

Muscles artifacts were eliminated using Independent Component Analysis (ICA) after the filtering procedure. A computational technique called ICA divides a multivariate signal into additive parts. Klug et al. [13] emphasizes that ICA can still effectively clean sensor data from eye and muscle activity artifacts, and they also recommend using higher high-pass filter cut-offs than traditionally applied. When it comes to separating and eliminating non-neural aberrations like muscular movements that could taint the EEG data, this method works especially well. The EEG data are cleaned up by using ICA, leaving only the neuronal activity that is relevant to the research.

The EEG signals were then analyzed, cleaned, and stored in a new file. By ensuring that the dataset is prepared for further feature extraction and analysis, this stage protects the preprocessed data's quality and integrity. The study's subsequent phases are based on the saved dataset, which makes it easier to classify sleep conditions accurately and consistently.

E. Feature Extraction

The preprocessed EEG signals are transformed into a format appropriate for machine learning through feature extraction. Welch's method was used in this study to calculate Power Spectral Density (PSD), which was the main technique for feature extraction. PSD provides information about the frequency content of the signal by estimating the power distribution of the EEG signal across various frequencies. Using Welch's approach, the signal is divided into overlapping windows, each segment is subjected to a Fourier transform, and the outcomes are averaged. When compared to single-segment approaches, this methodology minimizes variance and provides a robust estimation of the power spectral density of the signal. Each segment's PSD is provided by:

$$P_{xx}(f) = \frac{1}{N}\sum_{n=0}^{N-1}|X_n(f)|^2$$

where $P_{xx}(f)$ is the power spectral density, N is the number of data segments, and $X_n(f)$is the Fourier transform of the n-th segment.

In addition, the power within each frequency band—beta, gamma, alpha, theta, and delta—was calculated to examine the signal dispersion among all channels. Since different frequency bands are linked to different cognitive and physiological processes, this band-specific examination is essential. The goal of the study is to identify the distinctive alterations in brain activity brought on by sleep deprivation by measuring the power in these bands. The building of an accurate classification model is facilitated by the comprehensive picture of the EEG signal characteristics under various sleep situations provided by this detailed frequency analysis.

F. Classification

To create and assess a model that could differentiate between sleep deprivation and normal sleep based on the variables that were retrieved, the classification process required several crucial phases. Originally, the dataset was structured for machine learning using the features X and labels y. The collected PSD values were represented by features, and the labels were binary, designating either regular sleep (0) or sleep deprivation (1). To train the classifier to identify patterns linked to each condition, this configuration was necessary.

The dataset was then divided, usually in an 80-20 or 70-30 ratio, into training and testing sets. We have allocated 80% of the data for training and 20% for testing is used to computed accuracy. This section made sure there was enough data available for the model to be trained and for assessing its performance, which helped to avoid overfitting and guaranteed the model's applicability to fresh data.

Various classification techniques with its algorithms were examined, such as SVM, ANN, k-NN, and RF. SVM for its efficacy in high-dimensional spaces, ANN for its capability to model complex nonlinear relationships and its flexibility in learning from large amounts of data, k-NN for its simplicity and ease of implementation, and RF for its resilience and capacity to handle noisy data were the specific advantages that led to the selection of each algorithm.

The equations for SVM, ANN, k-NN, and RF are shown in equations (1) until (4), respectively. The equation of SVM is provided by:

$$SVM\ ;\ K\left(x_{i,}x'_{i}\right) = \left(1+\sum_{j=1}^{p} x_{ij}x'_{ij}\right)^{d} \quad (1)$$

where K is some function called the kernel, $\left(x_{i,}x'_{i}\right)$ are the inner products between all pairs of training observations, and d is the positive degree of polynomial kernel.

Next, NN is depicted by:

$$ANN\ ;\ y = f^{x}(x) \quad (2)$$

where input x is therefore assigned to category y, and according to the feed forward model, $y = f(x;\theta)$.

The equation of k-NN is shown by:

$$k-NN\ ;\ Pr\left(Y=j \middle| X=x_0\right) = \frac{1}{K}\sum_{i\in N_0} I\left(y_i=j\right) \quad (3)$$

where $I\left(y_i=j\right)$ is an indicator variable that equals 1 if $y_i=j$ and zero if $y_i \neq j$.

Lastly, Random Forest is calculated as the following:

$$Random\ Forest\ ;\ Gini\ Index = 1-\sum_{i=1}^{n}(P_i)^2 \quad (4)$$

https://doi.org/10.31436/ijpcc.v10i2.486

where *Gini index* is for knowing how impure or pure the splitting will be when selecting a feature to split further. A pure sub-split means either we should be getting 'yes' or 'no'. P_j represents the probability of a class whereby $P\_$ is the probability of a positive class and P is the probability of a negative class.

Using the collected features, the selected classification model was trained on the training set to identify patterns related to different sleep states. The model's parameters were fine-tuned during training to maximize classification accuracy.

SVM-with a radial basis function (RBF) kernel is selected for classification tasks. ANN-comprises, including two hidden layers with 64 and 32 neurons, respectively, and an output layer with a single neuron using a sigmoid activation function for binary classification and the training process iterates over multiple epochs (10 in this case) with a batch size of 32, KNN-with the number of neighbors set to 5 (n_neighbors=5), RF-with 100 decision trees (n_estimators=100) and a fixed random state for reproducibility (random_state=42).

Following training, several metrics were used to assess the model's performance, including precision, recall, F1-score, and accuracy. These metrics offered a thorough evaluation of the model's accuracy in classifying sleep environments. These metrics' formulas are as follows:

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP}$$

where TP represents true positives, TN represents true negatives, FP represents false positives, and FN represents false negatives. With the help of these measurements, the model's performance was thoroughly assessed, enabling modifications and enhancements to reach the maximum level of accuracy in categorizing sleep deficiency.

III. Results

The results of the EEG-based sleep deprivation categorization study are presented in this section, with an emphasis on the examination of EEG signals obtained from subjects who were sleep deprived as well as those who were not. Using various EEG channel configurations, the study assessed the effectiveness of numerous machines learning classifiers, including SVM, ANN, k-NN, and RF. Several figures and tables that give a thorough and objective depiction of the data gathered, and the accuracy attained by each classifier under different circumstances are used to illustrate the results.

A. *Varying EEG Signals*

Brain activity is dramatically affected by sleep deprivation, as EEG measurements show. The raw EEG signals of participants who were sleep deprived are shown in Fig. 4. The graphic shows a time-series graph that illustrates the EEG signal amplitudes recorded from various channels over a predetermined amount of time. A distinct EEG channel is shown by each subplot, which depicts the electrical activity of the brain during sleep deprivation. The amplitude variations show how the brain reacts to sleep loss; there are discernible patterns and fluctuations that may be connected to the subject's sleep deprivation. Before any preprocessing or feature extraction, the raw data is shown graphically in this figure.

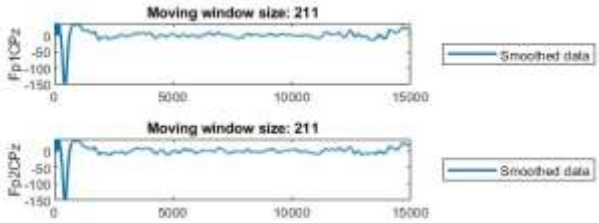

Fig. 3 Sleep deprived raw signals

EEG signals are crucial for comprehending brain activity in a variety of situations, such as diagnosing neurological disorders, monitoring cognitive states, and studying the effects of sleep deprivation on brain function. The raw EEG signals of participants who did not have sleep deprivation are displayed in Fig. 5. This image, like image 2, has several subplots that show various EEG channels over time. These signals' amplitude changes indicate typical brain activity when people are not sleep deprived. We can visually identify the changes in brain activity between sleep-deprived and non-sleep-deprived states by comparing Figures 1 and 2, which highlight potential features that could be used for classification.

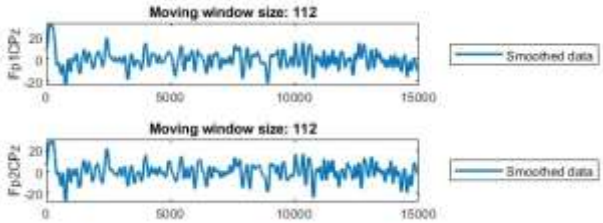

Fig. 4 Non-sleep deprived raw signals

https://doi.org/10.31436/ijpcc.v10i2.486

In this study, we use MATLAB's "smoothdata" function with the "movmean" method and a smoothing factor of 0.65. It was observed that sleep-deprived subjects exhibit slow wave activity, whereas non-sleep deprived subjects display active wave patterns.

B. *Classifiers Average Accuracy*

The average accuracy rates of SVM, ANN, k-NN, and RF classifiers under various situations are summarized in Table 1. The table has distinct columns for each classifier's accuracy when utilizing all 19 EEG channels and when restricted to frontal channels. For instance, when employing 19-channel set, k-NN demonstrates the greatest accuracy of 99.7%. However, when limited to frontal channels, all classifiers show decreased accuracy, highlighting the significance of complete EEG data for precise classification.

TABLE 1
THE AVERAGE ACCURACY TABLE OF SLEEP DEPRIVATION CLASSIFICATION

Subject	Accuracy (%) for 19-channels				Accuracy (%) for frontal channels			
	SVM	ANN	KNN	RF	SVM	ANN	KNN	RF
S1	98	99	100	98	94	94	93	93
S2	99	99	100	97	94	94	93	93
S3	98	99	100	98	94	94	93	93
S4	96	97	99	95	94	94	93	93
S5	98	98	99	96	94	94	93	93
S6	96	98	100	96	94	94	93	93
S7	99	99	100	98	94	94	93	93
S8	96	98	99	96	94	94	93	93
S9	98	99	100	98	94	94	93	93
S10	97	99	100	97	94	94	93	93
Average	**97.5**	**98.5**	**99.7**	**96.9**	**94.0**	**94.0**	**93.0**	**93.0**

For the average performance of classifiers on non-sleep deprived data—19 channel, KNN achieved the highest accuracy at 99.8%, and for the frontal channel set, the highest accuracy for non-sleep deprived data was achieved by SVM and ANN at 94%.

TABLE 2
THE AVERAGE ACCURACY TABLE OF NON-SLEEP DEPRIVATION CLASSIFICATION

Subject	Accuracy (%) for 19-channels				Accuracy (%) for frontal channels			
	SVM	ANN	KNN	RF	SVM	ANN	KNN	RF
S1	98	99	100	98	94	94	93	93
S2	99	100	100	99	94	94	93	93
S3	99	99	100	98	94	94	93	93
S4	99	99	99	98	94	94	93	94
S5	95	97	99	94	94	93	94	93
S6	100	100	100	100	94	93	94	93
S7	97	99	100	97	94	94	93	93
S8	99	99	100	98	94	94	93	93
S9	98	100	100	98	94	94	93	93
S10	99	99	100	98	94	94	93	93
Average	**98.3**	**99.1**	**99.8**	**97.8**	**94**	**93.8**	**93.2**	**93.1**

C. *Average Accuracy Plots*

The classification accuracy of the four methods (SVM, ANN, k-NN, and RF) is shown in Fig. 6. The graph contrasts each classifier's performance while employing 19 EEG channels against just frontal channels. To differentiate between sleep-deprived and non-sleep-deprived settings, the bars are color-coded and categorized according to the classifier. The data in Table 1 and Table 2 is graphically supported by this figure, which also demonstrates that k-NN obtains the maximum overall accuracy, and that the accuracy decreases dramatically when utilizing only frontal channels for all classifiers.

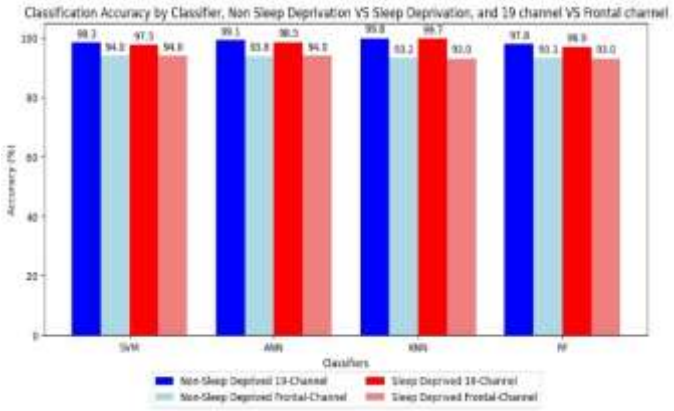

Fig. 5 The overall classification accuracies between four classification algorithms of sleep-deprived and non-sleep-deprived data for 19-channel and frontal-channel sets

IV. DISCUSSIONS

A. *Impact of EEG Signal Consistency*

Normal cognitive function and attentiveness are reflected in the consistent EEG signal patterns seen in persons who are not sleep deprived. Because it stands in stark contrast to the increased variability observed in sleep-deprived people, the brain's attempt to make up for the lack of sleep is shown in the more irregular and less smooth theta and delta wave patterns. This contrast emphasizes how fundamentally different sleep deprivation induces different states of brain activity, underscoring the significance of regular sleep in maintaining normal brain function.

B. *Importance of Channel Selection*

Classifying sleep deprivation data is more accurately achieved when a full set of 19 EEG channels is used. On the other hand, while still useful, employing exclusively frontal channels results in marginally less accuracy. This result highlights the benefit of using a wider range of channels to achieve a more precise classification. Multiple channels are anticipated to record a larger range of brain activity, which gives the classifiers a more robust dataset to work with and ultimately improves their performance. In contrast, it also can be said that 2 frontal channels are enough to detect

https://doi.org/10.31436/ijpcc.v10i2.486

sleep deprivation in normal subjects in this study, although with lesser accuracy but still higher than 90% accuracy.

C. *Classifier Accuracy*

The k-NN classifier's better performance when using all 19 channels of EEG signals indicates that this algorithm is especially good at processing the high-dimensional data that comes with extensive EEG recordings. The efficacy of the k-NN classifier in differentiating between sleep-deprived and non-sleep-deprived states is demonstrated by its 99.7% accuracy rate. In contrast, the SVM and ANN classifiers' performance, which achieved a 94% accuracy rate employing frontal channels, shows their durability and dependability, even though their accuracy was marginally lower than that of the k-NN classifier. These findings imply that although ANN and SVM are good competitors for classification tasks, k-NN is especially well-suited for this case due to its ability to use the entire spectrum of EEG data.

D. *Proposed Protocol*

In this section, we propose a protocol to detect sleep deprivation, for future work. This suggested procedure in Fig. 7 below uses EEG readings in a step-by-step manner to methodically investigate sensory and cognitive functioning. Initially, subjects would rest for four minutes, two of which would be spent with their eyes open and two with them closed, to establish baseline EEG activity both with and without visual input. Subsequently, auditory situations involving both noise and no noise scenarios would be presented to the subjects to evaluate the brain's reaction to auditory stimuli. After that, tests of visual conditions with and without lighting would be conducted to assess how well the brain processes visual data. Lastly, participants would engage in a Go/No-go task that tests reaction inhibition and cognitive control. For 'Go' trial (yellow square), they would click a button; for 'no-go' trials (blue square), they would restrain their answer.

With the use of this extensive methodology, it would be possible to analyze EEG data from a variety of sensory and cognitive states, offering new perspectives on the brain processes that underlie response inhibition and sensory processing. However, in our current study, we used pre-existing data from earlier research subjects for our current investigation. Our method enabled us to concentrate on examining the impact of channel selection performance on classifier accuracy within the framework of EEG-based sleep deprivation categorization. The suggested approach considers how various sensory and cognitive states affect EEG recordings, emphasizing how crucial it is to choose the right EEG channels to improve classifier performance for identifying hypoxia. Khan et al. [14] summarized the negative effects of SD on behavior as a whole and cognitive function as the neural pathways slow down, resulting in a lower mental state and reaction time.

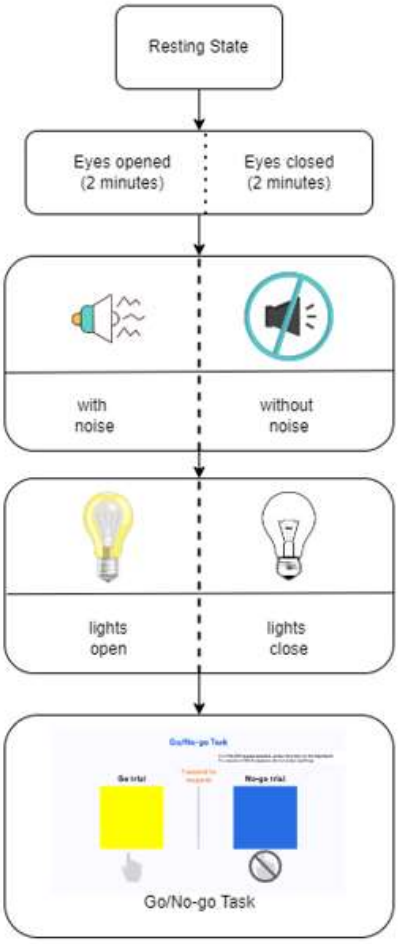

Fig. 6 The proposed protocol for the EEG experiment to detect sleep deprivation

E. *Suggestion for Classification Algorithms*

Based on the classification accuracy from the bar plots, the k-NN is the optimal option for 19-channel, demonstrating the maximum accuracy for both non-sleep-deprived (99.8%) and sleep deprived (99.7%) stages. The SVM, which obtains the maximum accuracy for both non-sleep-deprived and sleep deprived (94.0%), is advised for frontal channel data. These findings show that SVM is more successful with frontal-channel data while k-NN performs better with 19-channel data, indicating that k-NN and SVM are the recommended classifiers for these specific configurations.

V. Conclusion

This study shows that choosing the right EEG channel is essential for correctly categorizing sleep deprivation. Significant changes in brain activity are observed when EEG signals from sleep-deprived persons are analysed. The non-

sleep-deprived state shows more stable and consistent patterns than the erratic and fluctuating signals observed in sleep-deprived subjects in certain signals when observed. The results indicate that the k-Nearest Neighbours (k-NN) algorithms is robust when handling high-dimensional data, as evidenced by its maximum classification accuracy among the investigated classifiers, especially when using a comprehensive set of 19 EEG channels. Although they had somewhat less accuracy than k-NN, support vector machine (SVM) and artificial neural network (ANN) classifiers also fared well, particularly when used with frontal channels (Fp1 and Fp2).

These results highlight the value of using a wide variety of EEG channels to improve classification accuracy and imply that obtaining complete EEG data is necessary to create dependable and efficient sleep deprivation monitoring systems. To further enhance classification performance and resilience, future studies should investigate the application of sophisticated machine learning algorithms and the integration of new physiological information.

In addition, we also have proposed a procedure to methodically examine sensory and cognitive performance for sleep deprivation for future work. This technique emphasizes the significance of good EEG channel selection. It also intends to provide extensive insights into brain activities across a range of sensory and cognitive states.

ACKNOWLEDGMENT

The authors would like to thank Neurocoach Digital Lab (NDL) and Pervasive Computing and Brain Development research group (PCBDG), Kulliyyah of ICT, IIUM for their support during this study. The fourth author was partially supported through IRAGS18-030-0031.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

REFERENCES

[1] J. C. Lo and M. W. Chee, “Cognitive effects of multi-night adolescent sleep restriction: current data and future possibilities,” Current Opinion in Behavioral Sciences, vol. 33, pp. 34–41, Jun. 2020, doi: https://doi.org/10.1016/j.cobeha.2019.12.005.

[2] K. Sing E. Yee. "Resting-state electroencephalography (EEG) microstates of healthy individuals following mild sleep deprivation." *Scientific Reports* 14.1 (2024): 16820.

[3] Y. Jeon, S. Jo, and H. Kim, "Sleep Stage Classification Using Multiple EEG Channels: A Machine Learning Approach," IEEE Transactions on Biomedical Engineering, vol. 66, no. 6, pp. 1320-1323, June 2019.

[4] E. Eldele et al., "An Attention-Based Deep Learning Approach for Sleep Stage Classification With Single-Channel EEG," in IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 29, pp. 809-818, 2021, doi: 10.1109/TNSRE.2021.3076234.

[5] M. Kamrunnahar, T. Ahmed, and F. Rabbi, "Channel Selection Algorithms for EEG Signal Processing: A Review," EURASIP Journal on Advances in Signal Processing, vol. 2015, no. 1, pp. 1-19, Dec. 2015.

[6] T. Alotaiby, F. E. A. El-Samie, S. A. Alshebeili, and I. Ahmad, “A review of channel selection algorithms for EEG signal processing,” EURASIP Journal on Advances in Signal Processing, vol. 2015, no. 1, Aug. 2015, doi: https://doi.org/10.1186/s13634-015-0251-9.

[7] B. Sen.; M. Peker.; A. Çavu¸so˘ A. glu,.; F.V. Çelebi. A comparative study on classification of sleep stage based on EEG signals using feature selection and classification algorithms. J. Med. Syst. 2014, 38, 1–21.

[8] S. Takumi, and M.i Othman. "Prediction of ADHD from a Small Dataset Using an Adaptive EEG Theta/Beta Ratio and PCA Feature Extraction." *International Conference on Soft Computing and Data Mining*. Cham: Springer International Publishing, 2022.

[9] U. P. Kumar, and C. Nagpal. "Wavelet based performance analysis of SVM and RBF kernel for classifying stress conditions of sleep EEG." *Science and Technology* 23.3 (2020): 292-310.

[10] Li. Junbiao. "Automatic sleep staging algorithm based on random forest and hidden Markov model." *Computer Modeling in Engineering & Sciences* 123.1 (2020): 401-426.

[11] K. Muhammad ‘A. Ammar,. "EEG Features for Driver’s Mental Fatigue Detection: A Preliminary Work." *International Journal on Perceptive and Cognitive Computing* 9.1 (2023): 88-94.

[12] M. Fu et al., “Deep Learning in Automatic Sleep Staging With a Single Channel Electroencephalography,” Frontiers in Physiology, vol. 12, Mar. 2021, doi: https://doi.org/10.3389/fphys.2021.628502.

[13] M. Klug and K. Gramann, “ Identifying key factors for improving ICA - based decomposition of EEG data in mobile and stationary experiments,” European Journal of Neuroscience, vol. 54, no. 12, pp. 8406 – 8420, Oct. 2020, doi: https://doi.org/10.1111/ejn.14992.

[14] M. Khan and H. Al-Jahdali, “The consequences of sleep deprivation on cognitive performance,” King Abdullah International Medical Research Center, vol. 28, no. 2, pp. 91–99, Apr. 2023, doi: https://doi.org/10.17712/nsj.2023.2.20220108.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.487

Design and Development of a Requirements Conformance Tool (RCT)

Siti Syara Aiman Seh Wali, Azlin Nordin

Department of Computer Science (DCS), Kulliyyah of Information and Communication Technology (KICT), International Islamic University Malaysia (IIUM), 53100 Gombak Kuala Lumpur, Malaysia

*Corresponding author: azlinnordin@iium.edu.my
(Received: 29th June 2024; Accepted: 25th July 2024; Published on-line: 30th July 2024)

Abstract— To guarantee that a quality requirement is well-defined, it should meet various criteria, including completeness and unambiguousness. When a requirement statement is manually written, the quality of the requirements could be affected because the majority of requirements engineers particularly the inexperienced ones, have not been adequately trained. If they are unable to transfer stakeholders' needs into the requirements, they may end up with problematic requirements. As a result, they may be unable to provide high-quality specification requirements as a reference throughout the software development process. To reduce this problem, standard boilerplates' formats were established as one of the solutions. Nevertheless, requirement engineers may still require guidance in order to adopt any boilerplates that suit their needs. In this project, we seek to increase the quality of requirements by assisting requirement engineers in comprehending boilerplates. The Requirements Conformance Tool, which uses semi-automated boilerplates, was created to help requirements engineers determine whether the requirement conforms to the chosen requirements boilerplate or not. To show the use of boilerplates, the project was constructed in Java using basic Part-of-Speech (POS) tagger.

Keywords— boilerplates, ambiguity, requirements, conformance, software development, semi-automated

I. Introduction

Before developing a project, it is crucial to write requirements to specify what should be implemented. Requirements Engineering (RE) is described as the process involved in developing the system requirements [1] which describe how a system should behave, application domain information, obstacles on the operation of the system or the specifications of the system attribute. Requirements have also been described as [2]:

- A situation or functionality needed by a user to solve a hassle or gain a goal.
- A situation or functionality that needs to be met or possessed by a system or system component to satisfy a formally imposed document.
- A documented representation of a condition or capability as in (1) or (2).

The effect of the RE on successful and customer-oriented system development cannot be disregarded. It has turned out to be the usual practice to supply the sources for RE [2]. Requirement engineers play an important role to ensure the system requirements specification is being written correctly. RE is performed to allow communication between the stakeholders and programmers. To avoid project failures, it is crucial to handle the requirements of a system carefully. Requirement of a system is written in a document called Software Requirement Specifications (SRS). SRS is an important document which contains a list of requirements, and it explains what the stakeholders' wants which are intended as a basis for developing the software design [3]. A good SRS has the capability to ensure that the system developed is successful and meets the real users' needs while being a cost-effective creation. A full requirement free from any errors are important for a successful system development.

The errors in SRS need to be discovered early during the writing requirement phase, or the cost to pay for the maintenance will be high. One of the challenging issues in the current software industry is that requirement engineers frequently develop incorrect requirements with possibilities of various requirements errors. Such issues could inherently lead to reducing the SRS quality.

