International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 9, Issue 2 (2023)
https://doi.org/10.31436/ijpcc.v9i2.405

Analyses of Privacy-Preserving Techniques for IoT Data in 6G Networks with Blockchain Integration: A Review

Ahmad Anwar Zainuddin[1*], Nuraina Fitrah Binti Omar [2], Nurul Nadhirah Binti Zakaria[3], Nana Aichata Mbourou Camara[4]

[1,2]*Dept. Computer Science, International Islamic University Malaysia. Kuala Lumpur, Malaysia,*
[3,4]*Dept. Information Technology, International Islamic University Malaysia. Kuala Lumpur, Malaysia*

*Corresponding author: anwarzain@iium.edu.my
(Received: 13rd April 2023; Accepted: 14th May 2023; Published on-line: 28th July 2023)

Abstract— Sixth-generation networks (6G) are predicted to be started use by 2030, supporting the complex communication requirements of a data-centric civilisation where everything is interconnected. The research and academics started to analyse the 6G wireless network technology after the implementation of the 5G technology globally. The 6G networks will be more deliberate to extend cell communication and network capabilities to reach ultra-high-speed connectivity which could precede into the regions where the generation before could not. The new security features need to be advanced to guarantee the data is secure and protect the network from being invaded. The technology of blockchain and integration of the Internet of Things (IoT) has the prospect to revolutionize the networking system. This paper explores the applications of blockchain in IoT networking, addressing challenges such as security, scalability, and trust. Blockchain also enhances security, audibility, and traceability in IoT networks. Use cases in the supply chain, management, healthcare, and smart cities demonstrate the benefits of this integration. Challenges include scalability, energy consumption, interoperability, and privacy concerns. Future research should address these challenges to fully exploit the potential of IoT blockchain applications in networking systems.

Keywords— 6G networks, Wireless network technology, Blockchain technology, Internet of Things (IoT), IoT networking, Security features, Data Security, Privacy concerns, IoT blockchain applications, Networking systems, Supply chain, Management, Healthcare, Smart cities.

I. INTRODUCTION

Although 5G has been widely adopted, the article points out that it would not be able to satisfy all needs after 2030 [1]. According to predictions, 6G will have better coverage, use less energy, and be more affordable than 5G. To accomplish these objectives, the system will employ channel coding techniques, various antenna technologies, waveform design, multiple access, cloud edge computing and network slicing [2]. Additionally, 6G is anticipated to provide fresh intelligent services and apps using big data and AI technology [4,5,6,7]. However, the paper also emphasizes the need for robust security and privacy measures for 6G networks. Several crucial security issues must be resolved, including data encryption, traffic analysis, and threat detection. The large traffic processing needed locally and dynamically can be handled by dispersed security systems, which are recommended as a conceivable resolution [12]. To secure success and sustainability, the 6G report emphasizes the necessity of strong security precautions to be integrated into the technology from the start.

IoT, the Internet of Things and the Internet in general have revolutionized most of all the interactions including human-to-human and human-to-machine in this present day [15]. The core of the IoT ideas is the networking system that has been developed, the current network 5G that is implemented widely in the world, while 6G is still in the research and development process [16]. Moreover, security requirements for both IoT and internet networking core systems rely on the trusted authority that controls the system by failing other's variety of attempts to range or attack from a single point to spoofing [16]. The nature of IoT never leaves the idea of exposure to threats or attacks from the third-party making security a serious challenge faced. Blockchain is a system in which a record of transactions restricted in cryptocurrency usage is maintained across computers linked in a peer-to-peer network [15]. Any industry may utilise the blockchain to make data immutable [7]. Since its introduction in 2009, the use of the blockchain has multiplied thanks to the development of numerous cryptocurrencies, applications for decentralised finance,

non-fungible tokens, and smart contracts [5] [8] [11]. This paper emphasizes several methods in Blockchain of 6G technologies. The first section outlines the introduction of the blockchain's fundamental and 6G concept, and Section 2 displays an overview of the 6G's security and privacy and the blockchain emphasis. Section 3 contains a summary of the article's supporting literature. Section 4 is devoted to methodology, Section 5 is a suggestion to innovate, and Section 6 is the article's conclusion.