The most common mistake is that the requirements are missing and not clearly formulated [3]. One of the ways to improve the quality of SRS is boilerplate [3]. Boilerplates or also known as the requirements template is a blueprint for the syntactic structure of individual requirements. In this research, we are focusing on two boilerplates which are IREB's boilerplates and Easy Approach to Requirements Syntax (EARS) boilerplates.

https://doi.org/10.31436/ijpcc.v10i2.487

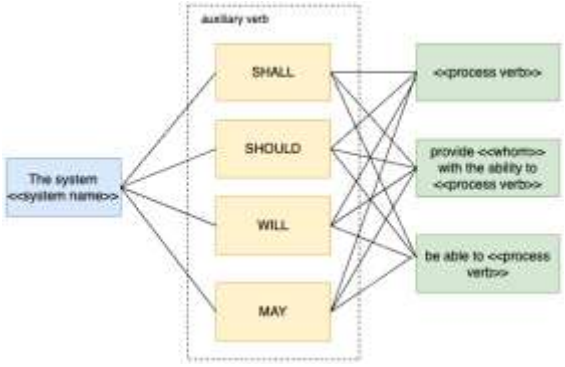

Fig. 1 Core requirement for IREB Boilerplate [2]

The International Requirement Engineering Board IREB) has come up with a step-by-step explanation of the correct approach of the requirement template. See Figure 1. It is also called Rupp's boilerplate. IREB boilerplates have three basic templates [2]. The first one is for the autonomous system activity where the users do not interact with the activity. The template is: THE SYSTEM SHALL/SHOULD/WILL/MAY <process verb>.

The second template is for the user interaction where the system provides a functionality to the user which requires them to interact with the system. The template is: THE SYSTEM SHALL/SHOULD/WILL/MAY provide <whom?> with the ability to <process verb>.

Finally, the third template is meant for interface requirements where the system is performing an activity, and it depends on the neighbouring system. The template is: THE SYSTEM SHALL/SHOULD/WILL/MAY be able to <process verb>.

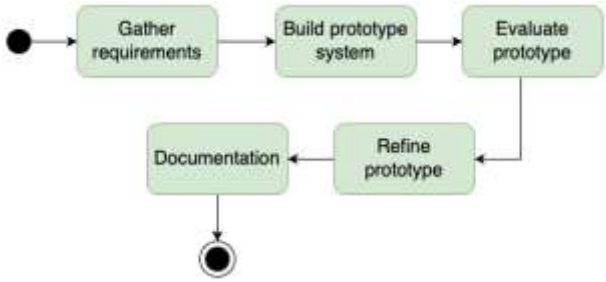

Fig. 2 Core requirements for EARS Boilerplate

In this research, there are six phases in this model. The first phase is to gather the requirements. All the information needed is collected and analysed through literature review. There are two tools that have been discovered in the process of collecting data which is the SRS tool [6] and Rubric tool [7]. The next phase is building the prototype. Once the team has finished the research on how to improve the quality of boilerplates, the prototype will be built.

The prototype is built using Java Eclipse where it focuses on creating new requirements and improving the existing requirements. The third phase is evaluating the prototype. The prototype is evaluated by making sure that it is functioning before it is shown to the supervisor. The supervisor will provide the feedback required to further improve the prototype which marks the fourth phase of this model. The fifth phase is where the feedback is taken into account, and improvements will be made to refine the prototype. The last phase is documentation. If there are no more alterations to be made, the prototype will be documented in a report.

II. LITERATURE REVIEW

In this paper, we analyzed two of the study papers that discussed requirement tools used to improve the quality of requirements. The papers are:

A. *Software Requirements Specification Tools*

The SRS tool focuses on requirement management feature. The tool provides the functionalities such as generating the requirements based on the boilerplates and modifying the boilerplate to the desired format where the user will be given the option to choose.

B. *RUBRIC*

Rubric Tool is a natural language processing (NLP) tool for automatic checking of conformance to the requirement boilerplates. Besides, the tool can also detect the problematic constructs in natural language requirements (see Figure 3).

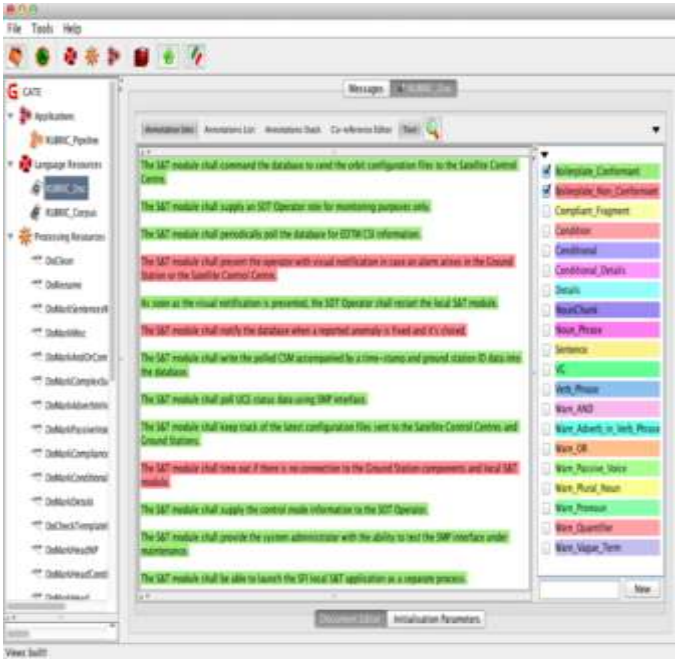

Fig. 3 RUBRIC [7]

https://doi.org/10.31436/ijpcc.v10i2.487

Based on the comparison in Table 1, we analyzed two existing tools. This is because these tools are in line with our tool. The chosen tools are Software Requirements Specification Tool [6] and RUBRIC Tool [7]. However, the Specification Tool is not published yet. After reviewing the three tools, we made a simple comparison between them as well as our proposed tool, Requirement Conformance Tool (RCT).

TABLE I
COMPARISON BETWEEN EXISTING TOOLS AND PROTOTYPE

Aspect	**Tools**		
	SRS Tool [6]	**Rubric Tool [7]**	**RCT Tool**
Requirement specification approach	Any boilerplate	IREB Boilerplate	IREB Boilerplate
Import requirement from text file	No	No	Yes
Export Requirement	Yes	No	Yes
Guiding in writing requirement	No	No	Yes
Support functional and non-functional requirements	Yes	Yes	Yes

For our tool, we focused on guiding requirement engineers to generate requirement statements so that they will not mistakenly use wrong words or structure. From the above comparison, it is observed that all the required engineering tools are using boilerplates. Nonetheless, the features and focuses provided in each of the tools are different.

In summary, our tool allows requirement engineers to export the generated requirements and also import the existing requirements to test whether the requirements are conformant to the boilerplate or not, which is an added advantage for our tool. As a future enhancement, the tool may include various existing templates, such as EARS boilerplates, to assist in producing requirements. This method could make the tool more adaptable to its users.

III. TOOL OVERVIEW

Prior to categorizing the requirement according to the IREB boilerplate, a set of possible rules of POS tag for each requirement statement have been studied and developed. Based on existing literature on the boilerplates and its structures, we derived the respective rules in Table 2. These rules highly depend on the three categories of the boilerplates i.e. (1) requirements for system activity, (2) requirements for user interaction, or (3) requirements for interface. For each of these categories, it will be used to detect different patterns for the conformance matching algorithm.

TABLE 2
RULES DEVELOPED TO CATEGORIZED REQUIREMENTS

User
DT(.*)MDVBDT(.*)INDTNNTOVB(.*)
Interface
DT(.*)MDVBJJTOVB(.*)
System
DT(.*)MDVB(.*)

In this table, (.*) (.*) can be NN, NNP, NNS, NNNNP, NNPNN and (.*) can be any part-of-speech tags based on what the requirement engineer chooses to write. The list of part-of-speech tags used are summarized as below.

TABLE 3
ABBREVIATIONS USED IN RULES

POSTAGGER	CATEGORY
DT	Determiner
NN	Noun, singular or mass
NNP	Proper noun, singular
NNS	Noun, plural
MD	Modal
VB	Verb, base form
IN	Preposition or subordinating conjunction
TO	To
JJ	Adjective

Figure 4 provides an overview of the process implemented in RCT. The process consists of three main steps: (1) Text Splitting, (2) POS Tagger to identify the tag meaning of each word, (3) Structure checking, and (4) Boilerplate Conformance Checking. In the first step, requirement statements are read in line and segmented into

https://doi.org/10.31436/ijpcc.v10i2.487

constituent parts (noun phrases, verb phrases, etc.) and annotated with appropriate tags by using POS Tagger.

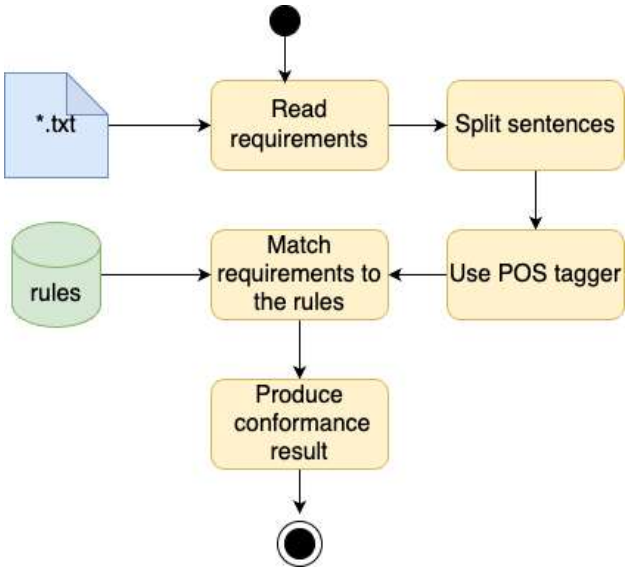

Fig. 4 Process in RCT

The annotated requirements, along with the IREB boilerplates' syntax grammar rules and structure checking are used in the next step to produce requirements that are conformant to the boilerplates results based on the position of the part-of-speech tags in the array.

IV. ANALYSIS AND DESIGN ALGORITHM FOR RCT

This section describes the algorithm used in identifying the conformance of the requirements to the chosen boilerplate template. In this approach (as can be seen in Figure 5), an abbreviated requirement array signifies that each statement is pushed into a three-dimensional array and placed in the first array. The location of the abbreviation indicates that each word of the sentence will be pushed into the second array. The third array will be populated with the position of the string modal verb array, with each word segmented using POS tagger. If the requirements satisfy the rules, they will be described as conforming to the boilerplates; otherwise, they will be stated as a faulty or non-compliance requirement, with an indication of which segment of the requirement source.

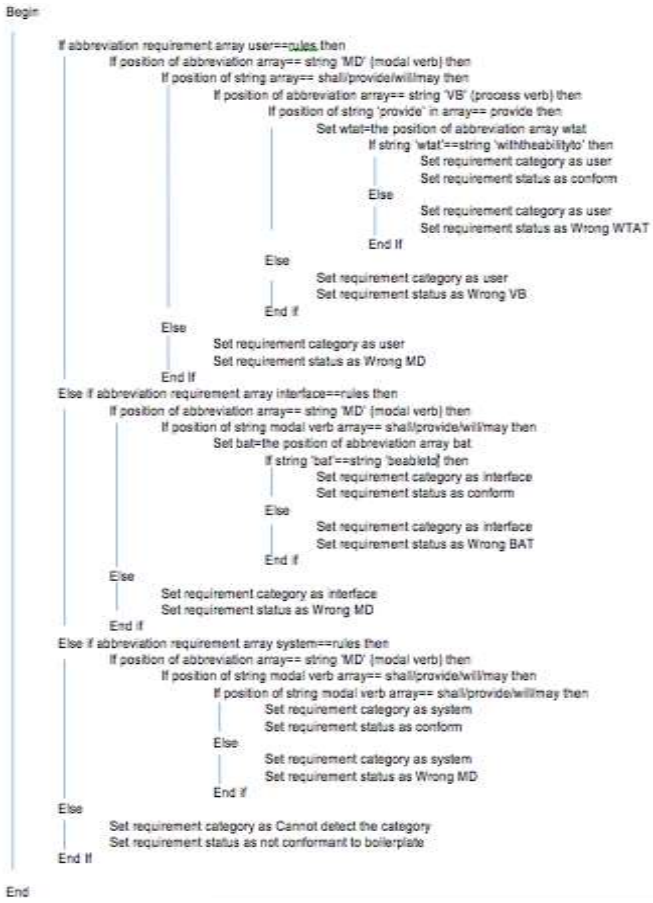

Fig. 5 Algorithm for Matching Requirements

V. RCT PROTOTYPE

This section elaborates a few of the snapshots of the RCT prototype. The screen shot in Figure 6 shows the RCT's main page where requirement engineers can choose to generate new requirements or to import existing requirements from the text files. Additionally, the requirement engineer should enter the project name before they want to write the requirements.

Fig. 6 Boilerplates Option

https://doi.org/10.31436/ijpcc.v10i2.487

The screen in Figure 7 shows the boilerplates option that requirement engineers can choose before writing the requirements. When they choose this feature, they will be able to pick any of these options i.e. (1) requirements for system activity, (2) requirements for user interaction, or (3) requirements for interface. Each of these options will lead into different requirements boilerplates.

Fig. 7 Generate Requirements

The subsequent Figure 8 demonstrates the fields that the requirement engineer should enter in order to generate the requirement based on the chosen boilerplate. This include the option for system name, auxiliary verb and the process verb. The typical process for defining project requirements is for project managers to decide ahead of time what kind of auxiliary verbs will be used and what they will signify. For example, in this Software Requirements Specification (SRS) sample in [9], the authors define the following auxiliary terms:

1. 'Must'- indicates requirements strictly to be followed to conform to the document and no deviation is allowed. Must is synonymous with "shall."
2. 'Should'- indicates that a possibility among a set of possibilities is recommended as particularly suitable
3. 'May' - indicates a course of action permissible within the limits of the document.

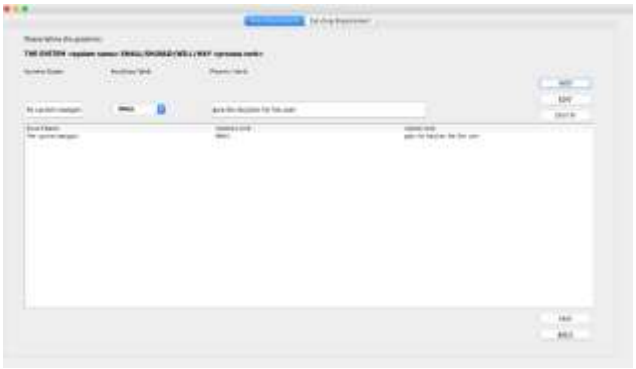

Fig. 8 Adding Requirements

Figure 9 shows the requirement is added to the table. The requirement engineers are able to add more requirements, edit, and delete the requirements by interacting with the respective buttons.

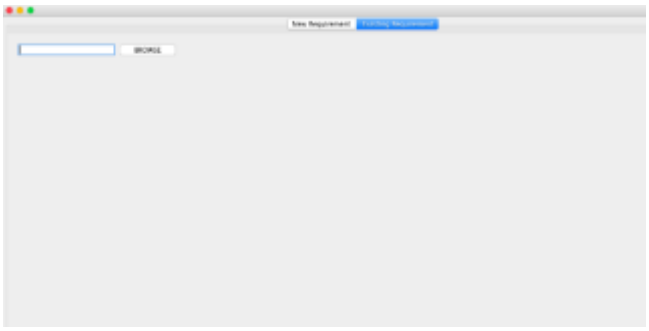

Fig.9 Upload Existing Requirement from Text File

Figure 9 depicts when the requirement engineers choose to import an existing requirement file. The requirements engineer could browse and import the text file to the tool. Based on the tool's process as depicted in Fig. 4, the result will display if the requirements conform to the boilerplates or not.

VI. IMPLEMENTATION

The Requirement Conformance Tool (RCT) was created using the Java programming language and includes a part-of-speech (POS) tagger for analyzing language components. However, the prototype has a few drawbacks. It is currently limited to IREB boilerplates and only considers the syntactic structure of requirements, not their semantic content. Furthermore, the tool requires conformance to a specified template for requirement creation prior to importing text files, and it runs as a standalone application rather than a web-based platform. This indicates that the tool is a standalone solution that cannot benefit from the web-based implementation's features, such as accessibility and collaboration.

VII. CONCLUSION

This tool provided guidance for the users to assist them in producing quality requirements using requirements boilerplates. Nonetheless, the current implementation supports only IREB boilerplate but in the future, this project is expected to generalize the tool to include other types of boilerplates as well. RCT aims to distinguish which existing requirement that has been written is conformed to the IREB boilerplate.

The challenge with the prototype is that the team lacks NLP skills, which has made it difficult to code the tool by utilizing the text chunking pipeline. The text chunking pipeline includes a tokenizer, a sentence splitter, a POS tagger, Named Entity Recognition, and an NP chunker.

This coding was completed in a restricted amount of time, thus the team devised an alternative method that uses only available JAVA libraries and imports only POS tagger libraries. This research effort has been a learning process, with many new discoveries. In addition, another limitation of this work is that the tool has not been validated for its usefulness, and its applicability. We plan to further evaluate this tool to the relevant potential users and get their feedback for future improvement.

ACKNOWLEDGMENT

The authors would like to extend our appreciation to the Kulliyyah of Information and Communication Technology (KICT), International Islamic University Malaysia (IIUM) as well as the Computer Science Department for the opportunity to work for this project.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

REFERENCES

[1] G. Kotonya., & I. Sommerville, *Requirements engineering: processes and techniques*. Wiley Publishing. 1998.

[2] K. Pohl. *Requirements engineering: fundamentals, principles, and techniques*. Springer Publishing Company, Incorporated. 2010.

[3] U. Anuar, S. Ahmad, & N.A. Emran. A simplified systematic literature review: Improving Software Requirements Specification quality with boilerplates. In *Software Engineering Conference (MySEC), 2015 9th Malaysian* (pp. 99-105). IEEE.

[4] C. Arora, Sabetzadeh, M., Briand, L. C., & Zimmer, F.. Requirement boilerplates: Transition from manually-enforced to automatically-verifiable natural language patterns. In *Requirements Patterns (RePa), 2014 IEEE 4th International Workshop on* (pp. 1-8). IEEE.

[5] R.S. Weinberg. Prototyping and the systems development life cycle. *Information System Management*, *8*(2), 1991, 47-53.

[6] K. Meng Y. Yeow "*Software Requirement Specification Tool.*" in Final Year Project report, pp. 29-30, 2016

[7] C. Arora, Sabetzadeh, M., Briand, L., Zimmer, F., & Gnaga, R. (2013, August). RUBRIC: A flexible tool for automated checking of conformance to requirement boilerplates. In *Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering* (pp. 599-602). ACM.

[8] R.A. Carter, A.I. Antón, A. Dagnino, & L. Williams,. Evolving beyond requirements creep: a risk-based evolutionary prototyping model. In *Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on* (pp. 94-101). IEEE.

[9] T. Hedberg Jr., M. Helu, and M. Newrock. (2017). 'Software requirements specification to distribute manufacturing data', National Institute of Standards and Technology, Gaithersburg, MD, NIST AMS 300-2, Dec. 2017. doi: 10.6028/NIST.AMS.300-2.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.455

Brain Tumour Classification Using Vanilla Convolutional Neural Networks

Md Najmul Huda, Akeem Olowolayemo, Ayesha Dupe Adeleye, Amin Nur Rashid, Abrar Habib Haque
Department of Computer Science, Kulliyyah of Information & Communication Technology, International Islamic University, Malaysia

*Corresponding author akeem@iium.edu.my
(Received: 20th February2024; Accepted: 8th June 2024; Published on-line: 30th July 2024)

Abstract— Brain tumours are a common and dangerous type of malignant tumour that, if not detected early enough, can cut short a patient's life. The segmentation and classification of brain tumours using solely traditional medical image processing is a difficult and time-consuming task. Various imaging modalities, such as Computed Tomography (CT), Magnetic Resonance Imaging (MRI), and ultrasound image, are frequently utilized to assess brain, lung, liver, breast, prostate and other tumours. MRI images are specifically utilised in these analyses to detect brain tumours. As a result, developing approaches for detecting, recognizing, and classifying the conditions based on image analysis becomes essential. A comprehensive and automatic classification system is important to saving human lives. The geographical and anatomical heterogeneity of brain tumours makes automatic categorization challenging. This study proposes an automated method for detecting brain tumours using Convolutional Neural Networks (CNNs) classification, with the primary goal of developing a deep learning model that is capable of accurately identifying and classifying images as either having a brain tumour or not. In this paper, we provide a classification model for brain tumours based on a Deep Convolutional Neural Network with a vanilla neural network technique. The proposed method's performance on a publicly available dataset of 3000 Brain MRI Images yielded superior results, with accuracy and F1 score of 98.00 percent and 98.00 percent, respectively. This study shows that the proposed vanilla-CNN model can be used to make it easier for brain tumours to be automatically classified.

Keywords— Brain tumour, CNN, Classification, Deep learning, MRI, Vanilla-CNN.

I. Introduction

The brain is one of the most sensitive organs in human body, controlling the body's main functions and traits. According to the most recent data from the World Health Organization (WHO), brain tumours are one of the most common types of cancer that kill people around the world. Brain tumours may be malignant or benign. Gravity within the skull might hasten the growth of a brain tumour. In the worst-case scenario, it can induce brain damage, which can be deadly. Cancer of the brain and nerve system is the tenth highest cause of mortality in both men and women. This year, primary brain and CNS tumours are expected to kill 18,280 adults in the United States (10,710 men and 7,570 women) and in 2020, an estimated 251,329 persons worldwide are expected to die from primary brain and CNS cancers [1]. A malignant tumour is dangerous and can lead to death. Based on their characteristics, the WHO divides brain tumours into grade 1 and 2 tumours, which are low-grade tumours also known as benign tumours, and grade 3 and 4 tumours, which are high-grade tumours also known as malignant tumours [2].

Several techniques are used to diagnose a brain tumour, including CT scans and EEGs, but the most effective and extensively used method is magnetic resource imaging (MRI). Radio waves and strong magnetic fields are used in MRI to make images of the organs inside of the body. MRI delivers more comprehensive information about interior organs than CT or EEG scans, consequently it is more effective. It has been shown that there is no universal system for detecting and segmenting brain tumours independent of their location, shape, or intensity [3]. Recent research has presented several algorithms for the feature extraction and categorization of brain cancers. The grey-level co-occurrence matrix (GLCM) [4],[5] is a popular tool for extracting low-level characteristics. Conventional brain tumour classification approaches typically include region-based tumour segmentation before feature extraction and classification, which has outstanding performance for both 2D and 3D medical imaging [6],[7]. We proposed developing a deep learning model for classifying MRI images containing brain tumours into "Tumour" or "Non-tumour" in this research. We also look at how well the proposed model works in terms of accuracy and high F1-score.

II. Related Work

Classifying brain tumours into subtypes is a challenging research problem. Recent work on automated medical diagnosis improves performances because of the arrival of deep learning concepts. Deep learning techniques have

https://doi.org/10.31436/ijpcc.v10i2.455

been broadly used in medical image analysis for cancer diseases and cancer diagnosis [1]. Zuo et al. [2] developed a deep learning algorithm for human skin detection, which is a part of dermatology diagnostics. Charron et al. [3] used a deep convolutional neural network (CNN) to monitor brain metastases. More recently, a particular class of deep learning, known as deep transfer learning, has dominated the studies on visual categorization, object recognition, and image classification problems [4]. Transfer learning allows using a pre-trained CNN model, which was developed for another related application to be utilised for another classification problem set. Transfer learning has shown its potential in CAD of medical problems also. Zhou et al.[5] used a pre-trained InceptionV3 model for differentiating benign and malignant renal tumours on CT images. Deniz et al. [6] proposed a classifier for breast cancer on histopathologic images. The authors used a pre-trained VGG-16 model and a fine-tuned AlexNet for extracting features, which were then classified using a support vector machine (SVM). Hussein et al. [7] introduced a learning model for lung tumour characterization and pancreatic tumour characterization. The learning model was based on knowledge transfer and had a 3D CNN architecture. The accuracy measures reported in the transfer learning-based algorithms were superior to those obtained using handcrafted algorithms. Specifically, transfer learning has gathered attention in applications related to neuro-oncology. Studies were conducted to extract deep features from brain MRI images using pre-trained networks [8], [9]. The studies showed the capability of transfer learning to work with smaller datasets. Yang et al. [10] used AlexNet and GoogLeNet in their research work on the grading of glioma from MRI images. Regarding the performance measures observed, GoogleNet proved superior to AlexNet for the task. Talo et al. [11] achieved remarkable classification performance with deep transfer learning in their work on brain abnormality classification. The authors used ResNet-34, and the experiments included training of modified dense layers, training with data augmentation, and fine-tuning of a transfer learning model. The experimental results concluded that a deep transfer learned model could be adapted to medical image classification with minimum pre-processing. Jain et al. [12] used a pre-trained VGG-16 network to diagnose Alzheimer's disease from MRI. Transfer learning was applied to content-based image retrieval (CBIR) for brain tumours [13]. The evaluation was performed on a publicly available dataset and obtained promising results.

The digital image processing community has developed several segmentation methods, many of them ad hoc. The four most common methods are 1.) amplitude thresholding; 2.) texture segmentation; 3.) template matching and 4.) region-growing segmentation. These types of procedures are used for dividing the brain images into three categories: (a) Pixel-based, (b) Region or Texture Based (c) Structural based. Based on the region obtained, the required information is extracted. Different researchers proposed different methods and algorithms for detecting brain tumours, stroke, and other abnormalities in the human brain using MRI.

A. *Brain Tumour Classification in Medical Imaging*

A brain tumour is one of the most complex disorders that occurs when the brain cells begin to grow uncontrollably. The most crucial issue before starting treatment is detecting and classifying tumours from brain magnetic resonance imaging (MRI) scans. For ages, researchers have worked hard to develop the best approach for real-life medical image recognition with greater precision. The current manual approach is inconvenient, time-consuming, and human error-prone. These flaws emphasize the significance of establishing a fully automated deep learning-based brain tumour classification approach. The task of brain tumour classification in medical imaging has been a prominent area of research due to its critical implications for diagnosis and treatment planning. Early efforts primarily relied on traditional image processing techniques and manual feature extraction. Studies such as [13] demonstrated the effectiveness of these methods but were limited by their dependence on handcrafted features and the challenges posed by the complex and diverse nature of brain tumour images.

B. *Deep Learning in Medical Image Analysis*

In recent years, the advent of deep learning has revolutionized medical image analysis. Convolutional Neural Networks (CNNs) have shown remarkable success in various tasks, including image classification, segmentation, and detection. Researchers have applied CNNs to brain tumour classification with notable achievements. For instance, the study in [14] proposed a deep learning model that outperformed traditional methods by automatically learning hierarchical features from MRI images.

Recent research shows that the deep learning methods perform well on image classification tasks and provide better accuracy than machine learning methods. Deep learning is that subset of machine learning which do not require manual feature extraction, which is an added advantage to such techniques. Paul et.al had developed a generalized method for brain tumour classification using fully connected neural networks that achieved an accuracy of 91.43% [8]. Brats-2013 is the benchmark dataset used by most of the researchers. Later, various CNN-based methods for classification of brain tumour were proposed. In one such method, three types of tumours: Meningioma, Glioma, and Pituitary tumours were classified, which yielded the

https://doi.org/10.31436/ijpcc.v10i2.455

classification accuracy of 97.3% [9]. In another work, the CNN based approach tried on three different datasets and after data augmentation using Deep CNN, it yielded 95.23% for Meningioma, 95.43% for Glioma, and 98.43% accuracy for Pituitary tumour [15].

C. MRI-Based Brain Tumour Classification

Several studies have specifically focused on utilizing Magnetic Resonance Imaging (MRI) for brain tumour classification. [16] explored the use of advanced MRI sequences, such as diffusion-weighted imaging, in conjunction with deep learning to improve classification accuracy. In recent years, an enormous number of approaches to brain tumour classification on MRI brain images have been proposed based on deep transfer learning models. CNN was realized as the first real-world application in 1998 to observe handwritten digits. Also [17] developed a hybrid model based on CNN for classifying the tumour type in the brain. The study in [16] proposed an automated brain tumour detection mechanism applying CNN with transfer learning models on the MRI brain image dataset. The effect of MRI image data preprocessing steps analysed by authors improves the classification accuracy in predicting brain tumour disease. Researchers focused on developing a new CNN-based model to classify the three forms of tumours that existed in brain MRI images. The study in [16] investigated presenting a CNN pretrained model with image segmentation techniques. The authors in [18] suggested a VGG-16 pretrained CNN model for the classification of multigrade brain tumours. ImageNet Large-Scale Visual Recognition Challenge (ILSVRC), a visual database project, was launched by ImageNet in 2010. This challenge provides a platform for many researchers to analyse the performance of proposed methodologies developed on the given image dataset and obtain a higher classification accuracy rate. Equally, the study in [15] proposed CNN architecture AlexNet to achieve good results on various tasks based on visual recognition. Meanwhile, [13] investigated the fusion of multiple MRI modalities for a comprehensive understanding of tumour characteristics.

D. Vanilla Convolutional Neural Networks

While sophisticated architectures like U-Net and ResNet have been widely employed in medical image analysis, the use of vanilla CNNs for brain tumour classification has gained considerable attention. Vanilla CNNs, with their simpler structures, offer advantages in terms of interpretability and computational efficiency. The study in [19] demonstrated the efficacy of a vanilla CNN in brain tumour classification, paving the way for exploring less complex architectures. Vanilla neural networks are termed as an extension to linear regression supervised algorithm. Vanilla neural networks are similar to other linear regression and just differ in their hidden layers which plays a major role as all the extra computations in vanilla neural networks work in the hidden layer. The hidden layer, denoted with H, has three "neurons" (H_0, H_1, H_2) and any number of neurons can be added in hidden layers. With hidden layer, backpropagation algorithm can be used in Vanilla neural network [19].

E. Challenges and Future Directions

Despite the progress made in brain tumour classification, challenges such as limited annotated datasets, class imbalance, and interpretability persist. Recently, researchers have focused their attention to automating the feature extraction process and standardizing the networks by exploring the scope of CNNs and Transfer Learning in the field. All these techniques extract features of individual images in an automated fashion, but they lack the ability to learn the image level relationships or the pixel-to-pixel relationships. This creates a scope for adding a novel step in feature extraction, that is to explore pixel-pixel relationships. The motivation and objective of this research is to devise a mechanism to account for the pixel-based relationships and to create a relation-aware representation for Brain tumour classification. Relation aware representation uses the relationships amongst the data points as a knowledge base for effective learning of the model. Future research should address these challenges and explore novel techniques, potentially integrating domain knowledge and multi-modal information to further improve the accuracy and robustness of the classification models.

III. Proposed Methodology

CNN has recently been popular in a variety of medical image processing applications, particularly in the classification and segmentation of MRI brain tumours. In this paper, a new CNN model is proposed for classifying brain tumours.

In this study, we developed a basic CNN model and used it to extract augmented MRI image data of 512 x 512 input size with RGB Colour channels and a batch size of 64. The important feature is pulled out by using four convolutional layers. 4 x 4 filters are used in each convolutional layer and 4 x 4 are used in the pooling layers. A modest number of filters are utilised to detect edges, corners, and lines. Then, a max-pooling layer was applied to the image in order to produce the most comprehensive summary possible. Finally, we used a 256-neuron fully connected dense layer with a SoftMax output layer to compute the probability score for each class and classify the final decision labels as Yes or No, depending on whether the input MRI image contains cancer or not. The layout of our suggested CNN architecture is shown in Figure (1).

https://doi.org/10.31436/ijpcc.v10i2.455

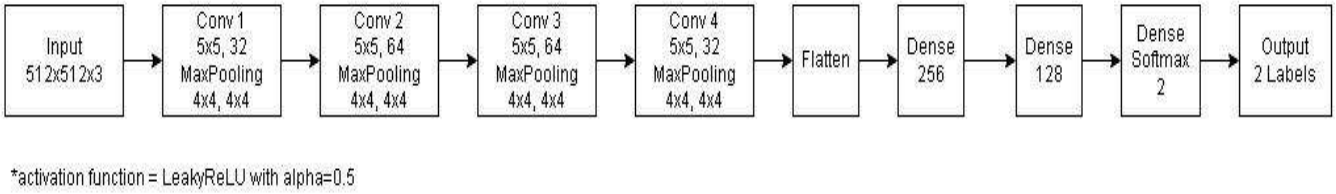

Fig. 1 The proposed Convolutional Neural Network Architecture.

A. Convolution Layer

This layer is the most significant and core component of the CNN model, and it is also where the name "Convolution Neural Network" comes from. A CNN's fundamental design consists of many convolutional layers, pooling layers, and fully connected layers [8]. The convolution layer's job is to figure out which of the existing layer's features correspond to the various kinds of local connections.

B. Non-linearity Layer

The non-linearity layer represents the second layer of the model. CNN is made better at fitting by adding the nonlinear factor. Activation functions such as Sigmoid, ReLU, leaky ReLU, and ELU are used to do this. To evaluate the CNN's classification performance and learning speed, the leaky ReLU function was chosen as the activation function. The expression is (Equation 1), where x is the input value.

$$f(x) = \begin{cases} 0.01x \ for \ x < 0 \\ x \ for \ x \geq 0 \end{cases} \quad (1)$$

C. Pooling Layer

The pooling layer is responsible for combining related features in order to reduce the precision of feature maps [9]. The dimension of feature maps is lowered in the suggested model by using the MaxPooling operation, which is simple to use and produces the best results.

D. Fully Connected Layer (FC)

The fully connected layer (FC) works with a flattened input, which means that each input is coupled to every neuron. At the network's end, the FC layer is used. The goal of this layer is to flatten the output of the preceding layer because the features must be one-dimensional (1D) data before training with the classifier. The output is fixed as the number of classes used when it is used as the last layer [10].

E. Optimization

In deep neural networks, we use a variety of optimization techniques to minimize the loss by modifying parameters such as weights and learning rates. In this experiment, the 'adam' optimizer proposed by Diederik Kingma [11] is utilised. The stochastic gradient descent principle is used in the learning process to provide a strategy for stochastic optimization. Because it can handle sparse gradients on noisy situations, the 'Adam' optimizer, which stands for adaptive moment estimation, was chosen.

F. Performance Measure

F1-score accuracy was employed in this study. The F1-score considers both recall and precision. Recall and accuracy are averaged together to get an F1-score. If the dataset has a good balance of recall (R) and precision (P), the F1-score is the best. The formulas for determining these performance measures are shown in Equations 2 through 5:

$$Accuracy = \frac{TP+TN}{(TP+TN+FP+FN)} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

$$F1\ Score = 2 \times \frac{Recall \times Precision}{Recall+Precision} \quad (5)$$

where TP stands for True Positive, TN stands for True Negative, FP stands for False Positive, and FN is for False Negative. These characteristics are calculated using the confusion matrix, which contains information on the incorrect and correct classification of images across all categories.

G. Image Data

Publicly available dataset is imported from Kaggle website [12]. It consists of 3000 images, 1500 of which are MRIs of the brain that have tumours and 1500 of which do not contain tumours.

https://doi.org/10.31436/ijpcc.v10i2.455

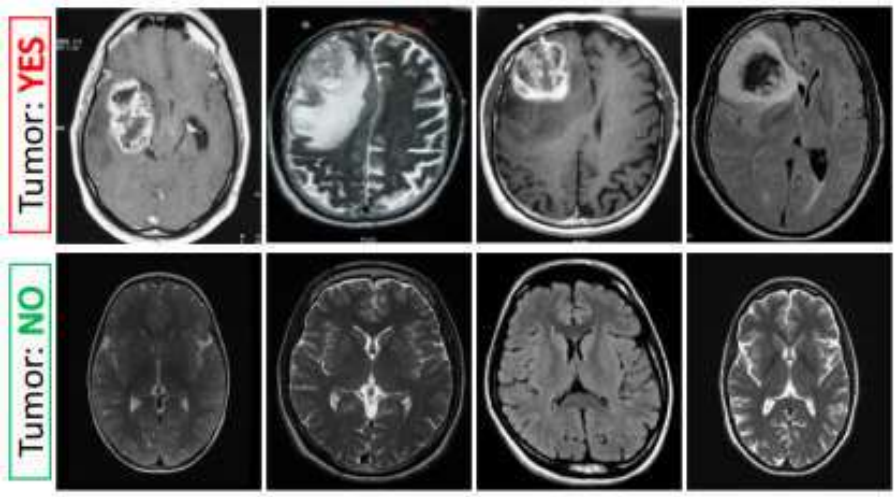

Fig. 2 Dataset examples[20].

IV. Results and Discussion

MRI scans of tumours and non-tumours are included in our dataset. We divided our data into three categories: training, validation, and testing. There are 80% images for training, 10% for validation, and 10% for testing to determine the accuracy of our model. With a batch size of 64, we trained the models for 25 epochs. Our proposed model demonstrated a 98 percent accuracy rate on both our Training and Validation on our datasets.

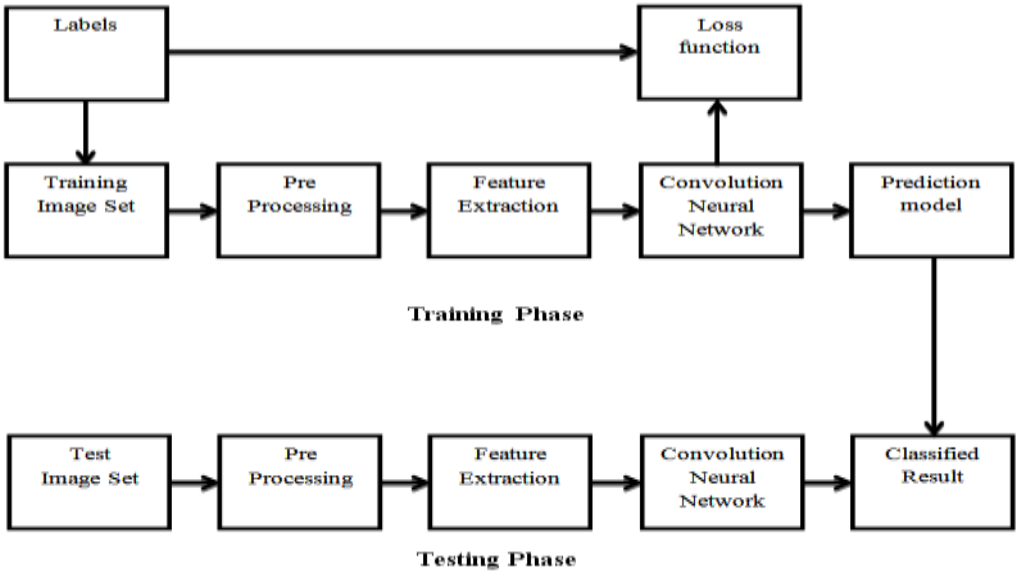

Fig. 3 Block diagram for brain tumour classification using CNN.

Figure 4 shows the Model Accuracy and Model Loss of the proposed Model. The time of computation and complexity is low, and an accuracy is high.

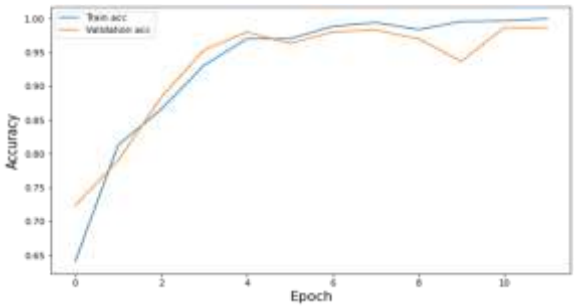

Fig. 4 Model Accuracy.

https://doi.org/10.31436/ijpcc.v10i2.455

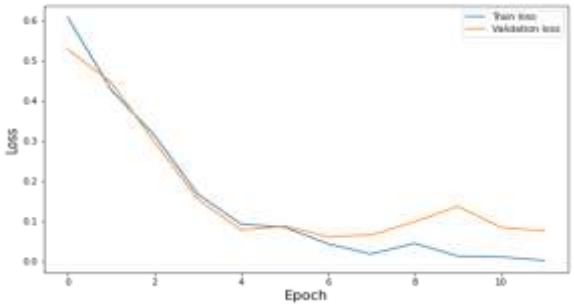

Fig. 5 Model Loss.

We evaluated our model on unseen testing data. As shown in Fig. 5, True Positive and True Negative show the correct way to classify, with TP showing abnormal brain images as positive and TN showing normal brain images as positive. False Positive and False Negative, on the other hand, show the incorrect way to classify, with FP showing normal brain images as positive tumours and FN showing abnormal brain images as negative tumours.

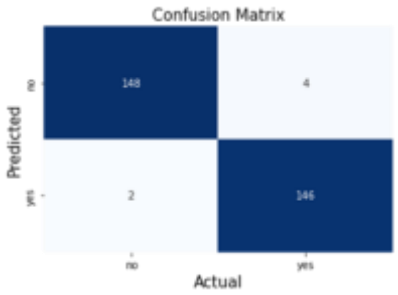

Fig. 6 Model Loss.

The algorithm is slightly better at predicting true negatives than true positives, according to the confusion matrix.

Classes	Precision	Recall	F1 Score	Support
Yes (Tumorous)	0.99	0.97	0.98	150
No (Non-Tumorous)	0.97	0.99	0.98	150

Fig. 7 Classification report.

All it is more crucial for a classifier to classify abnormalities than a normal case from a medical standpoint. Both tumourous and non-tumourous labels in this report had the same precision, recall, and F1-score classification metric values. This demonstrates that the model is functioning effectively while maintaining a high level of accuracy.

V. Conclusions

In this research, we employed the Vanilla CNN model to classify MRI brain tumours. Our model makes use of many layers of varying sizes as well as the SoftMax classifier. The proposed technique's experimental investigation is based on publicly available datasets, as previously mentioned. The architecture's training and validation accuracy achieved a remarkable 98.00 percent performance. This high accuracy underscores the superior performance of the proposed technique based on the Vanilla CNN model. It is hoped that utilizing this technique may aid in the early detection of brain tumours before they cause physical complications such as paralysis, other impairments, or death.

Future studies in this work would focus utilizing images from other modalities and improving deep network topologies by incorporating a multi-channel classifier that significantly increases classification performance. We equally hope to include different classifications of tumors rather than just tumour or no-tumour identification

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] "Brain Tumor: Statistics | Cancer.Net." Accessed: Jun. 19, 2022. [Online]. Available: https://www.cancer.net/cancer-types/brain-tumor/statistics

[2] "Brain tumours - NHS." Accessed: Jun. 19, 2022. [Online]. Available: https://www.nhs.uk/conditions/brain-tumours/

[3] N. Abiwinanda, M. Hanif, S. T. Hesaputra, A. Handayani, and T. R. Mengko, "Brain tumor classification using convolutional neural network," *IFMBE Proc*, vol. 68, no. 1, pp. 183–189, 2019, doi: 10.1007/978-981-10-9035-6_33.

[4] Q. T. Ostrom *et al.*, "American Brain Tumor Association Adolescent and Young Adult Primary Brain and Central Nervous System Tumors Diagnosed in the United States in 2008-2012," *Neuro Oncol*, vol. 18, pp. i1–i50, 2015, doi: 10.1093/neuonc/nov297.

[5] N. Gordillo, E. Montseny, and P. Sobrevilla, "State of the art survey on MRI brain tumor segmentation," *Magn Reson Imaging*, vol. 31, no. 8, pp. 1426–1438, 2013, doi: 10.1016/j.mri.2013.05.002.

[6] L. C. Chen, Y. Zhu, G. Papandreou, F. Schroff, and H. Adam, "Encoder-decoder with atrous separable convolution for semantic image segmentation," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11211 LNCS, pp. 833–851, 2018, doi: 10.1007/978-3-030-01234-2_49.

[7] F. Milletari, N. Navab, and S. A. Ahmadi, "V-Net: Fully convolutional neural networks for volumetric medical image segmentation," *Proceedings - 2016 4th International Conference on 3D Vision, 3DV 2016*, pp. 565–571, 2016, doi: 10.1109/3DV.2016.79.

[8] I. A. El Kader, G. Xu, Z. Shuai, S. Saminu, I. Javaid, and I. S. Ahmad, "Differential deep convolutional neural network model for brain tumor classification," *Brain Sci*, vol. 11, no. 3, 2021, doi: 10.3390/brainsci11030352.

[9] J. Yang, F. Xie, H. Fan, Z. Jiang, and J. Liu, "Classification for dermoscopy images using convolutional neural networks based on region average pooling," *IEEE Access*, vol. 6, pp. 65130–65138, 2018, doi: 10.1109/ACCESS.2018.2877587.

[10] W. Ayadi, W. Elhamzi, I. Charfi, and M. Atri, "Deep CNN for Brain Tumor Classification," *Neural Process Lett*, vol. 53, no. 1, pp. 671–700, 2021, doi: 10.1007/s11063-020-10398-2.

[11] D. P. Kingma and J. L. Ba, "Adam: A method for stochastic optimization," *3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings*, pp. 1–15, 2015.

[12] "Br35H :: Brain Tumor Detection 2020 | Kaggle." Accessed: Jun. 19, 2022. [Online]. Available: https://www.kaggle.com/datasets/ahmedhamadaa0/brain-tumor-detection

[13] T. Rahman and M. S. Islam, "MRI Brain Tumor Classification Using Deep Convolutional Neural Network," in *2022 International Conference on Innovations in Science, Engineering and Technology, ICISET 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 451–456. doi: 10.1109/ICISET54810.2022.9775817.

[14] H. A. Khan, W. Jue, M. Mushtaq, and M. U. Mushtaq, "Brain tumor classification in MRI image using convolutional neural network," *Mathematical Biosciences and Engineering*, vol. 17, no. 5, pp. 6203–6216, 2020, doi: 10.3934/MBE.2020328.

[15] S. Arora and M. Sharma, "Deep Learning for Brain Tumor Classification from MRI Images," in *Proceedings of the IEEE International Conference Image Information Processing*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 409–412. doi: 10.1109/ICIIP53038.2021.9702609.

[16] C. Srinivas *et al.*, "Deep Transfer Learning Approaches in Performance Analysis of Brain Tumor Classification Using MRI Images," *J Healthc Eng*, vol. 2022, 2022, doi: 10.1155/2022/3264367.

[17] S. Divya, A. Ali, N. Ibrahim, and L. Padma Suresh, "Automated Models for the Classification of Magnetic Resonance Brain Tumour Images," in *ICAC 2023 - 28th International Conference on Automation and Computing*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICAC57885.2023.10275235.

[18] M. Aamir *et al.*, "A deep learning approach for brain tumor classification using MRI images," *Computers and Electrical Engineering*, vol. 101, Jul. 2022, doi: 10.1016/j.compeleceng.2022.108105.

[19] M. Ravinder *et al.*, "Enhanced brain tumor classification using graph convolutional neural network architecture," *Sci Rep*, vol. 13, no. 1, Dec. 2023, doi: 10.1038/s41598-023-41407-8.

[20] Md. A. B. Siddique, S. Sakib, M. M. R. Khan, A. K. Tanzeem, M. Chowdhury, and N. Yasmin, "Deep Convolutional Neural Networks (CNN) based Brain Tumor Detection in Brain MRI Images," in *Proceedings - 5th International Conference on Smart Systems and Inventive Technology, ICSSIT 2023*, 2023, pp. 976–979. doi: 10.1109/ICSSIT55814.2023.10060968.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.488

Next-Generation Hotspot (NGH): Advancing Automatic Roaming and Seamless Wi-Fi Network Logins

Zainab S. Attarbashi[1], Atikah Balqis Binti Basri[1], and 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: 20th June 2024; Accepted: 8th July 2024; Published on-line: 30th July 2024)

Abstract— In an increasingly connected world, Wi-Fi hotspots play an important role in ensuring continuous and reliable internet access for users and devices. Next-Generation Hotspot (NGH) technology has been introduced to decrease the possibility of multiple authentications for users because it uses the network providers to exchange the user authentication and it will be the upgraded version of Hotspot 2.0. NGH addresses the growing challenges of Wi-Fi connectivity, such as network congestion, security vulnerabilities, and complex authentication processes. As the demand for wireless access increases, NGH uses advanced features like Passpoint standards and IEEE 802.1x protocols to offer seamless, one-time authentication across multiple networks. This article provides an overview of NGH, focusing on its ability to enhance user experience by simplifying login procedures and improving security. By investigating the limitations and reasons why this NGH technology is being used, as well as security-related topics that concern the user. It also explains the benefits of NGH, this research highlights its potential to revolutionize wireless communication, offering valuable insights for service providers and the network industry to optimize and innovate future Wi-Fi solutions.

Keywords— Next-Generation Hotspot, Passpoint, authentication, seamless WiFi.

I. Introduction

In the era where seamless connectivity is essential, the role of Wi-Fi hotspots has become increasingly critical in maintaining uninterrupted internet access for both users and devices. As the demand for reliable and widespread wireless connectivity continues to increase, Next-Generation Hotspot (NGH) [1] technology became as an important advancement that is building upon the existing Hotspot 2.0. NGH aims to address key challenges associated with Wi-Fi connectivity, such as network congestion, security vulnerabilities, and complex authentication processes.

The evolution of Wi-Fi technology emphasizes its growing importance and capability. From the early days of Wi-Fi 802.11b, which offered basic wireless connectivity, to the advent of Wi-Fi 5 (802.11ac) with its significant improvements in speed and capacity. The latest advancements, such as Wi-Fi 6 (802.11ax) and the emerging Wi-Fi 7 (802.11be), promise even greater enhancements in speed, efficiency, and handling of multiple devices as summarized in table 1.

However, the current technology is challenged by complex logins and limited roaming [2]. These limitations disrupt connectivity and restrict user experience, especially in areas with frequent network handovers. Complex logins require unnecessary input of complex passwords, wasting valuable time and disrupting user flow [1]. Traditional Wi-Fi networks function as isolated entities, requiring manual reconnection and re-authentication when transitioning between hotspots. This disrupts ongoing activities and decreases productivity, creating a disjointed experience.

TABLE I
Comparison between different WiFi technologies

Feature	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 7
Standard	802.11n	802.11ac	802.11ax	802.11be
Frequency Bands	2.4 GHz, 5 GHz	5 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz, 6 GHz
Max Speed	600 Mbps	3.5 Gbps	9.6 Gbps	30 Gbps
Channel Bandwidth	20, 40 MHz	20, 40, 80, 160 MHz	20, 40, 80, 160 MHz	20, 40, 80, 160, 320 MHz
MIMO	Up to 4x4	Up to 8x8	Up to 8x8	Up to 16x16
Latency	Higher	Lower	Lower	Lowest

Next-Generation Hotspot (NGH) addresses these limitations by introducing automatic roaming and seamless logins [3]. This is achieved through innovative technologies like WiFi certified Passpoint, which automatically connects users to authorized networks without manual logins.

https://doi.org/10.31436/ijpcc.v10i2.488

The Wi-Fi Certified Passpoint Program, commonly referred to as 'Passpoint' (or 'Hotspot 2.0') [4], was developed to address the limitations in seamless interworking between WiFi networks and mobile cellular networks, as well as among Wi-Fi hotspots themselves. Prior to Passpoint, Wi-Fi technology struggled with smooth transitions between networks and hotspots, creating a fragmented user experience. The Passpoint initiative aims to integrate Wi-Fi networks as a seamless extension of service provider networks, enabling users to transition effortlessly from one hotspot to another, like the seamless handovers experienced in cellular networks. Passpoint technology facilitates all control-plane functions required for automated and uninterrupted connectivity to Wi-Fi hotspots. Through Passpoint, service providers can utilize advanced Wi-Fi systems to offload traffic and offer high-bandwidth services, while subscribers benefit from reduced frustration and enhanced performance compared to traditional Wi-Fi hotspots. NGH also utilizes the latest security standards like WPA3 to secure data. Figure 1 compares traditional hotspots and NGH across different categories such as authentication, security, and user experience.

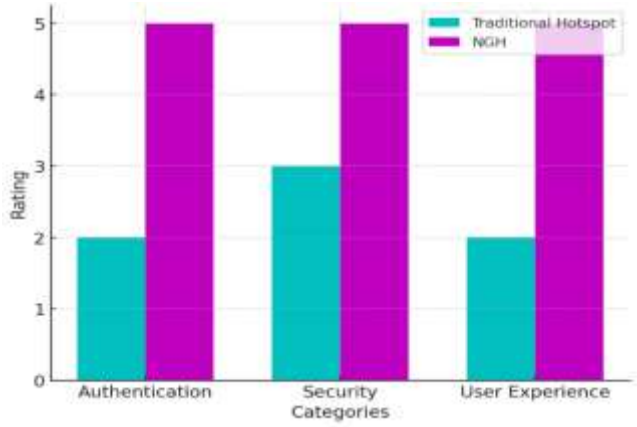

Fig 1. Comparison between traditional hotspot vs. NGH

In NGH, Passpoints can detect nearby Wi-Fi networks and immediately connect to the one for which the user has authorization. The second key benefit of Passpoint is enhanced security. Passpoint networks provide a higher level of security than standard Wi-Fi networks since they require the use of the enterprise-grade WPA2 security protocol for wi-fi access. The third advantage that Passpoint provides is seamless roaming across multiple WiFi networks of the same organization or partner networks without the requirement to maintain the SSID name consistent throughout the networks. It also eliminates the need for MAC addresses for visitor recognition and authentication, making it a future-proof solution for MAC randomization threats [5]. Users will register once for the NGH and download a secure password profile to their device via a variety of out-of-band mechanisms. When users return to or visit any of the brand's or partner's locations, they will be immediately connected to Wi-Fi via a safe and encrypted connection.

NGH outperforms the previous ones when it comes to issues such as efficiency and reliability during congestion or overloads as figure 2 showing the multiple steps involved in the traditional authentication process versus the one-time authentication process of NGH.

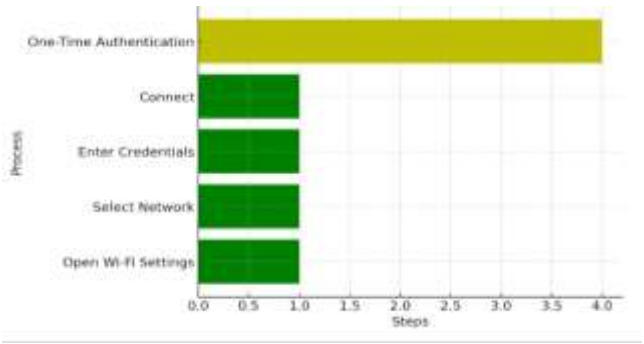

Fig 2. Steps for traditional authentication process

Another key development is beamforming. Unlike conventional signals that are broadcast in the general direction, beamforming allows an individual hotspot to direct the signals to each device connected to it. Narrow-based signal transmission is very reliable, fast, and can be extended far enough for longer distances. Also, Orthogonal Frequency Division Multiple Access (OFDMA) which allows dividing the available frequencies into small sub-channels for use by separate devices. They improve spectrum usability, reduce latency, and increase performance generally within congested areas.

II. Related Works

The development and deployment of Hotspot 2.0, also and Next-Generation Hotspot (NGH) technologies made significant advancements in enhancing Wi-Fi connectivity and user experience. These technologies aim to address longstanding challenges associated with seamless network access, user authentication, and efficient integration with cellular networks. As the demand for reliable and continuous wireless access increases, recent research has focused on evaluating the performance, security, and overall impact of these technologies on modern Wi-Fi networks. Table 2 provides a summary of recent studies related to Passpoint and NGH technologies, highlighting key findings and areas of focus. This overview includes performance evaluations, security considerations, and the impact of these technologies on both service providers and end-users.

https://doi.org/10.31436/ijpcc.v10i2.488

TABLE III
SUMMARY OF RELATED WORKS

Ref.	Title	Key Findings
[6]	Analysis of multiple access methods of modern Wi-Fi networks	Provides a comparative analysis of various access methods in contemporary Wi-Fi networks and their effectiveness.
[7]	Automatic Roaming Consortium Discovery and Routing for Inter-federation Wireless LAN Roaming System	Investigates automatic discovery and routing methods for inter-federation roaming in wireless LANs.
[8]	DVB-NGH: The Next Generation of Digital Broadcast Services to Handheld Devices	Discusses advancements in DVB-NGH for digital broadcasting to handheld devices and its implications for wireless communication.
[9]	Wi-Fi 7: The Next Frontier in Wireless Connectivity	Describes new features in Wi-Fi 7, including Multi-Link Operation (MLO), and their impact on performance.
[10]	DOLOS: Tricking the Wi-Fi APs with Incorrect User Locations	Wi-Fi user location privacy by creating ambiguity in location estimates, significantly degrading the accuracy of state-of-the-art localization systems without compromising Wi-Fi communication performance.
[11]	Challenges and Opportunities of 5G Network: A Review of Research and Development	Explores the potential benefits and challenges of integrating Passpoint with 5G technology.
[12]	A Review of Wi-Fi 6 : The Revolution of6th Generation Wi-Fi Technology	Reviews key enhancements in Wi-Fi 6, including efficiency and high-speed capabilities.

III. ADVANTAGES OF NEXT-GENERATION HOTSPOT

NGHs provide significant advantages over traditional Wi-Fi networks by automating the roaming and login processes. These advantages can be divided into three categories:

A. *Improved User Experience*

- *Seamless Connectivity:* Users can move between access points with uninterrupted connectivity, eliminating the need to manually search, select, and enter passwords for each network. This improves the overall user experience significantly, especially in dynamic environments such as airports, train stations, and shopping malls.
- *Reduced Frustration:* Manual password entry on mobile devices can be time-consuming. Automatic logins minimize the problem by allowing users to connect to Wi-Fi networks quickly and easily.
- *Increased Efficiency:* Automatic roaming saves users time by eliminating the need to reconnect to a new network each time they move. This improves overall efficiency and productivity, especially for mobile users.

B. *Enhanced Security*

- *Reduced Risk of Password Theft:* Manually entered passwords on public Wi-Fi networks are vulnerable to interception and theft. Next-Generation Hotspots (NGHs) utilize secure protocols for credential transmission, thereby mitigating the risk of unauthorized access and password breaches [14].
- *Enhanced Network Security:* NGHs can implement more stringent security measures and authentication methods, such as WPA2/WPA3 enterprise security, which offer superior protection against cyberattacks compared to traditional open Wi-Fi networks [11].
- *Centralized Credential Management:* With NGHs, user credentials are managed centrally through automatic logins. This approach simplifies the process of updating and revoking access, thereby strengthening overall network security.

C. *Network Management Optimization*

- *Decreased Administrative Burden: The elimination of manual configuration and troubleshooting tasks reduce the workload on IT personnel, thereby enhancing the efficiency of network management [12].*
- *Enhanced Network Performance: NGHs can dynamically allocate resources and prioritize user traffic based on location and usage patterns. This optimization improves overall network performance and ensures a stable, high-quality connection for all users.*

IV. IMPLEMENTATION ISSUES

Next-generation hotspots (NGH) may have replaced the current Hotspot 2.0, which implements Hotspot 2.0 into a real network. Users seem to favor WiFi over hotspots due to the coverage area, and taking over the mobile network will strain the users' mobile phones. Even with such advancements in the network, there are some weaknesses and limitations where the system is not immune to any threats and attacks from outside of the network due to the behavior of the hotspot:

A. *Cost of Implementation*

The usage of hotspots is widespread across the technology world as every service provider has expanded to provide wide coverage to public places. For the user to experience full coverage of the Next-Generation Hotspot, service providers need to lay out plans for implementing the Next-Generation Hotspot (NGH), which would definitely be costly due to the high demand from the users [13]. Due to

the technological advancement of the Next-Generation Hotspot (NGH), they cost more due to the use of a wireless 5G network.

The other reason for it to cost more than the current network is maintenance, where every service provider will offer users higher speed and network efficiency than before, which logically will cost more to upgrade to better performance with the help of network technical experts.

B. *Speed of Connectivity*

In general, hotspot connectivity is depending upon the strength of the wireless network signal within the coverage area provided by the service provider. Consequently, regions with suboptimal signal reception, regardless of the network, may experience slower connection speeds.

As the Next-Generation Hotspot (NGH) technology becomes widely adopted, it is anticipated to achieve a level of integration similar to established network standards such as 4G and 5G. Currently, 5G provides the highest data rates and increased network capacity; however, once NGH reaches global normalization, managing the growing number of users and devices on the same network standards may present challenges. Technical expertise indicates that electronic devices in proximity to network equipment can contribute to connectivity issues, as interference from radio signal noise can degrade NGH performance [14].

C. *Device Compatibility*

Although the recent use of 5G networks has enhanced connectivity speeds and efficiency, Wi-Fi connections remain competitive in terms of performance. However, the transition to 5G presents compatibility challenges, as not all devices support this new standard. The new mobile phones manufactured subsequently are compatible with 5G, while older models are not, resulting in network compatibility issues.

Outdated software and devices can make additional challenges for the implementation of Next-Generation Hotspot (NGH) technology. To ensure seamless integration and functionality, both user devices and hotspot networks must be capable of updating to support NGH. This ensures that users can access the network effectively, similar to other users with updated equipment.

V. SECURITY CHALLENGES ON NEXT- GENERATION HOTSPOT (NGH)

There are some security challenges associated with implementing NGH, including vulnerabilities in authentication processes, data protection issues, and the potential for misuse:

A. Vulnerabilities in Authentication Processes

One of the main security challenges in NGH systems is ensuring robust authentication mechanisms. NGH technology relies on advanced authentication protocols, such as Passpoint, to enable seamless connectivity. While these protocols are designed to enhance user convenience by minimizing manual logins, they also introduce potential vulnerabilities.

For example, the automated authentication process can be vulnerable to man-in-the-middle (MitM) attacks if the initial certificate exchange or credential verification is compromised. Attackers could exploit weaknesses in the handshake or certificate validation processes to gain unauthorized access to the network. Moreover, if the credentials are intercepted or stolen, unauthorized users could potentially access sensitive information or exploit network resources [15].

B. Data Protection and Privacy Concerns

Data protection and user privacy represent significant concerns in NGH systems. NGH technology enables seamless connectivity by exchanging user credentials and session information between networks. While this facilitates a user-friendly experience, it also raises issues regarding the protection of sensitive data.

The transmission of user credentials and session data across multiple networks can expose this information to interception or unauthorized access if encryption protocols are not adequately implemented. Furthermore, the centralization of user data for seamless authentication increases the risk of data breaches, where attackers could potentially access large volumes of user information from a single compromised database [16].

C. Potential for Misuse and Exploitation

The widespread adoption of NGH technology could also lead to potential misuse and exploitation. As NGH systems streamline network access, they unintentionally create opportunities for malicious actors to exploit network resources. For example, attackers could exploit vulnerabilities in the NGH infrastructure to launch denial-of-service (DoS) attacks or disrupt network services.

Additionally, the seamless nature of NGH connectivity could facilitate unauthorized access to restricted or sensitive areas within a network. Without adequate security measures, attackers could leverage the ubiquitous connectivity to bypass security controls or gain unauthorized access to protected resources [15].

D. Challenges in Securing Roaming and Interoperability

NGH technology supports interoperability and seamless roaming across different network operators. However, this very capability caused security challenges. Ensuring secure communication and data integrity between different network domains requires robust interoperability protocols and encryption standards. The lack of standardization or

inconsistent implementation across networks can create vulnerabilities that attackers might exploit.

VI. MITIGATION STRATEGIES

Addressing these security challenges requires a multi-faceted approach:

A. Enhanced Authentication Protocols: Implementing stronger authentication protocols and encryption standards can mitigate the risk of unauthorized access and data interception. Regular updates and security patches are essential to address vulnerabilities in authentication mechanisms.

B. Robust Data Encryption: Ensuring end-to-end encryption for data transmissions and user credentials can protect against interception and unauthorized access. Encryption standards should be regularly reviewed and updated to address emerging threats.

C. Network Monitoring and Intrusion Detection: Deploying comprehensive network monitoring and intrusion detection systems can help identify and respond to suspicious activities or security breaches in real time.

D. Standardization and Collaboration: Developing and adhering to standardized security protocols across different network operators and NGH systems can enhance interoperability and reduce security vulnerabilities. Collaboration among industry stakeholders is crucial to establishing and enforcing these standards.

VII. CONCLUSION

In conclusion, Next-Generation Hotspot is a significant advancement in Wi-Fi technology. While there are challenges, collaborative efforts among network providers, technology developers, and users will drive NGH adoption and optimization. Continuous research and development are critical to addressing security concerns and ensuring NGH's long-term success.

Despite these challenges, the potential benefits of NGH outweigh the disadvantages. Both users and network operators benefit from the seamless user experience, enhanced security features, and dynamic resource allocation capabilities. Additionally, NGH-enabled new applications such as AR/VR experiences and remote healthcare have the potential to revolutionize many aspects of our lives.

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] E. Yanmaz, "Next Generation Hotspot (NGH) – A Wi-Fi Roaming Solution," International Journal of Advanced Computer Science and Applications, vol. 13, no. 5, pp. 123-132, 2022.

[2] P. Morgado, L. Santos, and J. Pereira, "Next Generation Hotspot: A Review of the Technology and its Future," IEEE Access, vol. 11, pp. 36485-36502, 2023.

[3] Y.-H. Chiu, C.-C. Wang, and C.-F. Lin, "Performance evaluation of Wi-Fi roaming in Next-Generation Hotspot (NGH) with multi-operator environment," Journal of Network and Computer Applications, vol. 228, p. 104413, 2023.

[4] S. Hoteit, S. Secci, G. Pujolle, A. Wolisz, C. Ziemlicki, and Z. Smoreda, "Mobile data traffic offloading over Passpoint hotspots," Computer Networks, vol. 84, pp. 76-93, 2015.

[5] S. Gupta, M. K. Mishra, and S. Srivastava, "A survey on next-generation hotspot (NGH): A step towards seamless and ubiquitous Wi-Fi experience," Computer Networks, vol. 193, p. 108132, 2021.

[6] Zh. Ismagulova and E. Seidulla, "Analysis of multiple access methods of modern Wi-Fi networks," Q A Iasaýı atyndaǵy Halyqaralyq qazaq-túrik ýnıversıtetiniń habarlary (fızıka matematıka ınformatıka seriiasy), vol. 24, pp. 116-128, 2023.

[7] K. Irie and H. Goto, "Automatic Roaming Consortium Discovery and Routing for Inter-federation Wireless LAN Roaming System," Journal of Information Processing, vol. 28, pp. 378-386, 2020.

[8] D. Gomez-Barquero, C. Douillard, P. Moss, and V. Mignone, "DVB-NGH: The Next Generation of Digital Broadcast Services to Handheld Devices," IEEE Transactions on Broadcasting, vol. 60, pp. 246-257, 2014.

[9] A. S. George, A. S. H. George, and T. Baskar, "Wi-Fi 7: The Next Frontier in Wireless Connectivity," Partners Universal International Innovation Journal (PUIIJ), vol. 01, no. 04, pp. 133–145, 2023.

[10] J. Deposada, "Exploring hotspot 2.0 - Fon: The global WIFI Network," Fon, May 28, 2018.

[11] N. Sahu and R. Sahu, "Challenges and Opportunities of 5G Network: A Review of Research and Development," American Journal of Electrical and Computer Engineering, vol. 8, pp. 11-20, 2024.

[12] S. George and A. S. George, "A Review of Wi-Fi 6 : The Revolution of 6th Generation Wi-Fi Technology," Research Inventy: International Journal of Engineering and Science, vol. 10, no. 09, pp. 56–65, 2020.

[13] K. Poularakis, G. Iosifidis, and L. Tassiulas, "Joint Deployment and Pricing of Next-Generation WiFi Networks," IEEE Transactions on Communications, vol. PP, pp. 1-1, 2019.

[14] A. H. Khoula, N. Shah, and A. N. S. Shankarappa, "Smartphone's hotspot security issues and challenges," in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016, doi: 10.1109/icitst.2016.7856680.

[15] L. Suárez-Plasencia, C. M. Legón, J. Herrera, R. Socorro, O. Rojas, and G. Sosa Gómez, "Weak PassPoint Passwords Detected by the Perimeter of Delaunay Triangles," Security and Communication Networks, vol. 2022, pp. 1-14, 2022.

[16] J. Herrera, C. M. Legón, L. Suárez-Plasencia, R. Luis, O. Rojas, and G. Sosa Gómez, "Test for Detection of Weak Graphic Passwords in Passpoint Based on the Mean Distance between Points," Symmetry, vol. 13, 2021.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.489

Lifestyle Assistance using Smart Mirror for better Physical and Spiritual Wellbeing

Mohammad Afif Muhajir, Hibo Sulieman Amen, Akeem Olowolayemo
Department of Computer Science. KICT, International Islamic University Malaysia.

*Corresponding author akeem@iium.edu.my
(Received: 2nd June 2024; Accepted: 14th July 2024; Published on-line: 30th July 2024)

Abstract— Humans live through their lives with many activities or actions, some people have more activities tied to their lives while others have less. It is with these chains of actions or activities can people achieve what they want to do in their life. The problem arises when people do not plan their activities effectively or some may not plan at all due to factors such as the hassle in arranging their lifestyle or daily activities. Lifestyle in general defines how people conduct their daily life to meet their own needs in many aspects and by itself may affect people in many ways because it is the concept that governs how humans do their activities or how they live out their daily life. Unorganized lifestyle may cause more negative influences than people think, it may even affect their own overall health in physical or spiritual aspects. In the discussion of physical and spiritual health, we can define physical health as the condition of our body taking into consideration the absence of disease and fitness level. As for spiritual health or wellbeing, it is mostly known to be connected to people's mental health but in this research, we want to accommodate Islamic values of spirituality and how it helps maintain people's overall wellbeing. In accordance with the growing advancement of technology there are now many ways to help people organize their daily tasks and activities also their overall lifestyle such as an application that provides daily planners with notifications to help being reminded of their own plan for the day. It is with these points we would like to propose a project into studying general activities that supports a good lifestyle from physical and spiritual wellbeing while also incorporating the usage of technology in the form of an IoT (Internet of Things) device, in this case a Smart-Mirror, to help organize a good daily planner.

Keywords— *Daily Activities Planner, Lifestyle, Wellbeing, Smart Mirror, Digital Mirror, Digital Personal Assistant, IoT.*

I. Introduction

In general, the typical way of life of an individual, group, or culture is considered a lifestyle. A well-balanced diet, regular exercise, enough sleep, happiness, and positive thinking are all essential components of a healthy lifestyle. Living a healthy life is vital for an individual to be happy and feel good in the present and for the future. It also helps to live longer and to be less prone to sickness and diseases. According to WHO, 60% of related factors to individual health and quality of life are correlated to their lifestyle [1], [2]. To have a vibrant, healthy life, it is essential to pay attention to one's spiritual, emotional, mental, and physical health. It is often the case that when people think of being healthy, they might only consider their physical bodies. However, it is important to consider one's emotional, spiritual, and psychological health as well to have a well-rounded healthy lifestyle.

One of the ways to ensure a rounded lifestyle is to plan one's activities to encompass all the aforementioned aspects of human health. A planner can be a way to structure a healthy and appropriate lifestyle suitable for each person. An effective planning for a daily routine that takes into consideration all necessary activities can enhance a healthy lifestyle leading to better wellbeing.

Spiritual wellness is another factor that is often overlooked but have been identified to constitute in one' attainment of overall wellbeing. Spiritual Wellness or spiritual health is a concept that is lesser known but has an impact towards achieving peacefulness and meaningfulness in the life of an individual that may serve as a ground to deal with hardships. It is often defined and influenced by other aspects such as religion, belief, and values [3].

It should be worth noting that research has delved into the connection between spiritual health and how it can affect other elements of human's wellbeing. Spirituality and health-related behaviours can play a significant role in defining psychological well-being. Personal focus on physical health and the human body or psychosocial health and the human mind and spirit, have an immense impact on psychological well-being [4]. Spirituality can be identified and improved through many means such as meditation, religious activities (i.e. joining a faith group or conversing with a spiritual guide or chaplain). For Muslims, for instance, there are several ways to connect and improve spiritual health through actions that bring closeness to God such as reading holy books, prayer, fasting and reflection. With this information, it could be deduced that incorporating spirituality alongside physical and mental health can further help to achieve overall wellbeing. It can provide possible type of actions that can be incorporated in ones routine for that betterment of one's health. This can be further managed and enhanced with the assistance of modern technology.

In the past decades, there has been steady and significant growth in the use of smart devices with several applications for different aspects of human life. Modern

https://doi.org/10.31436/ijpcc.v10i2.489

technology has produced amazing tools and resources that have made it possible to access useful information and opening new opportunities for better quality life and enhanced way of life. This study proposes the use of a smart mirror for monitoring and enhancing lifestyle and overall wellbeing. Smart mirror has been chosen in this study due to the central role a mirror plays in daily life and every home. A mirror is one of the tools in every home that is used every day for things like brushing teeth, shaving, and applying cosmetics to the face and assessing other parts of the body. Many people see themselves or, more accurately, their reflections at least a few times each day in a mirror. Because of this widespread use, it might be interesting and beneficial if the mirror could communicate and assist in the same way as a real person or digital assistant. The idea behind this is that combining the concept of a mirror with technology might be able to replace the emotional, spiritual, and physical need of lost relationships. As we know 80% of older adults who are older than 65 have at least one chronic illness, have lost some loved ones and most likely living alone [1].

The advent of Internet of Things (IoT) technology has provided more opportunities for the use of sensors to acquire data, especially remotely. IoT has the potential to revolutionize the traditional healthcare system by making health management more efficient. IoT technology can be used to connect smart devices, machines, patients, doctors, and sensors to the internet through the use of sensors. This allows for more efficient health management and can help alleviate the strain on healthcare systems caused by an aging population and a rise in chronic illness. IoT technology can be used to monitor patients remotely and provide real-time feedback to healthcare providers. This can help reduce the number of hospital visits and improve patient outcomes. Additionally, IoT technology can be used to improve medication adherence by providing reminders and tracking medication usage. Finally, IoT technology can be used to improve the efficiency of healthcare systems by automating tasks such as inventory management and scheduling. The use of IoT technology has changed people's lives by saving time for healthcare workers and patients alike [5]. Since a Smart Mirror is a part of smart devices found in residences, it can also act as a device which assists in monitoring the health of a user and regularly update and send reports of patients to respective authorities in the medical field [5].

In this study, we attempt to design a system using Smart Mirror as a digital assistant that will enable individuals to enhance their lifestyles and overall wellness. Using digital mirror as a digital assistant can help people to schedule their life by providing a variety of basic functionalities in the form of weather updates, news updates, clock and alarm settings, appointment schedule, daily tasks monitoring and spiritual and emotional activities monitoring, etc. all can be made available by integrating APIs into the system. A user can access the Smart Mirror either by voice input using the inbuilt microphone or through touch using a touchpad.

II. Related Works

With the advancement of technology, many aspects and factors of human's life can be affected, one of those in this research case is Self-Healthcare (SHC). SHC is supported by many inventions and innovations such as IoT, service robotics, cloud computing, etc. Many people nowadays, especially millennials, have grown accustomed to a rather unhealthy lifestyle that mostly warrants health issues. These issues commonly are being checked by frequent visits to the doctor, but now with the help of technological implementation in the form of integration of IoT elements such as a Smart-Mirror and wireless devices to monitor real time health and fitness [5].

Across the years, people's busy working schedules have led to a decline in the amount of time they spend reading newspapers on a daily basis, resulting in a lack of awareness about current news. Another significant time-consuming aspect of their routine is the time spent changing appearances in front of a conventional mirror. However, the introduction of smart mirror systems in households has emerged as a solution to address these challenges and enable individuals to accomplish more in less time. The study in [6], implemented a Smart Mirror to save time by combining functionality and convenience. This innovative device not only serves as a conventional mirror but also provides valuable information at a glance, allowing individuals to stay updated with current news and events. By integrating a display into the mirror, the smart mirror acts as a time-saving tool, offering users quick access to relevant information while going about their daily routines.

Mirrors have been around for almost 200 years and have been a high-end piece of decor. Now adding technology, produces one of the most beautiful products with a lot of potentials. Some conditions like anxiety, stress, and depression have affected many people's health. According to estimates, depression affects 4.4% of the world's population, and anxiety disorders affect 3.6% [6]. Depression is a serious mental health condition characterized by a lack of interest in enjoyable activities, sadness, guilt, low self-esteem, trouble sleeping, and difficulty in paying attention.

Smart mirrors and IoT can benefit individuals in numerous ways especially considering the mental issues aforementioned. Previous studies such as [6] has proposed that the growth of mobile applications has provided opportunities to implement a non-intrusive way of combating a sedentary life, which has been found as one of the big factors for many health-issues, by developing a mobile application that can provide solutions to promote physical activity and active engagement to prevent or minimize sedentary lifestyle.

Other studies have equally consodered the effectiveness of using digital mirrors for physical rehabilitation. For instance, the study in [11] evaluated the effectiveness of pose estimation models as enablers for a smart-mirror physical rehabilitation system, with the objective of providing digital solutions to support older adults in extending their independence. The proposed system utilizes medium or small-sized smart mirrors that cover essential body areas, particularly focusing on the face and shoulders. To assist individuals in their physical rehabilitation routines, a comprehensive list of exercises and a management system are integrated into the system. The study investigated various pose estimation models, considering their suitability and performance for the targeted rehabilitation purposes.

One of the main focus in this study include integrating spirituality and value into the proposed system with the expectation to help users gain a more serene lifestyle through physical or mental aspects of healthy lifestyle with a spiritual reinforcement. This is in agreement with the study in [7] that identified mental health as one aspect of human life that connects to psychological wellbeing as a whole, and how spirituality is a crucial factor to understand both concepts. Furthermore, the right spirituality provides whoever believes with means to relate spirituality and mental health to the values introduced inside the religious principles especially learning from the lives religious personalities who faced more challenging circumstances, hence, providing characteristic examples to learn from and implement in one's life as one of the ways to elevate spirituality, and with it, overall mental health and wellbeing.

In the study presented in [8], spiritual health is considered abstract, subjective, and complex, as well as constantly changing depending on context and religion. Spiritual health has also been found to be connected to some diseases and physical health problems. The study employed specific methods that consist of theoretical, fieldwork, and analytical processes backed by studies of literature to acquire reliable evidence to further provide significance for spiritual health to wellness and support in some healthcare fields, such as nursing. This research provided critical foundations for the approaches in implementing regular spiritual activities to help in attaining better lifestyle and overall wellbeing.

Moreover, in [9], the authors researched the beneficial effect of applying the lifestyles of religious leaders such as Muhamad or Jesus Christ in general daily activities to gain a healthier body by combatting causes of disease. For instance advocating basic eating etiquette and suggestions to do more physical activities could potentially be useful to combat diabetes and obesity. The researchers showed that following dietary and light fitness information validated by dietitian and health experts to provide relevance to better people' quality of life from the aspect of physical health and wellbeing.

In a similar application that helps people to lead a smart life, the authors in [10], implemented voice-activated controller as a module inside the smart mirror that can handle many tasks, such as creating a schedule and task reminder. This is similar to our aim in this study, but with the exception of using traditional key-in input and expanding the idea of suggestion-supported schedule planner that helps people with providing them relevant and beneficial activities and doings.

Other authors such as [11], have focused using smart mirrors to provide health monitoring for the elderly to monitor their situation when they are at home. The researchers in [8] developed a smart mirror for elderly emotion monitoring using a semi-electronic display device designed to detect and identify initial signs of depression in the elderly. It functions as a smart mirror, providing users with daily information such as weather updates, events, headline news, currency rates, stocks, and reminders. The device is a communication tool for telemedicine, making it easier for elderly patients at home to feel more connected to their doctors. Long-term patient diagnosis, follow-up, and treatment are all made easier by this. While dressing themselves in front of a mirror, elderly users can view information about their mental health. In the same way that a housekeeper or nurse would, information on their daily emotions will be collected to long-term monitor their health. We also incorporate additional systems like a chat bot, facial recognition, voice/speech recognition, and posture recognition in order to observe the emotions of elderly users.

III. Methodology

A. *Smart Mirror Design & Development.*

In this study, the first major effort is devoted to assembling the smart mirror, as an IoT device containing a two-way mirror with an electronic display behind the glass. The display can show the viewer various kinds of information in the form of widgets, such as weather, time, date, and news updates. The usage for this device would be as a platform to house and initialize the planned lifestyle assistance algorithms and procedures with all its functionality installed within the smart mirror.

The aim of this work is to take advantage of people's common act of using a mirror, usually at the start of their day to groom themselves, and promote an alternative usage of common mirrors that is hoped to provide more efficiency in doing tasks in this case planning for daily hustle with technological upgrades.

B. *Lifestyle Assistance Application*

The planned application would also be equipped with the ability to suggest and include some of supportive activities that may range from physical exercises to activities that support the wellbeing of the mind; especially in accordance with the spirituality dimension. The application algorithm is also incorporated to suggest motivational and

https://doi.org/10.31436/ijpcc.v10i2.489

spiritual quotes as well as interface with health care providers, personal trainers, therapists, and other caregivers specifically recommended for that has been regarded as a way to increase overall personal wellbeing and spirituality as well as training users for improved mindfulness.

The system development life cycle (SDLC) is considered at all stages to develop the system in this project. Specifically, the Agile System Development methodology, which consists of six main stages as shown in the figure, is being followed for developing the smart mirror application. Starting with the Project Requirement Initiation, time was spent on planning and discussing the project vision and the ROI justification. After the system requirements were defined and the way it would function and assist users was determined, data was collected and elicited from random people who felt interested in the topic. Then, the plan and duration of the application were discussed by the authors. Additionally, the objectives and significance of the system were listed down.

Next, stage 2, which is the Designing Phase, was initiated, where the focus was on Software Design and the UI design of the application. Following that, stage 3, Development and Coding, was carried out, with the focus on producing code and translating design documentation into actual software. Moving on to stage 4, Integration and Testing, efforts were made to ensure that the software is bug-free and compatible with several existing similar applications that have been built previously. Furthermore, deployment and review stages were performed, where the software was prepared for deployment and the implemented system's performance was evaluated. Feedback from users and stakeholders was gathered during the review process to identify areas for improvement and address any remaining issues.

C. *Application Modules and Features*

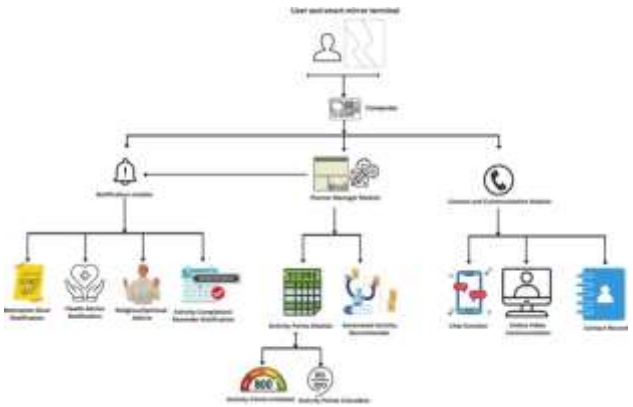

Fig. 1. Visual Representation for Lifestyle Assistance Modularity

Throughout the project, the Agile principles have been followed, embracing flexibility and adaptability, allowing for continuous improvement and customer satisfaction. In each stage of the Agile System Development methodology, a dedicated approach has been adopted to create a well-structured, high-quality system that aligns with the project's objectives and meets the stakeholders' needs.

One of the main goals of developing this lifestyle assistance system is to help people with planning and organizing their bustling activities with many features and modules that are expected to bring a better lifestyle for the user. The detail functions provided by the system are as described below:

1) Activities Planner.

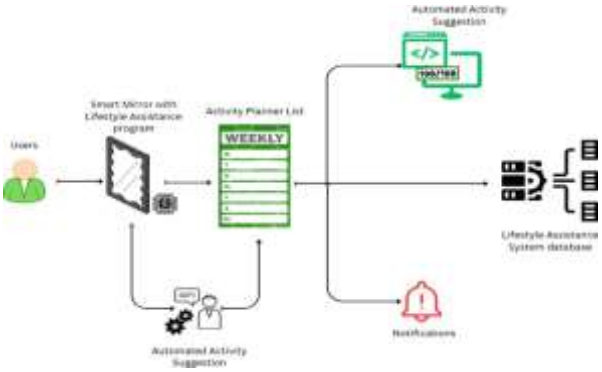

Fig. 2. Activity Planner module connection representation

Fig. 3. Module representation for the activity planner

This module will serve as the primary unit of our proposed system. As described previously, this module's main objective is to give the users of this system the ability to manage their activities, tasks, or duties especially those considered to be done routinely so that they can plan ahead to give them an early grasp on what those activities entail.

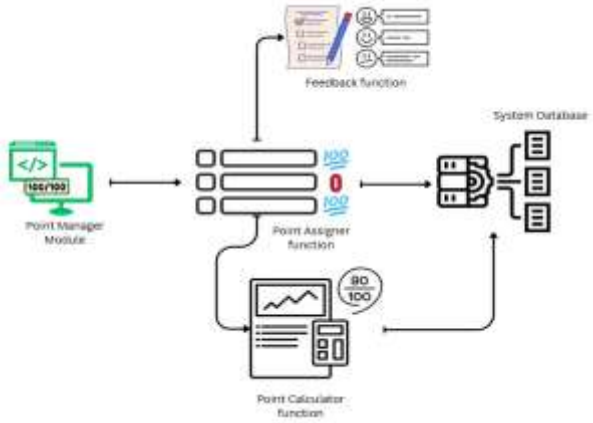

Fig. 4. Points manager module representation

https://doi.org/10.31436/ijpcc.v10i2.489

The activity planner will record elements that are commonly used for activity details, such as what should be done, when and where those endeavours will take place. Other parts of this module are point assignment and counters. The activity planner is connected to the notification module to help notify users on upcoming activities, and also check if the user has done some required activities by recording the acknowledgement of completion of the activities. The notification module also provide notifications on useful health tips and advices about spirituality wellness.

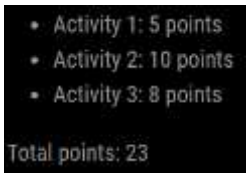

Fig. 5. Total points module representation

2) Point manager functions.

As described in the planner module description above, this is one of the internal functions included inside of the aforementioned module. The objectives of these functions are to allocate a set amount of points into each activity that the system user has assigned into the planner and to count the points accumulated by completing each activity and set the specific period of time. A set of formulas has been theorized to help us with the points-related module that is part of the daily activity planner. Below are the expositions of each formula:

3) Point-Setter functions.

The main idea of this function is to set the weight for each activity point. The initialized point for each activity will differ based on the type of activity that is input into the planner list. This table will be used to determine the point value for each activity in the activity planner. The process starts by determining the type of activity; activities that are automatically set by the planner system will be under the type "Extra Activity" which could be either "Physical" or "Spiritual" boosting, while activities that the user set themselves into the planner will always count as "Mandatory". After determining the type and its importance of each activity, it will assign the "weight" - Activity Weight (A_w for short). All the numbers provided in the table above are hypothetical.

TABLE I
POINT-SETTER CRITERIA

No	Activity	Type	Importance	Activity Weight (AW)	Initial Point (IP)
1	Activity 1	Main User Activity	Mandatory	Mandatory = *1	10
2	Activity 2	Extra Activity (Physical-Boosting)	Preferred by User or Recommended	Recommended =*0.5	5<=10
3	Activity 3	Extra Activity (Spiritual-Boosting)	Optional	Optional =*0.25	3<=10

After determining the A_w for each activity it will be multiplied with the initialized point for each activity. Initial points other than Main User Activities (which only covers Extra Activity provided by the system) will be determined based on research on how important or recommended for each activity. Therefore, if an activity is completed, point is multiply by 10, whereas if an activity is missed, it deducts 1.

The representation of the formula for the activity point (Ap_x) initializer would be:

$$Ap_x = A_W * IP$$

4) Point Accumulator Formula

The Point Accumulator will calculate all gathered points from the user's completed activities in a day. Each point will be added and then divided by the total amount of points that is available to be achieved in a day in the planner and then it will be multiplied by the full percentage to show the cumulative achievement within a day. The planner prompts the user for confirmation of any activity completion if the time set for each activity is reached. The calculation process is represented as the formulas below:

The summation of all activities points gathered compared to maximum activity point achievable is given as

$$\Sigma Ap = \frac{Ap_n}{Ap_m}$$

Then the addition of all activities points gathered is computed as

$$Ap_n = Ap_1 + Ap_2 + Ap_3 \ldots + Ap_x$$

And the addition of maximum activity point achievable can be written as

$$Ap_m = Ap_1 + Ap_2 + Ap_3 \ldots + Ap_x$$

5) Feedback subfunctions

https://doi.org/10.31436/ijpcc.v10i2.489

This function is directly related to the utilization of points and their accumulation in the system modules. After the final points are gathered and calculated, appropriate feedback messages will be shown to the user to reflect their quality of achievement in finishing daily tasks and additional beneficial activities.

6) Notification Module

This module is a component that will provide notifications to the user about many other features. This module will provide a display notification of users to track activities set in the activity planner. It also include notification of daily general health advice, spiritual or motivational quotes or reminders from the Qur'an and Sunnah or from other religious books depending on the faith of the user, to improve spirituality, emotional or overall wellbeing.

7) Mobile application

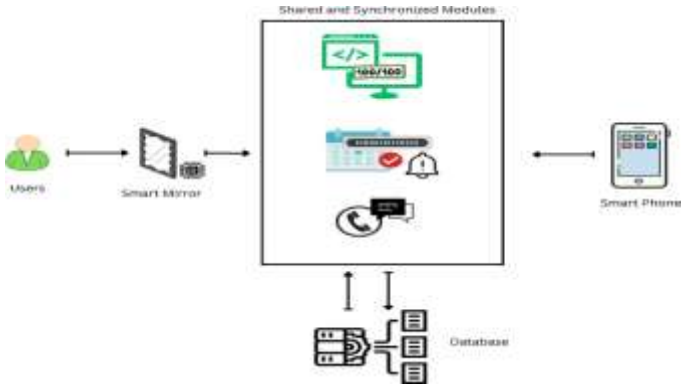

Fig. 6. Shared functionality available to Mobile App version

The planned smart mirror program module will include an application that will be available on mobile devices. This is to allow users to keep up with whatever plans that they have initialized in their smart mirror. The application will share the main functionalities of the smart mirror program and both devices will share data from the same database system.

8) Contact and Communication Manager

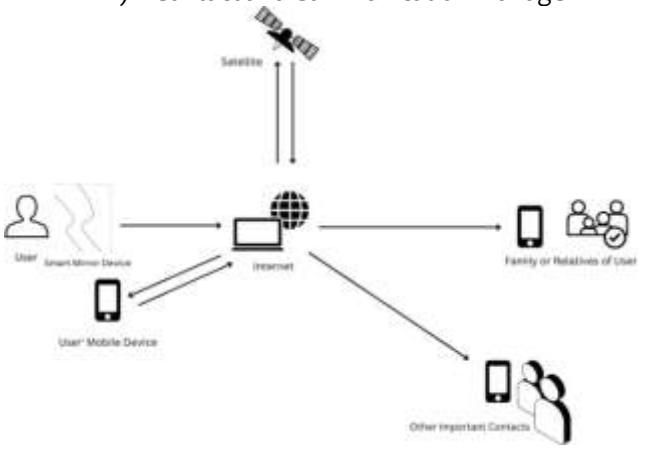

Fig. 7. Contact and communication connection flow

Fig. 8. Sample presentation of contact module

The system has contacts feature, which enables users to add and contact any relevant individuals such as their designated family members or relatives, or even their doctors and other related parties. It equally provide the users to directly share their planners and progress records or improved lifestyle condition. The available connection is as shown in Fig. 7.

D. System Features

The system features are divided into a few sections which are Planning and Initiation, System Flow, System Design User Interface.

1) Plan & initiate system features

During the planning and initiation phase, the system us as the development team allocated significant time and resources to carefully outline and establish the project's requirements. Both functional and non-functional requirements were meticulously documented, aiming to deliver a system that optimizes the efficiency of the product creation process while effectively managing user expectations. In the initial phase, all the identified requirements were successfully identified and implemented, ensuring the system's functionality and usability. However, as the project progressed into phase 2, the team decided to introduce additional features by creating two distinct versions of the system: a smart mirror version and a mobile application version. This decision was driven by the goal of providing users with more choices and enhancing their overall experience. The development work for these versions is currently underway, with a strong focus on meeting the requirements established in early phase while accommodating the unique functionalities and user interfaces of each version. The team is committed to ensuring that both the smart mirror version and the mobile application version are robust, user-friendly, and aligned with the project's objectives. By diligently addressing the requirements and continuously improving the system, the team is optimistic about the future success and effectiveness of the project. The ongoing efforts and dedication put into the development process aim to deliver a high-quality system that fulfils user needs and enhances the overall product creation experience.

2) System Flow

To illustrate and depict the system's functionality and flow, system flow diagrams was incorporated. These diagram serves as visual representations that showcases the sequence of activities and interactions within the system. By utilizing one of different types of system flow, a

https://doi.org/10.31436/ijpcc.v10i2.489

comprehensive overview of the system's behaviour and functionality was effectively communicated. For the users to able to gain a better understanding of the system's functionality and flow. The diagrams serve as valuable communication tools, enabling the project team and Users to visualize and analyse the system's behaviour, identify potential bottlenecks or improvements, and ensure alignment with the desired system objectives.

3) System Design User Interface

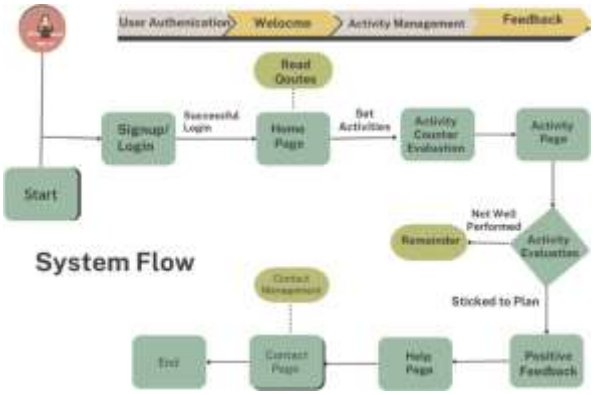

Fig. 9. Lifestyle Assistance System Flow

E. System Discussion

Two aspects of the system, the functional and non-functional requirements of the Lifestyle Assistance application would be discussed in this section. Functional requirements encompass the specific functionalities and features that the application must possess to meet user needs. These include modules such as Register and Login, Planner, Calendar, and other essential components that enable users to manage their schedules effectively. On the other hand, non-functional requirements focus on the qualities and characteristics of the application, such as performance, security, usability, and reliability. These requirements ensure that the Lifestyle Assistance application not only delivers the desired functionalities but also provides a seamless and secure user experience. By comprehensively addressing both functional and non-functional aspects, the system lays the foundation for a robust and user-centric application.

1) Functional Requirements

We used to build software or computerized device interfaces with an eye toward style is known as user interface (UI) design. It has been a strive to create user-friendly and enjoyable interfaces. The Register Page, the Login Page, the Planner Page, the Activity Page, point counter page, and the Contact Page are the six different pages in the Life Assist Application.

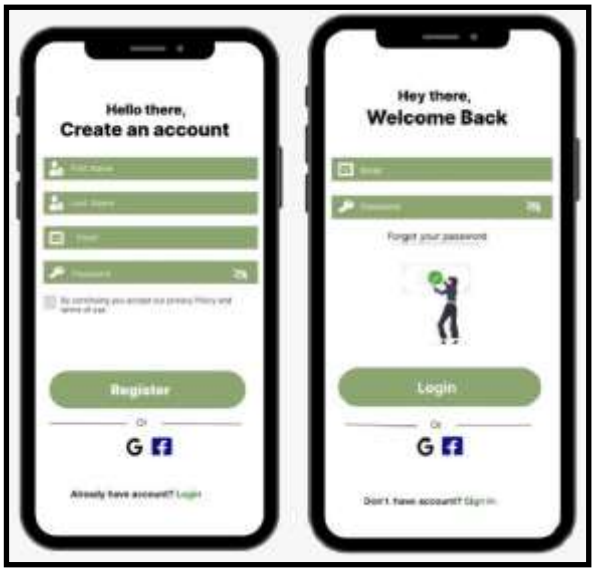

Fig. 10. Registration and Login UI

Fig. 10 represents the Register and Login modules, that are essential components of the system. These modules play a vital role in ensuring user access and security through the process of verification. In the Register Module, users are required to provide their first name, last name, email address, and password. This information is necessary for creating a user account. During the registration process, users must enter a valid and authentic email address. If an invalid email address is entered, the system will prompt the user to re-enter both their password and email for verification purposes. This step helps in preventing unauthorized access and ensures the accuracy of user data. This step serves as a privacy measure and is essential for verifying the user's identity. By requiring users to input their registered email and password, the system ensures that only authorized individuals can access the account and safeguards against unauthorized access. Both the Register and Login modules work together to establish a secure environment for users. By implementing these verification processes, the system maintains data integrity, protects user information, and enhances overall system security.

Welcome Page: The Welcome Page serves as the initial interface when users access the Life Assist application. It offers a positive and inspiring start to the day by displaying the day's quote: "Be the best version of yourself, spiritually, physically, and socially." This quote sets a motivating tone and encourages users to strive for personal growth in multiple dimensions. Additionally, the Welcome Page can be considered a lock page, providing a level of security and privacy for the user. Users also have the option to choose from a selection of quotes, allowing them to customize their experience and find inspiration that resonates with them.

https://doi.org/10.31436/ijpcc.v10i2.489

Fig. 11. Main page UI for the mobile app

Planner Module: The Planner Module is a fundamental component of the Life Assist application that assists users in managing their daily and weekly schedules. Users can customize their schedules according to their specific needs and preferences. The module consists of two sections: the planner and the calendar. The planner section enables users to input and organize tasks, appointments, and events for each day. It provides a clear and structured overview of the user's day, allowing them to plan and prioritize their activities effectively. Users can set reminders, allocate time slots, and mark completed tasks to stay on top of their commitments. Overall, the Planner Module empowers users to maintain better organization and productivity by tracking their day-to-day and weekly schedules. It serves as a reliable tool for users to stay on track, meet deadlines, and make the most of their time, ultimately helping them lead more organized and efficient lives.

Fig. 12. Activity Planner and Progress Monitor UI for mobile app

In the two pages mentioned, users have the ability to set their activities and schedule them accordingly. These pages serve as an activity list, allowing users to input and organize their tasks, appointments, and events based on their preferences and priorities. The users can specify the time, duration, and other relevant details for each activity. The system actively monitors the user's schedule and tracks the progress of their activities. If a user fails to complete an activity within the designated time, the system will send a reminder or notification to inform the user that they are behind schedule. This serves as a gentle nudge to encourage the user to catch up with their planned activities and maintain productivity.

On the other hand, if the user successfully adheres to their schedule and completes their activities on time, the system will provide positive feedback. This feedback can be in the form of messages, badges, or rewards, acknowledging the user's diligence and commitment to their planned tasks. This positive reinforcement aims to motivate the user and reinforce their adherence to the schedule, fostering a sense of accomplishment and productivity. These two pages are interdependent, working together to create a seamless workflow. The activity list page allows users to organize and plan their tasks, while the feedback-giving page keeps them informed and motivated by providing reminders and positive reinforcement based on their adherence to the schedule. This combined functionality helps users stay on track, manage their time effectively, and maintain a productive routine.

2) Non-Functional Requirements

The Non-functional requirements of Life assist application includes system's Security, Performance, and Reliability.

i. Reliability

The Life Assist application places a strong emphasis on reliability as a key requirement. Reliability refers to the ability of the system to consistently perform its intended functions without interruptions or failures. In the context of Life Assist, users rely on the application to effectively manage their schedules, track their activities, and receive timely reminders. By prioritizing reliability, the Life Assist application aims to provide users with a dependable and consistent experience. Users can confidently rely on the system to accurately store their schedules, send reminders, and assist them in managing their day-to-day activities effectively.

ii. Performance

The Life Assist application not only emphasizes reliability but also encompasses a strong performance functionality. Performance refers to the application's ability to deliver fast

https://doi.org/10.31436/ijpcc.v10i2.489

response times, efficient processing, and optimal utilization of system resources. In the context of Life Assist, performance plays a crucial role in providing users with a seamless and responsive experience. The application is designed and optimized to ensure quick loading times and smooth navigation, allowing users to efficiently access their schedules, input new activities, and interact with the system without delays or lags. By prioritizing performance, the Life Assist application aims to provide users with a smooth and efficient experience, allowing them to manage their schedules and activities seamlessly. The application's high-performance functionality enables users to navigate through the system effortlessly and accomplish their tasks with ease.

iii. Security

The login and sign-up pages of the Life Assist application incorporate robust user authentication mechanisms to ensure the security of user data and schedules. These authentication processes play a critical role in verifying the identity of users and safeguarding their sensitive information. When users register for an account, the sign-up page collects their required details, such as name, email address, and password. The application implements secure password storage techniques, such as encryption and hashing, to protect user passwords from unauthorized access. This ensures that even in the event of a security breach, user passwords remain securely stored and cannot be easily deciphered.

During the login process, the application verifies the authenticity of user credentials entered on the login page. This authentication step acts as a security checkpoint, ensuring that only authorized users can access their accounts and associated data. By validating the user's identity, the application prevents unauthorized access to user schedules and other personal information. The user authentication mechanisms implemented within the Life Assist application establish a secure environment for users to manage their data and schedules. These measures ensure that user data remains confidential and protected from unauthorized access, fostering trust and confidence in the application's security framework.

III Usability Evaluation

In trying to enact evaluation for this project, we opted to the use of cognitive walkthrough method due to some circumstances that preclude us to use the commonly used user-testing input gathering techniques. With going through the processes of cognitive walkthrough to understand how the researchers in this project understood the proposed system from the users' perspectives by predicting and simulating the thought processes of a user when engaged to our application.

A. *Tasks*

The researchers have arranged some set of available tasks to be completed using the lifestyle assistance smart mirror module application, these tasks include setting-up the daily activity planner, observing the points manager function and subfunctions to each activity, testing the notification message functions, correctly reviewing points calculated by the system, adding, and removing contacts, observing feedback based on points recorded, testing data integrity and correctness between smart mirror device application and the mobile application of the module.

B. *Evaluation Procedure and Results*

The authors have equally undertaken a structured procedure that allows us to overcome the setbacks to gather required data for evaluation. As mentioned above, there were several mediated tasks that we need to look into, in a setting similar to testing functionalities of programs modules, the authors who also acts as the impromptu observer/evaluator for this cognitive walkthrough evaluation process have well familiarized with the goals of each of those modules that is going to be perceived by the general user, and from that point the simulation of user execution of the program is done, or at the very least the modules that were able to be completed by the time this step is taking place.

After each of the functions has been observed and details of how they behaved are noted, the evaluation for those functions is then carried out. Information gathered from the evaluation is presented in the succeeding tables:

TABLE 2.
PLANNER MODULE TESTING

Test Case	***Test Steps***	***Test Data***	***Expected Result***	***Actual Result***
Check input function for planner	1. Activate system module 2. Input needed data into the input field	Activity details: Meeting Time: 10:10	Accepted and recorded	Achieved
Delete an activity	1. Choose an activity to be deleted 2. Click the 'x' button	One available activity on the recorded list	Activity record deleted	Achieved
Testing Auto-Activity Suggestion	1. Click the auto-add button	None	Shows sample workout or reminder of *Sunnah* activity at set time	Failed (only shows dummy data)

https://doi.org/10.31436/ijpcc.v10i2.489

The activity planner module's expected result is very simple. It receives input from user in the form of details of an activity and the time it is expected to take place and then the accompanying points-assigning subfunction of the point-manager function allows each activity to be assigned a set number of point(s). As of the writing of this article, the observation resulted in minimum level of output that only consisted of recorded activity, time, and points. But the points assignment is still not correctly calibrated.

TABLE III.
POINT MANAGER MODULE AND FEEDBACK SUBFUNCTION TESTING.

Test Case	*Test Steps*	*Test Data*	*Expected Result*	*Actual Result*
Automatic point assignment	1. Create an activity to be recorded. 2. Observe the point detail	Sample Activity Details Random Time (09:00)	Show a random point assigned to a 'dummy' activity record	Achieved
Point counter function calculation observation	1. Create an activity record 2.Wait until the appointed time for the calculation module to be shown	Sample Activity Details Random Time (09:00)	Show total activity time	Achieved
Feedback presentation based on achieved points	1. Wait for the appointed time set in the system and observe the feedback message	None	Show a sample feedback message	Failed

It is also deemed that point manager functions, which covers almost everything related to the points system this entire application is based on, as something to be thoroughly checked. Users are expected to find the correct range of points, after calculations that has been mentioned on previous section, assigned to the activity that they input to the application' record list depending on the level of importance of each activity. It is found that the activity is still being assigned random points from 1 to 10 and is ignoring the rule for assigning the points that has been set beforehand. Another part that is observed is the feedback subfunction, which is a subset of the point manager functionality. This module revolves around majority of the main objectives of this project, in which it handles how the program can provide an appropriate feedback based on how many points that is gathered by the users by accomplishing their activities for a day, and with that user may do retrospection on how they conduct their daily activities. The result that should be displayed on the Feedback subfunction still doesn't provide appropriate information for each range of total points. The output feedback still provides one general feedback, as it is currently set under dummy data.

TABLE IV
NOTIFICATION MODULE TESTING

Test Case	*Test Steps*	*Test Data*	*Expected Result*	*Actual Result*
Show Sample message to check output	1. Activate the MagicMirror program for smart mirror and observe the supposed message notification	None	Correctly showing a sample notification message	Achieved
Motivational Quotes notification message check	1. Activate the Magic Mirror program for smart mirror and observe the supposed message notification	None	Correctly showing a sample motivational notification message	Achieved
Checking for activity reminder notification message	1. Activate the Magic Mirror program for smart mirror and observe the supposed message notification	None	Correctly showing a sample reminder notification message	Achieved
Checking the notification function for presenting health advice and Prophetic 'Sunnah' reminders	1. Activate the Magic Mirror program for smart mirror and observe the supposed message notification	None	Correctly showing a sample advice and/or reminder notification message	Achieved

As it was mentioned under the methodology, the notification function/module is generally handling all kinds of notifications the lifestyle assistance module application may send out. This function is evaluated by observing if it can give out the supposed messages of reminder of an upcoming activity. The test therefore is done by using

dummy information of an activity and its supposed time to see if the reminder notification is actually being sent out, another subset of this function evaluation is to observe if the notification can give out supposed tips and reminders on health advices and suggestions on spiritual teachings that can be done to contribute to users' wellbeing. The resulting observations being done have shown that only the activity reminder module is being shown correctly and the needed specific time, while the health advice and reminders module has been set up but needs more adjustments.

C. *Data Analysis and Comments*

From the results received from the experimental walkthrough, there are still lots of work to do to improve the application based on the users' reviews on the promised functionality. There is the need to adjust correctly most of the application parts. There are still some components that are not providing the expected output. This is mostly suspected to be due to faulty synchronization between modules of the lifestyle assistance module.

Also, due to developmental setbacks that revolve around data synchronization and database management we couldn't simulate the functions created for the mobile application version of the proposed smart mirror module application. This preliminary result for the technicality report shall be updated in future updates in our endeavor to realizing a fully functional beneficial system.

IV. SDG Discussions

This work is an attempt to create a system, an IoT device, that can provide better quality of life through an alternative way of creating a structured lifestyle. The system was implemented through an application of Smart Mirror that allows people to arrange their daily activities, receive helpful suggestions, reminded of activities that revolves around the enhancement of physical, mental, and spiritual well-being, as well as a way to monitor progress of the activities by assigning points and providing feedback. The project is considered to promote one of the Sustainable Development Goals which is the ensuring of healthy lives and promote well-being for all ages (SDG 3) as well as SDG9 – Industry, Innovation & Infrastructure.

V. Conclusions

The focus of this study is the use of smart mirrors and IOT. Every morning, before leaving their homes, humans look in the mirror at least once to begin their day. The intelligent mirror system offers humans a comprehensive solution for effectively managing their activities to avoid time wastage. Day-to-day information can be accessed securely through the intelligent mirror. The smart mirror equally provides additional information such as the list of activities, the weather, time, date, calendar, daily plan, daily schedules with notifications, and point counts. The user will be able to monitor their progress daily and remain consistent as a result of this.

The team used a computing technology with the assistance of available resources to make significant modules to develop the smart mirror program to implement a mirror used for an enhanced and effective user experience. Ultimately, the project is still in the preliminary version stage and requires further enhancement to meet some of the system's requirements. We hope that perhaps the scholars concerned with artificial intelligence, monitoring devices, and IoT might very well benefit from the research. It also provides better insights into the implementation of successful works. Throughout the course of this project's development, research into how these things work was carried out. We came up with the concept of installing a Life Assist app that improves physical, spiritual, and mental health..The entertainment functions of this system make it possible for users to acquire a distinctive experience. Any device in the home environment can be applied and enabled through the IoT devices controlling the sub-system.

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]. D. D. Farhud, "Impact of Lifestyle on Health," Iran J. Public Health, vol. 44, no. 11, p. 1442, Nov. 2015, doi: 10.5040/9798400690945.ch008.
[2]. D. M. Campagne, "Accountability for an unhealthy lifestyle," Eur. J. Health Econ., vol. 22, no. 3, pp. 351–355, 2021, doi: 10.1007/s10198-020-01192-x.
[3]. "Spiritual Wellness | Health & Wellness," Accessed: Jul. 30, 2024. [Online]. Available: https://www.unh.edu/health/spiritual-wellness
[4]. A. Bożek, P. F. Nowak, and M. Blukacz, "The Relationship Between Spirituality, Health-Related Behavior, and Psychological Well-Being," Front. Psychol., vol. 11, Aug. 2020, doi: 10.3389/fpsyg.2020.01997.
[5]. A. Muneer, S. Fati, and S. Fuddah, "Smart health monitoring system using IoT based smart fitness mirror," TELKOMNIKA Telecommun. Comput. Electron. Control, vol. 18, pp. 317–331, Jan. 2020, doi: 10.12928/TELKOMNIKA.v18i1.12434.
[6]. T. Tufte, "Design and Development of a Healthy Lifestyle Tool for Mobile Devices," University of Bergen, 2016. [Online]. Available: https://bora.uib.no/bora-xmlui/handle/1956/15610
[7]. M. Farshoukh, "Prophetic Mental Health," J. Islam. Soc. Sci. Humanit., vol. 17, pp. 75–96, 2017, [Online]. Available: https://abqarijournal.usim.edu.my/index.php/abqari/article/view/88/74
[8]. A. Heydari, F. Khorashadizadeh, F. H. Nabavi, S. R. Mazlom, and M. Ebrahimi, "Spiritual health in nursing from the viewpoint of Islam," Iran. Red Crescent Med. J., Jun. 01, 2016, doi: 10.5812/ircmj.24288.
[9]. N. I. Mohd Fahmi Teng, N. A. Ismail, N. H. Ismail, and T. Ahmad, "Development and Validation of an Educational Booklet for

Sunnah Practices in Improving Quality of Life," Environ. -Behav. Proc. J., vol. 2, no. 5, p. 151, Mar. 2017, doi: 10.21834/e-bpj.v2i5.692.

[10]. [10] M. M. Yusri et al., "Smart mirror for smart life," in 2017 6th ICT International Student Project Conference (ICT-ISPC), 2017, pp. 1–5, doi: 10.1109/ICT-ISPC.2017.8075339.

[11]. [11] J. D. Chaparro et al., "Healthy and Active Ageing," Sensors, vol. 21, no. 7938, pp. 1–40, 2021, doi: 10.3390/s21237938.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.493

Design and Development of Cybersecurity Suite

Wan Aiman Wan Ibrahim, Ahmad Nazrin Ahmad Khalil, Adamu Abubakar *
Dept. of Computer Science, KICT, International Islamic University Malaysia, 53100 Kuala Lumpur, Malaysia.

*Corresponding author: adamu@iium.edu.my
(Received: 8th July 2024; Accepted: 25th July 2024; Published on-line: 30th July 2024)

Abstract— Protecting personal, corporate and government data in the digital age requires cybersecurity. Traditional cybersecurity methods sometimes lack comprehensive and dynamic protection mechanisms as cyber-attacks change and become more sophisticated. A new cybersecurity suite is proposed in this study. It integrates various advanced security technologies into a single user-friendly platform interaction. This paper specifically combines techniques for real-time phishing detection, strong password management, safe encryption and decryption services and an interactive module to promote user awareness and behaviours to improve digital security for individuals and organization. Rapid prototyping is used in iterative and incremental development phases to adapt to changing security needs and user input. This method allows the platform to be constantly improved to satisfy the current cybersecurity standards and react to new threats. The prototyped developed provides proactive digital defence, a complete cybersecurity platform that equips users to defend their digital presence. With the intuitive design and advanced feature set, the prototype aspires to democratize cybersecurity. Empirical testing of the prototype revealed that makes an effective protection of a wider audience without the complexities of security software. This paper contributes in the advances cybersecurity technology and shaping the digital protection measures.

Keywords— Cybersecurity, Cybersecurity-suite, phishing detection, password management

I. Introduction

Cybersecurity protects our computers, networks, data and software from threats, unauthorized access, and harm. This broad field protects digital data using numerous methods. It safeguards online-based programmes from unauthorized access, cyberattacks and web environment vulnerabilities. According to Nema and Wally [1]. Integrating cybersecurity prevention framework would address the needs to unified, easy-to-use online application that incorporates numerous cutting-edge security solutions. Specifically, integrating real-time phishing detection, password strength analysis and safe encryption and decryption can improve users' digital security. This is a crucial motivation of this current study. Where it proposed to design and developed an integrated cybersecurity suits.

The motivation of the research lies with cybersecurity protocols, information security and identity management and that each one of these need the other. This is critical in that computer security involves recognising and responding quickly to security threats. According to Buch et al. [2], operational security involves identifying information assets and setting their safeguards. An organization must utilize this method to maintain security. With its thorough security strategy, user-friendly design and instructional features that promote user comprehension, the platform offers several benefits. Dependencies on human interaction, a reliable internet connection and periodic upgrades to manage shifting cyber threats are also challenges. This study aims to safeguard and enable clients against cyber threats. It does this by offering comprehensive cybersecurity solutions at an inexpensive price that allows individuals and small to medium-sized enterprises to readily access them without the complexity of enterprise-level solutions. These criteria are essential for data and system security and monitoring.

In proposing a unified, user-friendly platform that incorporates a suite of advanced security tools, this research represents a paradigm shift in the approach to cybersecurity. Not only does this comprehensive strategy seek to safeguard against cyber hazards, but it also seeks to inform users on how to maintain a secure online presence. Nevertheless, the development of a solution that effectively balances user accessibility with advanced security measures will present a distinctive set of challenges. These challenges would include the integration of a variety of security functionalities. Plus, the adaptation to new and emerging threats and the necessity of fostering user trust and comprehension of cybersecurity principles would also be included.

This research also presents a suitable approach by suggesting a scalable comprehensive cybersecurity platform that combines modern technologies like real time phishing detection extension with necessary cybersecurity security tools. Moreover, this technique not only fills the holes caused by outdated methods but also improves the system's capacity to quickly adjust to new emergent threats. It also strives to provide comprehensive and user-friendly cybersecurity services that enable clients with varying levels

https://doi.org/10.31436/ijpcc.v10i2.493

of technical knowledge to effectively safeguard their online presence. This solution is designed to have both resilience and usability in order to effectively respond to the constantly changing digital risk environment.

The present cybersecurity environment is characterized by a fragmented approach to digital threats, with most solutions providing narrow [4]. Moreover, there are isolated defences that do not address the complete spectrum of dangers that users confront. This fragmentation will create substantial holes in defences, especially against phishing, malware and advanced persistent threats, which necessitate a more dynamic and integrated approach. Furthermore, the undoubtedly fast development of cyber threats outpaces standard security product update cycles [5]. Cybersecurity demands a system capable of adapting in real time to emerging problems. The goal is to provide a seamless, scalable and a very simple platform that allows users to simply and efficiently secure their digital assets [6]. Furthermore, the tool is sensitive for independently securing an entire platform. The overriding issue is particularly the integration of these tools and technologies into a unified and accessible application that remains at the forefront of cybersecurity innovation [7]. This will provide effective protection for its users in an ever-changing threat scenario [8].

The rest of this paper is organised as follows: Section 2 present the related work. Section 3 is the methodology. Section 4 is the result and discussion and finally Section 5 is the conclusion.

II. Literature Review

There are many previous research studies that developed cybersecurity suites enabling researchers to explore numerous cybersecurity issues to protect digital spaces. Similarly, this current study, seek to explore and discusses cybersecurity trends, methods and issues from major research. Which enable a clear path to the development of a better cybersecurity suite.

Among the most related previous research is the work of Craigen et al. [9] which proposed a framework to explain digital resource management and preservation. The paper provides the technical solutions and strategic resource allocation to defend cyberspace and its assets against threats that violate property rights. Similarly,

Jain and Gupta [10] examine detection of cybersecurity risk associated to phishing websites. They detect fake sites using visual similarities. Some visual-based solutions are beneficial and should be used in cybersecurity to boost protection. To improve detection, the study advises integrating these methods with machine learning.

Goyal and Khurana [11] study cryptography methods for securing vulnerable network connections. Their research emphasizes secure hybrid cryptographic systems that use symmetric and asymmetric key approaches. Mobile and wireless apps must avoid communication channel issues which increase the security threats. Comparing mobile communications security cryptography approaches is the research method. Combining these technologies may increase security, prompting research into optimizing them for low-power mobile devices.

The 2020 Springer report on Industry 4.0 cybersecurity underlines the prevalence of cyber dangers in online applications and the need for industrial application-specific security protocols. The research tracks cybersecurity threats and advises on digital asset protection using OWASP, NIST and MITRE data. Industry 4.0-specific cybersecurity measures are discussed after analyzing industry reports and guidelines. The study raises important considerations about how security solutions can adapt to constantly changing industrial technologies.

Nema BM, Wally [1] established that SQL injection attacks, being the key site security concern in 2019, requires a lot concern. The paper recommends multi-connect architecture to identify and mitigate hazards. Web application security is improved via SQL injection detection and remediation. As the study concludes and may fix a recurring issue, web developers must use advanced security measures like the recommended way in their apps.

Sarker et al. [12] established that cybersecurity data science from an overview of machine learning might improve the entire cybersecurity prevention. This research links theoretical data science applications to real cybersecurity solutions by examining machine learning algorithms for cyber threat prediction and mitigation. According to studies, cyber dangers are complicated making these creative methods difficult to apply. More empirical research is needed to confirm these theories which shows increased interest in AI and machine learning in cybersecurity is highly appreciated. Typically, machine learning techniques applied to cybersecurity dwells on how machine learning can improve cybersecurity. Despite the study of examines machine learning methods and how they may help cybersecurity issues are not certain. Sarker et al. [12] recommends strategies to increase digital security but it calls for more empirical research to test these techniques in real life. The gap between theoretical understanding and real implementation must be closed to produce more robust cybersecurity solutions.

According to Goyal et al. [13], cybersecurity risks and countermeasures covers all current web application cybersecurity concerns and offers remedies. The report's detailed analysis includes recent cybersecurity events and provides an up-to-date threat picture. The paper uses a systematic review technique to evaluate hazards and give cutting-edge solutions revealing the ever-changing nature of web application security. The paper is acclaimed for its comprehensiveness and timeliness but it recognises the need for regular revisions to stay relevant. Because the it

https://doi.org/10.31436/ijpcc.v10i2.493

recognises the rapid rise of technology and cyber methods in the digital world.

Ma et al. [14] established that Personal Information and Password Setup requires people's knowledge of the significance of protecting their personal information affects their password strength. The paper uses a mixed-method approach to perform a thorough research. The surveys part of the research assesses participants' awareness of password security and personal data protection. The finding indicate that security awareness improves password strength. Similarly, the other part of the study shows that security-savvy people choose stronger passwords to that do not associated to the age, and other demographic variables.

Kennison and Chan-Tin [15] revealed that "Taking Risks with Cybersecurity" requires using knowledge and personal characteristics in order to predict self-reported cybersecurity behaviours. That is why the study examines how cybersecurity knowledge and personal traits affect password security. The study employed a quantitative methods and assess participants' cybersecurity knowledge and behaviour. The findings indicate that knowledge, personal traits and reported practices increased cybersecurity expertise leads to enhanced safety processes according to the study.

Following an extensive review of all the previous research studies highlighted. This current research was able to extract a single research gap that is very crucial to the computing community. That is, there is a lack of consolidating cybersecurity preventive measures in majority of the research reviewed. Despite the awareness of different cybersecurity issues, yet the solutions are not provided in a consolidated approach. That is why this current study design a unified cybersecurity platform that integrates essential web and data security tools and develop a prototype suite of the essential security tools, including phishing detection, password strength analysis, encryption/decryption services and a password generator, along with an educational component focused on enhancing users' cybersecurity knowledge and practices.

III. Materials and Methods

This study relied on the formal software development process flow to design, develop and test a prototype of the cybersecurity suite. Specifically, rapid prototyping software development approach was adopted, which tests product functionality, designs and usability. This was done by quickly creating and revising prototypes. This kind of development require regular feedback and adaptation benefit, that is one of the reason for the selection of the approach. Since developers can quickly discover and fix design problems and user requirements makes rapid prototyping a suitable technique to follow.

A. System Design

The proposed system design for this study is presented in Figure 1. The system comprises of three layers as follows:

1. Application Layer:
2. Control Layer
3. Infrastructural layer

The Application Layer involves direct connection with end-users and includes crucial components such as: The Net Infrastructure like the Security APIs and the "System interfaces" for authentication and authorization. Similarly, the layer contents the "content delivery Network" that optimises worldwide content delivery and reducing bandwidth and load times. The layer is also responsible for "Balancing load" as well as spreading network or application traffic across numerous servers for stability and availability. Within this layer, there is a provision of "Firewall" which is essential for security technologies that filter network traffic according to security requirements. Similarly, this research constructs a firewall between a trusted internal network and an untrustworthy external network like the internet to prevent threats and unauthorized access.

The proposed design consider the "User Interfaces" to be part of the "Application layer", where the "End-User Interface" is structured. Crucial to this is the "Normal users" views are set to utilize the front end to inspect URLs or receive phishing alerts and also utilize other tools. Furthermore, the "Admin Screen" is conceptualized to manage users, configure settings and also examine analytics an all-user interface that may incorporate instructional materials and personal settings are the last part of this group.

The "Control Layer" was conceptualized to be responsible for the system's core logic and processing where the "Web Server" which serves as the static material or forwards user interface requests to the application server for dynamic content. Similarly, the "Application Server" is part of the control layer, where it manages all the complicated back-end activities and transactions. Third-Party Services (APIs) involving external and integrated services for data verification and additional information are also set out to be in this layer. Within the control layer, an "Encryption/Decryption Module" that provides users with tools to securely encrypt and decrypt their sensitive data are set out. There is also a provision, of Password Management Module: Generate customizable passwords and password strength checker with crack time estimation.

The next within this layer is the "Phishing Detection Module" where the fundamental component that checks URLs and other content for phishing are set out. Finally, the educational module that provides for an interactive or informational contents on cybersecurity education.

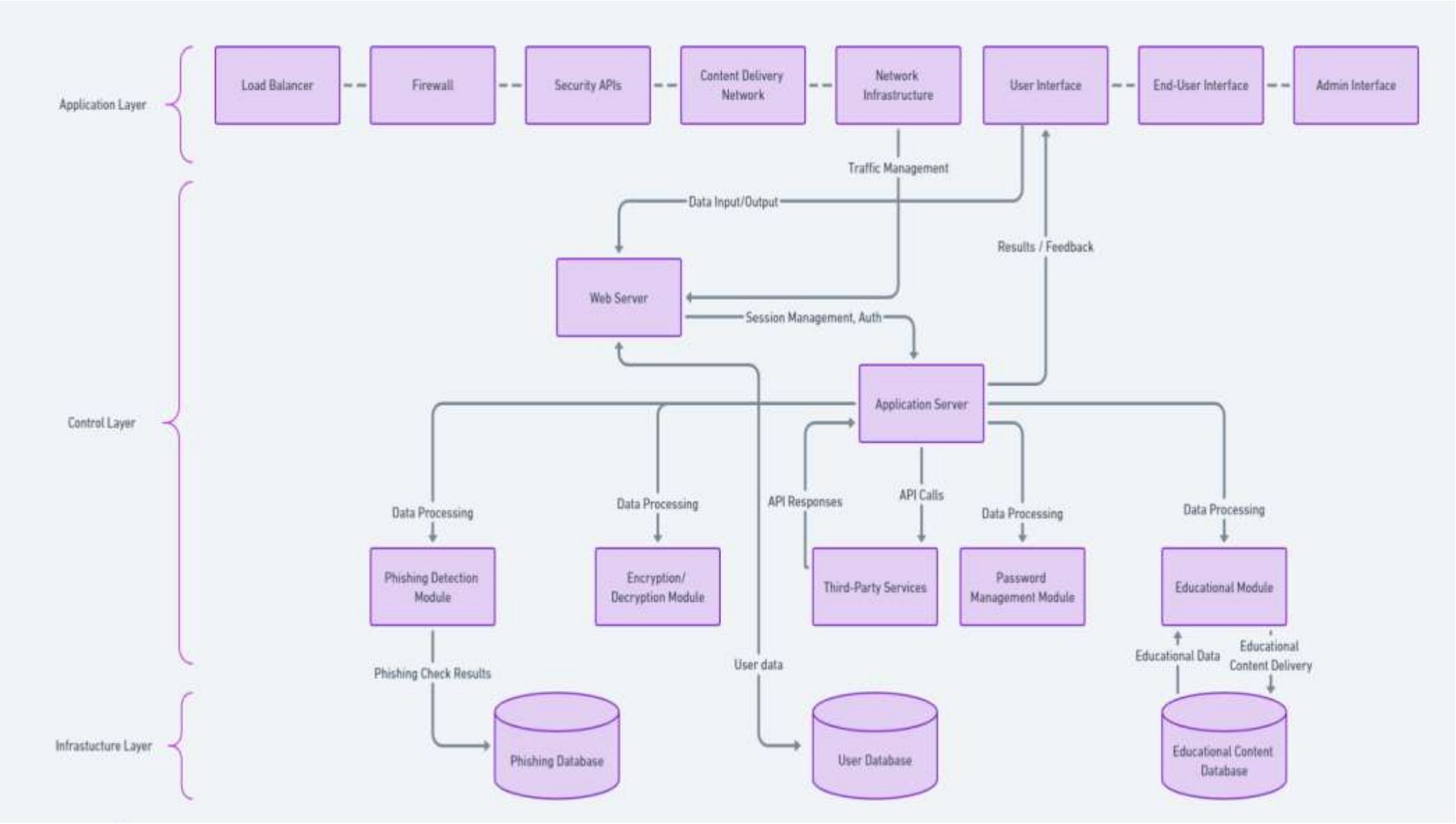

Fig 5. The Entire System Design

The last layer is the "Infrastructure Layer" this layer provide all the necessary computational operations defined for the infrastructure required. The layer provides data and content storage for the entire system. This is typical to the "Phishing Database" where it stores the identified phishing attempts, sites and disputed phishing results. Similarly, within the layer, there is a provision for "Educational Content Database" which search as the "Contains of quiz", "lessons", "videos", and other content for the Educational Module.

The three layers can be best describe as the functional layers, where "data Flow" from the users submitting to the URLs and access instructional content through various interfaces. Web servers handle requests and application servers will process them. The relevant modules analyse URLs, offer content and maintain passwords. The databases store the findings or content. The security and performance module handle the security APIs, CDNs and Load Balancers lock down the system. It will also handle excessive traffic and distribute content efficiently. Finally, the modularity of the architecture separates all the functions into modules for scalability and maintainability. This make it easy to update or modify one element without affecting others. This systematic approach makes the system strong, scalable, easy to manage, secure and user-friendly.

B. *Use Case Scenarios of the system*

There are four use case scenarios of the system proposed in this study (see Figure 2) "Use Case Scenario of Phishing Detection Tool", "Use Case Scenario of Password Management Tool", "Use Case Scenario of Encryption and Decryption Tool", and "Use Case Scenario of Cybersecurity Education Section".

The first use case associated to Phishing detection scenario start with the first action that lies with "Precondition": 1) The user has access to the phishing detection website. 2) The phishing detection system and database are operational.

The second case involve the "Main Flow". The first of this lie with the "User Enters URL/Domain/IP/File". In this case, the phishing detection website asks users to enter or upload URLs, domain names, IP addresses and files. Then follow by the user input the URL/domain/IP/file for analysis. The next action involves "System Processes Submission". The system processes the submission using phishing detection APIs. The detection mechanism evaluates the submission against a database of known phishing sites. After that, the next action is "User Receives Result" that is after examination, the system shows and alerts the user if the URL/domain/IP/file is safe or suspicious/phishing. The next action involves "Update Database". That is If the submission is identified as a new phishing threat, the system automatically updates the phishing database with this new information. This procedure may save URL, information and detection parameters.

The third case involves "Alternative Flow" where the first action is "User Disputes Result". That is, if they disagree with the detection result, users can dispute it. The user can provide feedback or explanations for the inaccurate result. Based on this feedback, system administrators may update the database. The next action that follows involves "Downloading Extension". The user can download a real-time phishing browser extension at any moment. The extension will automatically flag questionable URLs during browsing.

The final case associated to phishing is "Post conditions" where the first action involves the phishing database updating any new findings or corrections. The user will have a clearer understanding of the safety of the URL/domain/IP or file.

Considering that password management and systems hold an important concern. The "Use Case Scenario associated to Password Management Tool" Involve similar flow with the Phishing detections except that the "Precondition" is that the password management tools are accessible and operational on the website. The Admins have established initial password policies and algorithms.

Hence the "Main Flow" is associated to the "User Enters Criteria" where "User input criteria for a new password. Length, complexity (numbers, symbols, etc.) and preferences may be considered". The "Receives New Password" is the system that produces a password that meets the conditions. where "Users see their updated password", Receives Tips / Feedbacks, along with the new password, the system offers password strength tips and advice on building stronger passwords. Similarly, the regenerate New Password (Extension)

offer Users can regenerate passwords if they are unhappy with the generated ones. The system generates a new password using the same or updated criteria.

The Alternative Flow provide "User Inputs Password" In a different scenario, the user inputs any password into the system for validation. Receive Tips/Feedbacks on the system which evaluates the password and offers solutions for strength, security and improvement. In the "Postconditions", "Users receive strong passwords and password security advice" Then the action involve "Keeping password policies and algorithms current with best practices ensures user security.

https://doi.org/10.31436/ijpcc.v10i2.493

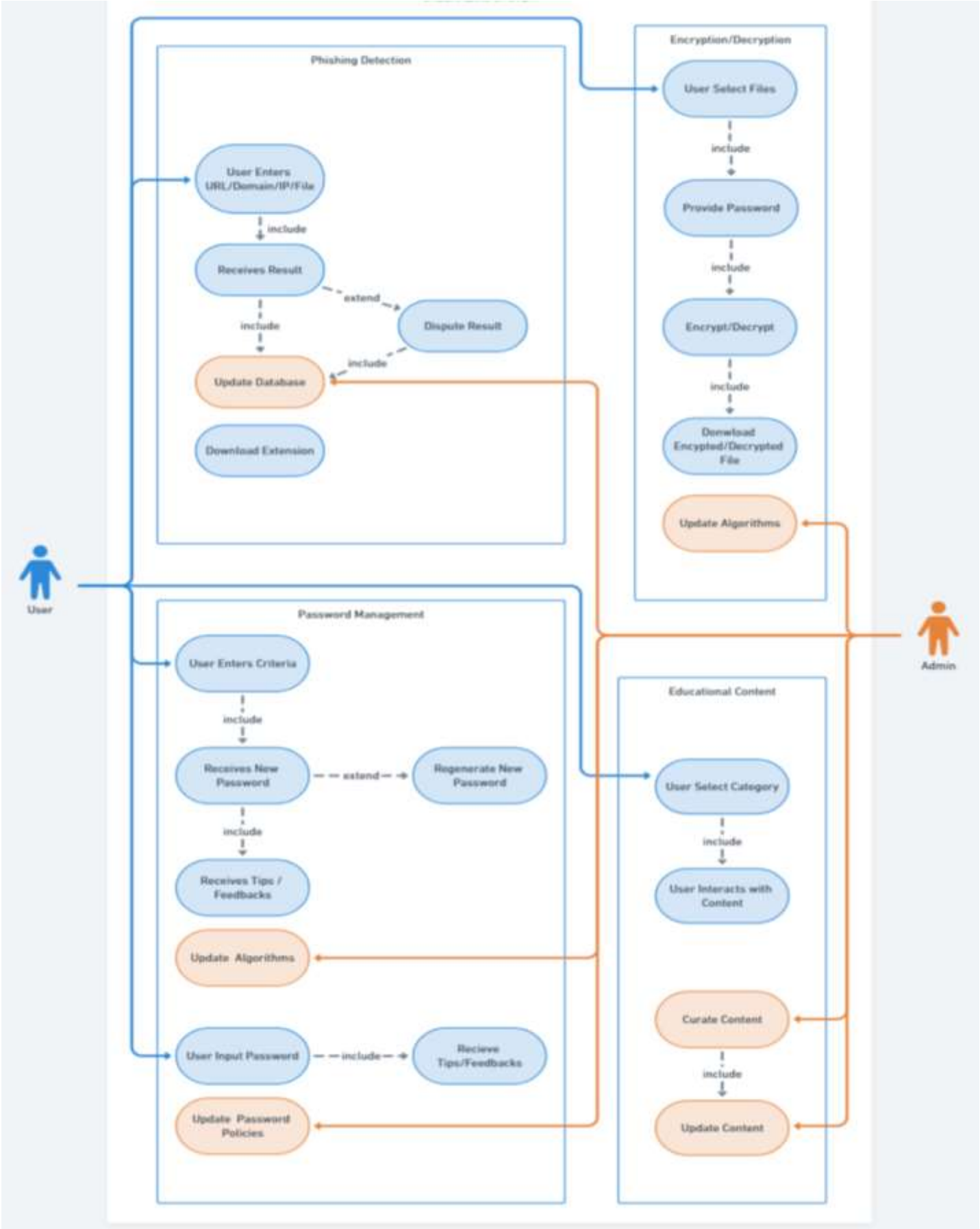

Fig. 2 The Use Case Scenarios of the Functional Flow

https://doi.org/10.31436/ijpcc.v10i2.493

The "Use Case Scenario associated to Encryption and Decryption Tool" provide that the

"Precondition" is the user has access to the encryption/decryption interface on the website. The encryption/decryption algorithms are correctly implemented and functional. The "Main Flow" involve "User Selects Files", Users visit the website's encryption/decryption area. The interface lets users submit files to encrypt or decrypt.

The "Provide Password" action initiated After selecting the files, the user must input a password for encryption or decryption. The key encrypts data and restricts access to them. the Encrypt/Decrypt action was initiated after entering the password, the user chooses to encrypt or decrypt files. The system processes files using the password and current encryption/decryption techniques.

The "Download Encrypted/Decrypted File" Initiated after encryption or decryption, the system lets users download the file. User can download encrypted or decrypted file to local device for use. Finally, the "Alternative Flow" lead the. System or Password Error, If the encryption/decryption procedure fails (e.g., wrong password), system will notify user and may demand for password re-entry or file upload retry. The "Postconditions" lead The files are encrypted or decrypted as requested by the User.

The final "Use Case Scenario" is associated to "Cybersecurity Education Section". The "Precondition" involves the educational content system that is operational and accessible through the website. The content is well-organized into categories. The "Main Flow" lies with the "User Selecting Category" associated to "Users visit Educational Content on the website. Users choose a category based on their interests. The "User Interacts with Content" only after choosing a category, users see articles, videos, tutorials and interactive quizzes. Reading, watching and interacting with material engages users. The "Postconditions" involves the Latest and reliable information is updated in the educational material database. Updated and selected content keeps users aware about phishing and cybersecurity

IV. Results

The system designed provided in the previous section has now been implemented. The result of the system flow is presented in this section. The First user interface of the system is presented in Figure 3. It provides a form features that is a very basic and simple form with clear input boxes for Email/Username and Password. This is accompanied by "Supportive Options" that includes links for registering or recovering passwords. This can provide a smoother user experience and accessibility.

Fig. 3 The First User Interface of the system

The next is the "Extended Form Features" (see Figure 4) where it provides an Identical to the login screen but with a password confirmation area. It ensures users set credentials safely and correctly. This is followed by "Guide for Users" involving a "Very clear instructions" and error handling could improve registration by ensuring users enter proper information.

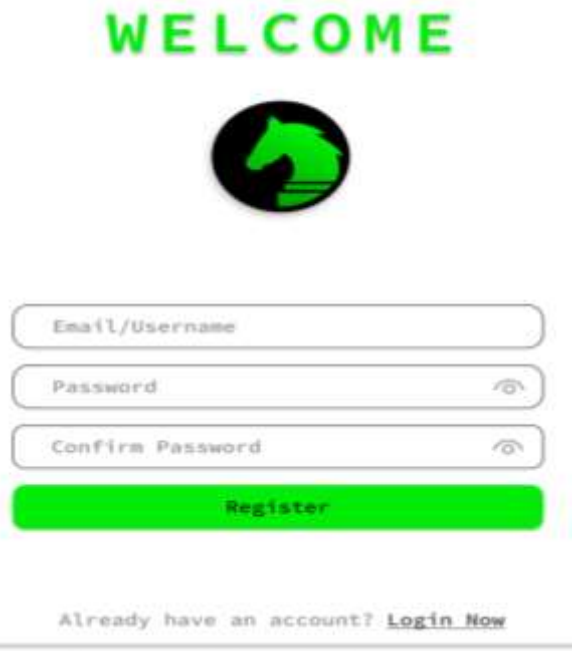

Fig. 4 The registration Confirmation Stage

Figure 5 present the main dashboard after an entry to the system. The dashboard is called "CyberAegiz". It involves a

https://doi.org/10.31436/ijpcc.v10i2.493

"Header and Navigation" where the top portion has the website's logo on the left, centrally oriented navigation buttons for "Home", "Tools" and "Education Hub" on the right, and a search box. The site is easy to navigate with this layout. The Main Content Area involves "A greeting message" with a vivid background and a cybersecurity-focused graphic. Below this are clickable tiles for "Phishing Detection", "Password Management", "Encryption & Decryption" and "Education Hub". The icons and brief descriptions on each tile explain each tool. The "Call to Action" involves a big "Learn More" button urges CyberAegiz users to explore its features. Finally, the "Footer" includes links to "About Us", "Privacy Policy", "Terms of Use" and "Contact Us", which are essential for website credibility and user support.

Fig. 5 The System ROC Curve for Naive Bayes with BOW

The phishing detection module functionality involve a system will scan URLs or uploaded files against a phishing database. The real-time phishing scanning extension is optional to download. Results Interface: Results will show a short summary of the URL status whether it is "Good" or "Suspicious". Educational Section: Teach people about phishing and protection techniques. This can promote safer browsing experiences.

The password management "Dual Functionality" combines password generator with strength checker. Users can customize password restrictions and receive real-time password strength feedback. The Interactive Elements involves the screen has sliders and toggles to define password parameters and visual indicators of user-generated or typed password. An advice and tips section provides practical guidance on building and keeping strong passwords for online security.

The Encryption and Decryption involves "Tool Operations" that involve "A drag-and-drop" or file selection interface simplifies encryption and decryption. Encrypted files are secure with passwords. Process Visualization: After encryption, users can download encrypted files with clear instructions and visual signals. Best Practices: Promotes encryption and provides instructions for safely managing encryption keys and protecting sensitive data.

The Educational model provide the "Read Articles". Many cybersecurity articles are available. Articles may cover broad knowledge, detailed guidelines or best practices. The tabs "All Articles," "General Guides," and "Cybersecurity Practices" enable readers to find articles based on their interest or ability level. Learning Through Multimedia: Articles with several photos may include multimedia features like films, infographics or interactive diagrams to enhance comprehension of sometimes very difficult cybersecurity issues. Interactive Quizzes or Assessments: Educational hubs may feature interactive quizzes or assessments. This could help to test readers' grasp of the topic. It can help retain knowledge and apply theoretical concepts.

V. Conclusion

This paper presents a design and development process emphasizing on rapid prototyping over extensive four cybersecurity modules. The development was performed base on the proposed designed intended to integrated cybersecurity feature into a single dashboard. The prototyped developed is called "CyberAegiz". It was tested and the result guarantee that the suit fit the user expectations and handle cybersecurity concerns. CyberAegiz benefits from rapid prototyping for various reasons. It integrates user and community insights with constant feedback. Feedback is essential for improving the application's functionality and usability and creating effective tools. Cyber threats are dynamic; thus a quick adaptation is very important. The rapid prototyping enables for any design changes. These are definitely necessary for integrating new cybersecurity defenses or responding to new vulnerabilities. The prototyping eliminates the need for major adjustments later in the development process. This optimize resource allocation and minimize lost effort. The outcome of the research can be used in a real-world difficulties and iterative feedback, improving learning style.

Acknowledgment

This research is supported by UMP-IIUM Sustainable Research Collaboration 2022 Research Grant (IUMP-SRCG22-014-0014).

Conflict of Interest

The authors declare that there is no conflict of interest.

References

[1] M.B. Nema, Wally HA. Cybersecurity risks detection and prevention. Al-Mansour Journal. 2019;31(1):65-86.

[2] R. Buch, Ganda D, Kalola P, Borad N. World of cyber security and cybercrime. STM Journal., 2017, 4(2),

[3] I.H. Sarker, Kayes AS, Badsha S, Alqahtani H, Watters P, Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big data. 2020 Dec; 7:1-29.

[4] C. Florackis, Louca C, Michaely R, Weber M. Cybersecurity risk. The Review of Financial Studies. 2023 Jan 1;36(1):351-407.

[5] D.W. Hubbard, Seiersen R. How to measure anything in cybersecurity risk. John Wiley & Sons; 2023 Apr 11.

[6] B. Gumaida, Ibrahim AA. IWDSA: A Hybrid Intelligent Water Drops with a Simulated Annealing for The Localization Improvement in Wireless Sensor Networks. Int. J. Appl. Inf. Technol. Vol. 2024;8(01):15.

[7] B.T. Familoni. Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions. Computer Science & IT Research Journal. 2024 Mar 22;5(3):703-24.

[8] A. Almuqren, Alsuwaelim H, Rahman MH, Ibrahim AA. A Systematic Literature Review on Digital Forensic Investigation on Android Devices. Procedia Computer Science. 2024 Jan 1; 235:1332-52.

[9] D. Craigen, Diakun-Thibault N, Purse R. Defining cybersecurity. Technology innovation management review. 2014;4(10).

[10] A.K. Jain, Gupta BB. Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks. 2017;2017(1):5421046.

[11] R. Goyal, Khurana M. Cryptographic security using various encryption and decryption method. International Journal of Mathematical Sciences and Computing (IJMSC). 2017;3(3):1-1.

[12] A.A. Alarood, Ibrahim AA, Alsubaei FS. Attacks Notification of Differentiated Services Code Point (DSCP) Values Modifications. IEEE Access. 2023 Nov 13;11:126950-66.

[13] D. Goyal, Lavania G, Sharma G. Review of modern web application cybersecurity risks and counter measures. InAIP Conference Proceedings 2023 Jun 15 (Vol. 2782, No. 1). AIP Publishing.

[14] Y. Ma, Twyman, Nathan W., "Cybersecurity: Personal Information and Password Setup" (2018). MWAIS 2018 Proceedings. 20.

[15] S.M. Kennison Chan-Tin E. Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. Frontiers in Psychology. 2020 Nov 4;11:546546.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.491

AutistiCare: A One-Stop Centre for Parents with Autism Spectrum Disorder Children in Perlis

Noor Azura Zakaria*, Nur Syazwana Tajuddin, Nur Faraayuni Sufea Mohd Supian
Dept. of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia

*Corresponding author azurazakaria@iium.edu.my
(Received: 18th June 2024; Accepted: 4th July 2024; Published on-line: 30th July 2024)

Abstract— Individuals with Autism Spectrum Disorder (ASD) typically struggle with social communication and interaction, psychomotor, activity daily living, cognitive, as well as behavioural and intention issues. It is difficult for parents and carers of children with ASD to manage their difficulties, particularly at home and at school. This going to be worst if the parents or carers are not well-equipped with related knowledge on the ASD management. The COVID-19 pandemic situation that spread the world in 2020 has caused significant mental health challenges for parents, such as anxiety and depression, as a result of additional challenges in coping with their children in everyday life, in which the usual therapies that they received at the therapy centre must be completed at home. As a result, supporting them in managing this problem is critical to improving their psychological well-being as a continual attempt from the therapy centre to home. Society nowadays is adapted to the use of the technologies because of COVID-19 phenomena. Strong evidence suggests that online intervention is equally important with a face-to-face approach that has positive effects to autistic children and provides psychological support for the parents. However, there is a gap on the digital intervention platform according to the needs of parents for ASD management especially in Perlis society. Therefore, the purpose of this project is to invent a telehealth platform, characterized as the delivery of healthcare to patients and caregivers via the Internet. The proposed system is AutistiCare targeting parents with ASD children in Perlis that will be developed through a web-based system. The system includes various intervention modules, such as online communities, including online consultations between experts and parents, psychological support through forums, psychoeducation delivered via learning materials such as videos or modules, and service-related postings such as advertisements for ASD programs or seminars. It is envisaged at the end; the system is equipped with optimal ASD management content to support parents with autistic children in Perlis. In addition, it can be a platform to seek knowledge and assistance from the expert remotely.

Keywords— telehealth, Autism, ASD, digital intervention, online intervention

I. INTRODUCTION

Autism Spectrum Disorder (ASD) is a persistent and widespread neurodevelopmental disorder marked by deficiencies in mutual social interaction, social communication, and the presence of restricted and repetitive behaviour [1]. ASD can be seen in early childhood, between 15 and 20 months of age [2]. As of now, autism spectrum disorder has no cure and individuals diagnosed with it must manage the condition throughout their entire lives. Children with ASD often face challenges in terms of behaviour, activity daily living, communication, cognitive, social, and psychomotor [1], [3]–[5]. In addition, children with ASD also often experience other symptoms such as sleeplessness, obsessions, self-injuring behaviour, and hyperactivity [2]. Therefore, an early diagnosis is crucially important to reduce the adverse effects caused by ASD by undergoing regular therapy sessions. However, with the presence of the pandemic Covid-19 in recent years, a lot of therapy centers have been shut down concerning the spreading of the virus. Consequently, this becomes an obstacle for the parents with ASD children to attend their regular treatment. This challenge is further worsened for individuals living in rural areas, where the closure of therapy centers may limit their already restricted access to essential services. For that reason, digital intervention is vital in helping to resolve the issue during the pandemic since the growing awareness of medical applications [6]. Learning from the Covid-19 situation, the acceptance of online learning is increasing because it can be accessed at anytime and anywhere. Hence, a digital intervention model for parents with ASD children in Perlis has been proposed. The proposed system is developed through a web-based system called AutistiCare which targeting parents with ASD children in Perlis. The system will help the parents and caregivers to cope with their ASD children's issues as this system provides the necessary support that can be accessed at any time and anywhere

https://doi.org/10.31436/ijpcc.v10i2.491

as long as there is a connection to the internet. As a result, parents and carers will not be confused while dealing with their ASD children's behaviour, as this platform will provide a necessary intervention that can be done at home.

The rest of the paper is organized as follows: Section 2 provides the background of the study. Section 3 details the methodology. Following that, Section 4 presents the results, and Section 5 concludes with the findings.

II. BACKGROUND OF STUDY

According to statistics, the latest figure revealed by Autism and Developmental Disabilities Monitoring Network estimates that 1 in 59 children has been identified under the Autism Spectrum Disorder (ASD). In Malaysia, as reported by the Ministry of Health Malaysia, the prevalence of ASD in Malaysia was approximately 1.6 in 1000 based on the feasibility study on the use of MCHAT among children of 18 to 36 months of age in child health clinics. The above statistics show that an extreme movement should be taken to help improve the condition of people with learning disabilities, especially when involving ASD children. It is equally essential to assist parents of children with ASD in managing these challenges, as some struggle with controlling their children. Children with ASD frequently face challenges in terms of behaviour, activity daily living, communication, cognitive, social, and psychomotor [1], [3]–[5]. In consequence, it leads them to negative family outcomes such as increased parent stress levels, parent depression, and caregiver burden. Therefore, psychological, and social support are needed to manage child disorder. Although it is not possible for patients who have been diagnosed with ASD to recover from it, at least an effective treatment and intervention can improve a person's condition.

III. METHODOLOGY

The Iterative Software Process Model, which follows agile principles, was chosen for this project for its flexibility and ability to achieve measurable progress through small, iterative cycles. The focus of this methodology is continuous improvement and adaptability to requirements changing. This approach consists of seven phases that include planning, design, development, testing, deployment, verification and launch.

Phase 1: Planning

In this phase, we conducted a literature review on the telehealth component from existing literature and systems. We also collaborated with the stakeholders, which in our case, the experts in ASD and parents with ASD children in Perlis through an interview session to get the user requirements for the system.

Phase 2: Design

In this phase, we analysed the requirements and produce a use case diagram and flowchart for the interaction between the users with the system.

- Design of the system
  In this phase, the overall architecture and structure of the system are designed. It includes identifying the key components, modules, and their interactions within the system. We address the specific requirements of the system, such as providing support for parents, providing educational resources, offering online consultation between parents and experts, and pre-screening.
- Design of user interface
  The user interface was designed taking into account the special needs and characteristics of people with autism spectrum disorder and their parents. The design should be intuitive, visually clear, easy to navigate and simple.
- Design of use case
  During this stage, the use case diagram has been produced. The system involves three actors in total who are parents, consultants, and system administrators. Figure 2 provides a visual representation of the use case.

Phase 3: Develop

After the design of the system was completed, the development phase took place. In this phase, we began implementing interactive prototyping to provide a tangible and dynamic representation of the system flow. For this purpose, Figma, a versatile design tool, was used, allowing our team to create an interactive experience that improved our understanding of system navigation and user interactions before diving into actual development. In the backend we used PHP as the scripting language and MySQL as the database management system.

Phase 4: Testing

After the system was completed, the test step took place. In this phase, we started testing the entire system functionality according to the system requirements. This step is required to identify the errors and verify that the entire application is working as per the stakeholders' requirements. Tests were also carried out to verify the performance, stability and usability of the system.

Phase 5: Deploy

In this phase, the deployment was conducted. It shows how the system functions properly in its environment, including installation, configuration, execution, testing, and making necessary changes before the product goes into production. The webserver and database server used for this purpose is Hostinger.

Phase 6: Review

In this phase, we conduct a review session of the final product with experts and parents with ASD children in Perlis to see whether it meets the needs of the stakeholders, whether the requirements are correct and whether the product works well.

https://doi.org/10.31436/ijpcc.v10i2.491

Fig. 1 Use Case Diagram

Phase 7: Launch

In this phase, we conduct a review session of the completed product with experts and parents of ASD children in Perlis to ensure that it meets the needs of the stakeholders, ensuring the requirements are correct, and additionally the product functions well.

IV. RESULTS

AutistiCare intends to promote the telehealth platform which is easy to be accessed by everyone at any location and at any time as long as there is internet availability. It leverages the conventional autism therapy to a digital platform. This is particularly advantageous for individuals in rural areas who may face challenges in reaching therapy centres. This is because the experts can provide one-to-one intervention plans when observing the children's behaviour through online consultation. Besides, parents and caregivers can stay updated on new modules through the system, allowing them to engage in ongoing interventions for their children with ASD.

AutistiCare is a web-based system that provides autism screening, digital intervention, learning modules, and consultation with experts. It can be accessed from this link: https://autisticare.site/

Five features were provided which are service-related posting, online community (consisting of virtual consulting with the expert), psychoeducation (consisting of learning modules and videos), psychological support through an online forum between the expert and the parents, and pre-screening (consisting of assessment using M-CHAT questions). For the online pre-screening, AutistiCare will suggest the parents to meet expert to have further consultation to discuss about their children condition if the pre-screening results for their children indicate a high risk. It can be scheduled through online consultation with an expert in the AutistiCare website. Figure 3 displays the webpage of the online expert consultation that has two features – schedule consultation and view consultant details.

Fig. 3 Online consultation page for parents

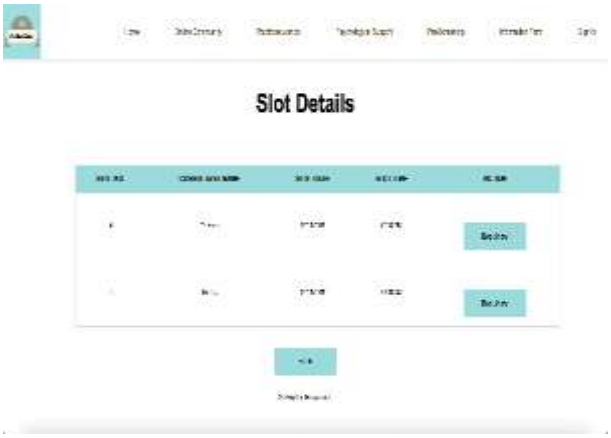

Fig. 4 Online consultation (slot details) page for parent

Figure 4 shows the available consultant's slot details for parents to choose to do the online consultation. The consultant is able to specify their available slot details as displayed in Figure 5 which will be presented to the parents.

https://doi.org/10.31436/ijpcc.v10i2.491

Fig. 5 Online consultation (slot form) page for consultant

Figures 6 and 7 are related to the psychoeducation module that consists of digital intervention. It can be in the form of modules, videos, multimedia and many more. However, at this moment, AutistiCare only provides the modules and video as the learning modules.

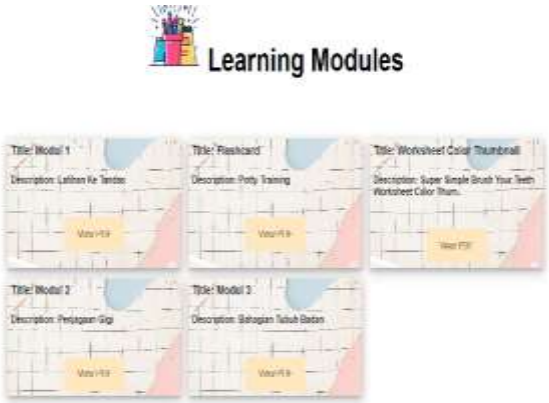

Fig. 6 Psychoeducation (learning modules) page for parents and consultant

Fig. 7 Psychoeducation (learning videos) page for parents and consultant

Another modules provided in the system is the psychological support. The psychological support intends to provide a platform for the parents and carers to further discuss regarding any benefit topics, tips and experiences related to ASD management. It will be beneficial to other audience and readers. Therefore, a forum has been developed in the system as a support for the parents and carers who has ASD children.

Fig. 8 Psychological support (forum) page for parents and consultants

In the pre-screening section, there are M-CHAT questions, which consist of 20 questions as shown in Figure 9. Parents need to respond to all the questions, and the responses along with the results will be stored in the database. If the result indicates that the children is at high risk of having autism, then the parent can schedule an online consultation with the expert through the online consultation section.

Besides, parents can utilize the online modules and videos available in the psychoeducation section to consistently support and overcome issues faced by their children. Moreover, parents and caregivers can reach out to the community for help or post their concerns through the provided forum in the Psychological Support section. This method can encourage them to be more proactive about their children's issues.

Fig. 9 Pre-screening page for parents

Although the system provides a pre-screening section to help parents determine whether their children have autism or not, this may not be entirely accurate and it is recommended to seek expert opinions on the matter. Therefore, parents can arrange a consultation with the expert for a comprehensive assessment and diagnosis. The subject matter expert has the necessary intervention training to conduct a complete assessment taking into

account various aspects of the child's behavior. Therefore, seeking their expertise makes more sense as they provide useful insights into addressing the special needs of children with autism and promoting their well-being in the child's development.

V. CONCLUSION

In summary, the proposed AutistiCare web-based system meets the essential needs of parents and other caregivers of children with ASD in Perlis. Given the challenges of the COVID-19 pandemic and the increasing number of ASD, a digital platform is crucial. It emphasises the wide range of difficulties that children with ASD and their families face as well as the lifelong effects on individuals. The disruption of conventional treatment options caused by the pandemic highlights how urgent it is to find alternative therapies. Given these difficulties, AutistiCare, a web-based system solution, presents itself as an innovative and integrated platform aimed at supporting parents and caregivers in overcoming the challenges associated with ASD. The aim of the project with this integrated platform is to support families with autistic children in Perlis by providing the optimum ASD management content and improving the psychological well-being of parents.

ACKNOWLEDGMENT

This research was funded by Jamalullail Research Grant Scheme (JRGS) with project ID: JRGS22-021-0021.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

REFERENCES

[1] American Psychiatric Association, Diagnostic and Statistical Manual of Mental Disorders. American Psychiatric Association, 2013. doi: 10.1176/appi.books.9780890425596.

[2] R. Oberleitner, S. Laxminarayan, J. Suri, J. Harrington, and J. Bradstreet, "The potential of a store and forward tele-behavioural platform for effective treatment and research of autism," in Annual International Conference of the IEEE Engineering in Medicine and Biology - Proceedings, 2004, pp. 3294–3296. doi: 10.1109/iembs.2004.1403926.

[3] O. Bonnot, V. Adrien, V. Venelle, D. Bonneau, F. Gollier-Briant, and S. Mouchabac, "Mobile App for Parental Empowerment for Caregivers of Children With Autism Spectrum Disorders: Prospective Open Trial.," JMIR Ment Health, vol. 8, no. 9, p. e27803, Sep. 2021, doi: 10.2196/27803.

[4] S. Y. Chu, S. N. S. A. binti Mohd Normal, G. E. McConnell, J. S. Tan, and S. K. D. Joginder Singh, "Challenges faced by parents of children with autism spectrum disorder in Malaysia," Speech, Language and Hearing, vol. 23, no. 4, pp. 221–231, Oct. 2020, doi: 10.1080/2050571X.2018.1548678.

[5] J. L. Matson, M. Sipes, M. Horovitz, J. A. Worley, M. E. Shoemaker, and A. M. Kozlowski, "Behaviors and corresponding functions addressed via functional assessment," Res Dev Disabil, vol. 32, no. 2, pp. 625–629, Mar. 2011, doi: 10.1016/j.ridd.2010.12.011.

[6] Alnaghaimshi N. I., Alhazmi A., Alqanwah S. A., Aldablan M. S., and Almossa M. A., "Autismworld: an Arabic Application for Autism Spectrum Disorder," 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), 2020.

[7] S. Hermaszewska and J. Sin, "End-user perspectives on the development of an online intervention for parents of children on the autism spectrum," Autism, vol. 25, no. 5, pp. 1234–1245, Jul. 2021, doi: 10.1177/1362361320984895.

[8] A. S. Shminan, N. Fauzan, and M. Aren, "The intensity of the research activities on e-learning for care givers of autistic children," in 2015 International Conference on Information Technology Systems and Innovation, ICITSI 2015 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Mar. 2016. doi: 10.1109/ICITSI.2015.7437682.

[9] H. Huang, X. Hei, Y. Gao, and C. Zhang, "Design an applied-behaviour-analysis learning WeChat tool to assess the learning capacities for autistic children," in Proceedings of 2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2020, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 333–340. doi: 10.1109/TALE48869.2020.9368393.

[10] S. Bardhan et al., "Autism Barta - A smart device based automated autism screening tool for Bangladesh," in 2016 5th International Conference on Informatics, Electronics and Vision, ICIEV 2016, Institute of Electrical and Electronics Engineers Inc., Nov. 2016, pp. 602–607. doi: 10.1109/ICIEV.2016.7760073.

[11] H. Chai, "The Background of the Computer Information 3D of Fine Arts Instructional Materials on Autistic Children Effects and Individualized Language Intervention Training Under," in Proceedings - 2021 International Conference on Forthcoming Networks and Sustainability in AIoT Era, FoNeS-AIoT 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 254–258. doi: 10.1109/FoNeS-AIoT54873.2021.00059.

[12] L. Kashani-Vahid, M. Mohajeri, H. Moradi, and A. Irani, "Effectiveness of Computer games of Emotion Regulation on Social skills of Children with Intellectual Disability," in 2018 2nd National and 1st International Digital Games Research Conference: Trends, Technologies, and Applications, DGRC 2018, Institute of Electrical and Electronics Engineers Inc., Jul. 2018, pp. 46–50. doi: 10.1109/DGRC.2018.8712024.

[13] A. Yakkundi., Dillenburger K., and Goodman L., "An inclusive reading programme for individuals with autism and intellectual disability using multi-media: Application of behaviour analysis and Headsprout early reading programme," 2017 23rd International Conference on Virtual System & Multimedia (VSMM), 2017.

[14] S. Bardhan, M. A. Ullah, H. U. Ahmed, M. G. Rabbani, and K. A. Al Mamun, "Autism Express-a cloud-based framework for autism screening, confirmation and intervention," in IEEE Region 10 Annual International Conference, Proceedings/TENCON, Institute of Electrical and Electronics Engineers Inc., Feb. 2017, pp. 414–419. doi:10.1109/TENCON.2016.7848032.

International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.490

A Comparative Performance of Different Convolutional Neural Network Activation Functions on Image Classification

Muhammad Zulhazmi Rafiqi Azhary, Amelia Ritahani Ismail*

Department of Computer Science, Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia, Kuala Lumpur, Malaysia

*Corresponding author amelia@iium.edu.my
(Received: 8th June 2024; Accepted: 16th July 2024; Published on-line: 30th July 2024)

Abstract— Activation functions are crucial in optimising Convolutional Neural Networks (CNNs) for image classification. While CNNs excel at capturing spatial hierarchies in images, the activation functions substantially impact their effectiveness. Traditional functions, such as ReLU and Sigmoid, have drawbacks, including the "dying ReLU" problem and vanishing gradients, which can inhibit learning and efficacy. The study seeks to comprehensively analyse various activation functions across different CNN architectures to determine their impact on performance. The findings suggest that Swish and Leaky ReLU outperform other functions, with Swish particularly promising in complicated networks such as ResNet. This emphasises the relevance of activation function selection in improving CNN performance and implies that investigating alternative functions can lead to more accurate and efficient models for image classification tasks.

Keywords— Activation Functions, Convolutional Neural Network , Image Classification

I. Introduction

Convolutional Neural Networks (CNNs) is a common machine learning algorithm used for image classification tasks. Image inputs are suitable for CNNs because of their ability to capture spatial hierarchies through convolutional layers. There are several factors that affect the effectiveness of a CNN in learning complex image patterns and features; this includes the CNN architecture, optimisation algorithms, and hyperparameters such as activation functions [1].

Activation functions are an important factor that impact the performance of neural networks. This is because they introduce non-linearity into the model. As such, they enable the model to learn from complex data and performs machine learning tasks such as classification. Currently, there are various activation functions that have been developed and are available to be used. These activation functions have their own strengths and limitations over each other. The most commonly used activation functions include Rectified Linear Unit (ReLU), Sigmoid, Tanh, Leaky ReLU, Exponential Linear Unit (ELU), and a recently proposed Swish [2][10].

The purpose of this study is to provide an extensive analysis of these activation functions across different CNN architectures on image classification tasks. We intend to discover further on how the selection of activation function affects the effectiveness of CNNs by systematically evaluating the performance of a simple CNN, VGG-like CNN, and ResNet-like CNN models using an array of activation functions. Our evaluations are done on the CIFAR-10 image dataset.

The findings of this study will assist researchers in selecting optimal activation functions for their CNN models. This will result in a more accurate and efficient neural networks for image classification.

II. Related work

This study presents Cone and Parabolic-Cone activation functions, which outperform ReLU and Sigmoidal functions on CIFAR-10 and Imagenette benchmarks. These new functions enable finer input space division, improving accuracy and training speed with fewer neurons [1]. This suggests a potential shift in neural network design, as they provide superior performance and efficiency compared to traditional ReLU and Sigmoidal functions, particularly for complex, non-linear datasets.

This study compares past and current functions, noting that while ReLU excels in classification, it struggles in physics-informed tasks. Alternatives functions like hyperbolic tangent, Swish, and sine, especially adaptive ones, perform better in complex scenarios [2]. This is because they offer smoother gradients and better adaptability for complex and physics-informed problems compared to ReLU, which can struggle with gradient consistency and specific task requirements.

This study introduces the "seagull" activation function, which, when used in layers handling exchangeable variables, greatly improves performance and reduces errors, even for

https://doi.org/10.31436/ijpcc.v10i2.490

high-dimensional data like CIFAR10 [3]. It can notably enhance neural network performance and error reduction, making it a valuable approach for both low and high-dimensional data.

This study surveys activation functions (AFs) in deep learning, covering types like Logistic Sigmoid, Tanh, ReLU, ELU, Swish, and Mish. It reviews their characteristics and compares the performance of 18 AFs across different networks and datasets to help researchers and practitioners choose the best options [4]. The survey highlights that understanding and choosing the right activation function is crucial for optimising neural network performance, as different functions offer distinct advantages depending on the network and dataset.

This study finds that combining ReLU, tanh, and sin activation functions can optimise neural network performance. ReLU is dominant, but initial layers favor ReLU or LeakyReLU, while deeper layers perform better with more convergent functions [5]. This suggests that the practice of optimising activation functions by combining different types can enhance neural network performance, with ReLU being dominant in early layers and more convergent functions benefiting deeper layers.

This study introduces Saturated Gaussian Error Linear Units (SGELU), SSiLU, and SMish, new activation functions that combine ReLU with non-monotonic functions. Experiments on CIFAR-100 show these functions outperform existing activation functions in various deep learning models [6]. This can significantly enhance performance in deep learning models, as demonstrated by their superior results on CIFAR-100.

This study offers an updated overview of popular activation functions, addressing their properties and evolution from traditional ones like logistic and ReLU to newer functions. It serves as a useful resource for understanding and applying activation functions in neural networks [7]. This indicates that understanding the properties and evolution of both traditional and new activation functions is crucial for effectively applying them in neural networks and deep learning.

This study introduces four new oscillatory activation functions that allow neurons to learn functions like XOR and outperform popular functions in classification tasks. These functions also address the vanishing gradient problem, which occurs when gradients become too small during backpropagation, preventing proper weight updates and training. The paper also discusses various activation functions, including the widely used sigmoid function, known for its nonlinearity and computational efficiency [8]. This enhances learning and performance in neural networks by overcoming the vanishing gradient problem, offering improvements over traditional functions like sigmoid.

This study examines how ReLU activation functions contribute to vulnerabilities in deep learning models to adversarial examples. It proposes a modified ReLU function that enhances robustness against such attacks and shows through experiments that this modification, combined with adversarial training, improves model resilience [9]. This suggests that by modifying ReLU activation functions, it can improve deep learning models' resilience to adversarial attacks, and combining this with adversarial training further enhances robustness.

This study compares a CNN using Swish activation (76% accuracy) with one using Adaptive Piecewise Linear activation (74.4%) for skin cancer detection, showing that Swish as a separate layer improves accuracy and reduces loss [10]. This indicates that using Swish activation as a separate layer in a CNN for skin cancer detection improves accuracy and reduces loss compared to using Adaptive Piecewise Linear (APL) activation, demonstrating the effectiveness of Swish in enhancing model performance.

Fig. 1 shows a comparison between six different activation functions used in neural networks: ReLU, Sigmoid, Tanh, Leaky ReLU, ELU, and Swish. These functions are critical for defining how neurons in a neural network activate, which affects the model's learning ability and performance. It depicts how each function converts input values (x-axis) to output values (y-axis). ReLU (blue line) activates only positive inputs and outputs them directly, whereas Sigmoid (green dashed line) and Tanh (red dashed line) squish inputs to a range of (0, 1) and (-1, 1), respectively, yielding smooth gradients but potentially vanishing gradients. Leaky ReLU (purple dotted line) introduces a slight slope for negative inputs, which alleviates the dying ReLU problem.

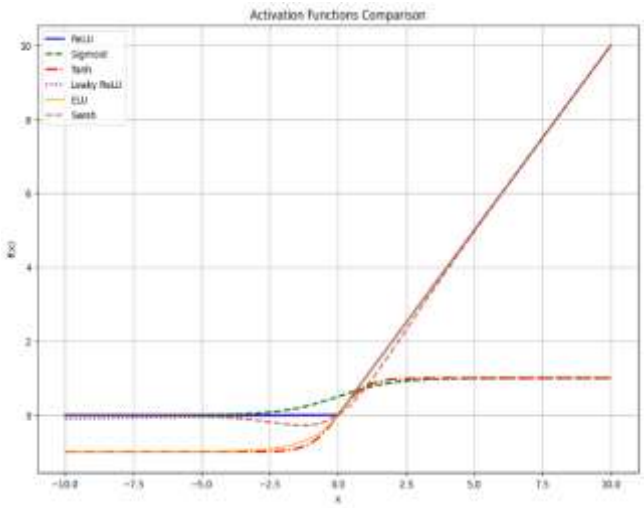

Fig. 1 Activation functions graphs comparison

III. METHODOLOGY

https://doi.org/10.31436/ijpcc.v10i2.490

A. Dataset

The image dataset used in this experiment is CIFAR-10. This dataset consists of 60,000 colour images with an image size of 32 *px* x 32 *px*. It has 10 classes, with 6,000 images per class. It is a common dataset used for image classification algorithms benchmark due to the diversity of its classes and a relatively small image size.

B. Data Preprocessing

The image dataset was transformed to tensors and normalised with a mean and standard deviation of 0.5 for each colour channels.

C. Model Architectures

- Simple CNN: This architecture includes two convolutional layers with the following parameters: filters of [32, 64], kernel size of 3, stride and padding of 1. Then, activation functions are applied to the convolutional layers, followed by a max pooling layer with a kernel size and stride of 2. Finally, a fully connected layer with filters of 512 for classification. It serves as a baseline model to assess basic performance of activations functions.
- VGG-like CNN: This architecture is based on the VGG architecture, it incorporates several convolutional layers with the following parameters: filters of [64, 128, 256], kernel size of 3, and padding of 1. Then, each convolutional blocks are followed by activation functions and max pooling layers with a kernel size of 2 and stride of 2. It ends with three fully connected layers with filter of 512, followed by activation functions for the first two layers. This architecture aims to capture more complex features and evaluate the impact of activation functions in deeper networks.
- ResNet-like CNN: This architecture is based on the ResNet architecture, it includes residual blocks that allow for deep networks by addressing the vanishing gradient problem through skip connections. The convolutional layers in the model have filters of [64, 128, 256, 512] with a kernel size of 3, stride and padding of 1. Then, followed by batch normalisation layers and activation functions. Before passing into the final fully connected layer, the output wen through an average pooling layer. This architecture is used to investigate the performance of activation functions in very deep networks.

D. Activation Functions

- ReLU: It outputs the input directly if it is positive; otherwise, it outputs zero. While it is effective in many situations, it can suffer from the "dying ReLU" issue, where neurons can become inactive and stop learning if they consistently receive negative inputs.
- Sigmoid: It outputs values between 0 and 1, making it useful for binary classification tasks as it can be interpreted as a probability. However, in deep networks, it often encounters vanishing gradients due to its tendency to saturate at the extremes, which can slow down the learning process.
- Tanh: It outputs values between -1 and 1, providing stronger gradients compared to sigmoid. This helps with learning in deeper networks, but it still suffers from gradient saturation at its extreme values, which can hinder training speed and effectiveness.
- Leaky ReLU: It addresses the "dying ReLU" issue by allowing a small, non-zero gradient when the input is negative. This adjustment helps prevent neurons from becoming inactive, maintaining learning efficiency while preserving the simplicity and speed of ReLU.
- ELU: It offers a smooth gradient for negative inputs, which helps mitigate the vanishing gradient issue. It allows for a more gradual learning curve by providing a small gradient when the input is negative, which can lead to faster and more stable training.
- Swish: It combines the input with a sigmoid function applied to that input, creating a smooth and non-monotonic activation function. This characteristic often results in better performance and training efficiency compared to tradition functions like ReLU, especially in deeper networks.

E. Experimental Setup

Each CNN architecture was trained using each activation function on CIFAR-10 dataset. All models were trained using the same set of hyperparameters as shown in Table I. This is done to keep the differences in results solely dependent to the changes of activation function used in the training; hence, ensuring a fair comparison.

TABLE I
CONSTANT HYPERPARAMETERS VALUES FOR EXPERIMENT

	Hyperparameter
Optimizer	Adam
Criterion	Cross-Entropy
Learning rate	0.001
Batch size	64
Epochs	15

F. Performance Evaluation Metrics

Results from this experiment is evaluated using a test set consisting of 10,000 images from CIFAR-10 with the following metrics: accuracy and loss. Accuracy would indicate the overall effectiveness of the model in predicting correct labels, while the loss value computed using the cross-entropy loss function providing insights how well the predictions of the model align with the true labels.

https://doi.org/10.31436/ijpcc.v10i2.490

IV. Results and Discussion

The results obtained from the experiment provide an extensive evaluation of the impact of different activation functions on three distinct CNN architectures: Simple CNN, VGG-like CNN, and ResNet-like CNN, with the CIFAR-10 dataset. The Adam optimiser, cross-entropy loss, a batch size of 64, 15 epochs, and a learning rate of 0.001 are the constant hyperparameters used throughout every experiment. These constant settings enable a fair comparison of the activation functions' performance.

Table II shows that ReLU, Tanh, and Leaky ReLU achieved reasonably high test accuracies of 70.96%, 71.30%, and 72.57%, respectively with the simple CNN. Despite the constant hyperparameters, all activation functions demonstrated varying levels of success, most likely due to their unique mathematical features. Leaky ReLU slightly beat the others in terms of test accuracy, whereas Tanh had the smallest train loss of 0.0017, indicating efficient training. However, Sigmoid and ELU performed poorly, with Sigmoid getting the lowest accuracy of 66.88% and ELU having the largest test loss of 2.382. Swish performed moderately, with a test accuracy of 71.58%, suggesting a modest improvement over ReLU but a greater test loss.

Table III indicates that Swish and Leaky ReLU outperformed other VGG-like CNNs, with test accuracies of 75.84% and 78.67%, respectively. Swish's smooth and non-monotonic characteristics resulted in a considerably decreased train loss, indicating effective gradient flow and better convergence. This performance highlights the potential of novel activation functions such as Swish in deeper networks. However, Sigmoid underperformed significantly, with a test accuracy of 10.00%, showing that it failed to train successfully in this more complex design, most likely due to issues such as vanishing gradients and ineffective convergence.

Table IV shows that ReLU and Swish had the highest test accuracies of 84.03% and 84.43%, respectively for the ResNet-like CNN. Swish outperforming ReLU marginally in terms of train and test losses. The residual connections of ResNet-like architectures take advantage of Swish's characteristics, resulting in greater performance. ELU also produced competitive results, with an accuracy of 83.14% and minimal train and test losses. Sigmoid continues to underperform, supporting the argument that it may not be appropriate for such architectures.

Across all three CNN architectures, the consistent performance of ReLU and its variations (Leaky ReLU and ELU) demonstrates their dependability in different situations. Swish emerged as a formidable competitor, especially in complex architectures such as ResNet, where it achieved the best overall performance. The significant underperformance of Sigmoid in the VGG-like CNN, with a test accuracy of only 10.00%, implies that its fundamental constraints, such as gradient saturation and slower convergence, are not properly compensated by the constant hyperparameters employed.

TABLE II
PERFORMANCE EVALUATION RESULTS FOR SIMPLE CNN

	Test accuracy	Train loss	Test loss
ReLU	70.96%	0.0536	1.9209
Sigmoid	66.88%	0.2307	1.0959
Tanh	71.30%	0.0017	1.4290
Leaky ReLU	72.57%	0.0333	1.9569
ELU	70.03%	0.0665	2.3822
Swish	71.58%	0.0401	2.2202

TABLE III
PERFORMANCE EVALUATION RESULTS FOR VGG-LIKE CNN

	Test accuracy	Train loss	Test loss
ReLU	78.22%	0.1344	1.0914
Sigmoid	10.00%	2.3027	2.3026
Tanh	67.33%	0.8008	0.9240
Leaky ReLU	78.67	0.1109	1.0210
ELU	76.50%	0.1799	1.4022
Swish	75.84	0.1334	1.2459

TABLE IV
PERFORMANCE EVALUATION RESULTS FOR RESNET-LIKE CNN

	Test accuracy	Train loss	Test loss
ReLU	84.03%	0.0491	0.7939
Sigmoid	52.41%	0,3399	1.9650
Tanh	76.72%	0.0794	1.1109
Leaky ReLU	84.24%	0.0453	0.8017
ELU	83.48%	0.0756	0.6840
Swish	84.43%	0.0445	0.7374

The choice of activation function is crucial for optimising CNN performance on the CIFAR-10 dataset. Fig. 2, Fig. 3 and Fig.4 shows that while traditional functions like ReLU and its derivatives continue to be useful, emerging functions such as Swish shows promise, particularly in more complex architectures. This study emphasises the significance of experimenting with different activation functions to obtain optimal performance in specific CNN designs.

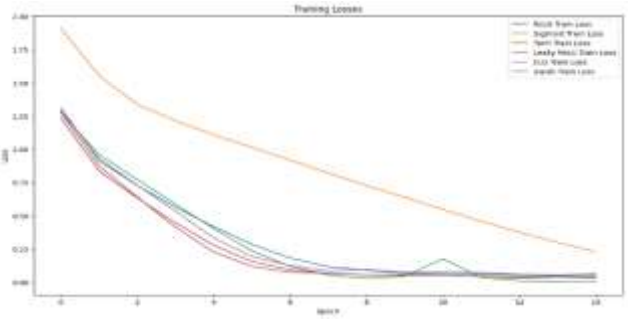

Fig. 2 Simple CNN varied activation functions training losses

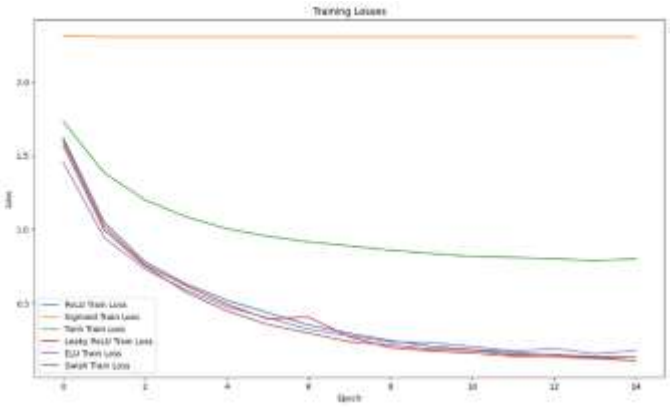

Fig. 3 VGG-like CNN varied activation functions training losses

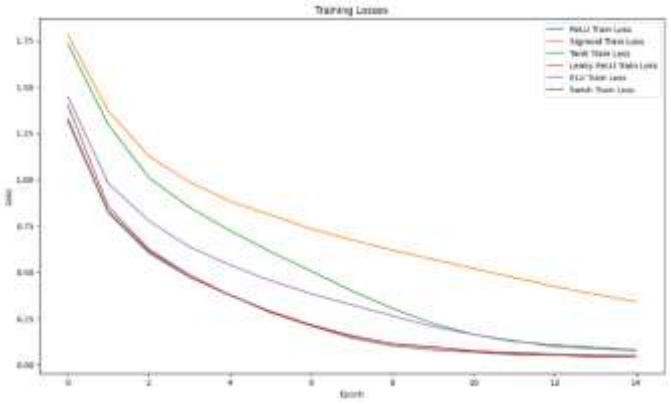

Fig. 4 ResNet-like CNN varied activation functions training losses

V. CONCLUSION

In conclusion, this comparative analysis of activation functions on Simple CNN, VGG-like CNN, and ResNet-like CNN architectures using the CIFAR-10 dataset demonstrates the importance of activation function selection for model performance. Despite constant hyperparameters (Adam optimiser, cross-entropy loss, batch size of 64, 15 epochs, and learning rate of 0.001), activation functions such as Leaky ReLU and Swish performed better than others. Swish outperformed Sigmoid overall, particularly in complex architectures such as ResNet. This study emphasises the need of experimenting with various activation functions to improve CNN performance for specific tasks.

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. Mathew, M. Noel, and Y. Oswal, "A significantly better class of activation functions than ReLU like activation functions," *arXiv*, 2024. [Online]. Available: https://doi.org/10.48550/arxiv.2405.04459.

[2] A. D. Jagtap and G. E. Karniadakis, "How important are activation functions in regression and classification? A survey, performance comparison, and future directions," *Journal of Machine Learning for Modelling and Computing*, vol. 4, no. 1, pp. 21-75, 2023.

[3] F. Gao and B. Zhang, "Data-aware customisation of activation functions reduces neural network error," *arXiv*, 2023. [Online]. Available: https://doi.org/10.48550/arxiv.2301.06635.

[4] D. Sukau, "Activation functions in deep learning: A comprehensive survey and benchmark," *Neurocomputing*, vol. 503, pp. 92-108, 2022.

[5] V. Bansal, "Activation Functions: Dive into an optimal activation function," *arXiv*, 2022. [Online]. Available: https://doi.org/10.48550/arxiv.2202.12065.

[6] J. Chen and Z. Pan, "Saturated Non-Monotonic Activation Functions," *arXiv*, 2023. [Online]. Available: https://doi.org/10.48550/arxiv.2305.07537.

[7] J. Lederer, "Activation Functions in Artificial Neural Networks: A Systematic Overview," *arXiv*, 2021. [Online]. Available: https://arxiv.org/abs/2101.09957.

[8] P. Liu, "A survey on recently proposed activation functions for Deep Learning," *arXiv*, 2022. [Online]. Available: https://doi.org/10.48550/arxiv.2204.02921.

[9] S. Korn, G. Hamerly, and P. Rivas, "Is ReLU Adversarially Robust?," *arXiv*, 2024. [Online]. Available: https://doi.org/10.48550/arxiv.2405.03777.

[10] M. F. R. Mariam, M. F. Farheen, M. M. Manjushree, and M. K. Pandit, "Skin Cancer Detection using CNN with Swish Activation Function," *International Journal of Engineering Research and Technology*, vol. 8, no. 14, 2020.