II. OVERVIEW OF SECURITY AND PRIVACY IN 6G TECHNOLOGIES

A. Security Evolution of Mobile Cellular Networks

This covers the potential threats to security and privacy brought by various cellular network generations. First of all, the early discussion started with 1G, 2G and 3G Networks. Using analogue modulation for voice transmission, 1G was created in the 1980s. However, it had problems with transmission, security, and handover. Data transmission is not secure since telephone services are not encrypted was neither secure nor private, creating a serious security risk to the network and individuals who used it [50].

Although 2G security has made significant improvements over the previous generation, there are still many flaws that need to be fixed. The difficulty with one-way authentication is the first significant concern with 2G security. In this instance, the user can be authorised by the network but not by the network itself. This leads to a weakness in security that unauthorised base stations can take advantage of to steal user data and personal information. Another issue is end-to-end encryption, which leaves the communication channel vulnerable to assaults because just one part of the network is encrypted while the others are not. To overcome these security issues, network providers must implement two-way authentication mechanisms to stop unauthorised access to the network and user data. To increase the security of 2G networks [51], stricter authentication and encryption standards should be introduced as well as encryption mechanisms to safeguard user data and signalling from unauthorised access. End-to-end encryption should also be used to safeguard the entire communication channel, not just specific portions of it. The security of 2G networks can be considerably improved by addressing these problems, lowering the danger of attacks like data theft and eavesdropping.

IP vulnerabilities, communication channel assaults, wireless interface threats, and Authentication and Key Agreement (AKA) protocol privacy issues are the key security concerns with 3G networks. Despite being introduced in 2000, 3G's 2 Mbps data transmission speed prevents it from supporting sophisticated services like TV streaming, internet surfing, and video streaming. As a result, the security of 2G technology is employed to safeguard 3G networks. Additionally, 3rd Generation Partnership Project (3GPP) supports several privacy concerns for 3G networks, such as safely finding, identifying, and tracking users [52]. Despite these precautions, 3G networks continue to be at risk from Internet Protocol, IP vulnerabilities and assaults. Additionally, one of the major security exposures in 3G that need to be solved is the difficulties connected to gasping users' identities and private information [53,54].

Second of all, it continues with the security matters in 4G & 5G networks. It is evident that as mobile networks develop and offer faster data rates, more intricate systems, and better connectivity, they also encounter more security issues. The main security issues with 4G networks involve wireless radio communication, network authentication, tampering, eavesdropping, and data manipulation. In addition to viruses and operating system threats, tampering with hardware platforms is another security risk that can seriously harm mobile terminal devices. In addition, 4G networks are weak to eavesdropping, replay, and data integrity invasions, as well as unauthorised user issues, location monitoring, and Medium Access Control, MAC layer protocol flaws [56,57,58,59].

The faster data speeds and better services to connect the expanding number of devices as 5G networks can be anticipated in marketing. However, 5G networks also bring up fresh security and privacy issues that require attention. In addition, the open nature of the 5G platform poses privacy concerns with the revelation of users' sensitive data to the open state, increasing the danger of attack while switching between different access technologies and device kinds [60]. Because they do not have device connections, backhaul networks, which are found between access and core networks, have fewer privacy issues than access networks.

In addition, as new techniques are created to speed up 5G networks, security flaws are also introduced. Security challenges arise with Network Functions Virtualization (NFV) services that switch across resources [61,62]. With increased network capacity and additional requirements for new applications, 6G networks will face even larger security difficulties in the future. To solve the latency created by security processes and ensure service and resource availability and continuity, effective security solutions will be needed. For Enhanced Ultra-Reliable and Low Latency Communication (ERLLC) to maintain service continuity and quality, security measures will be essential [63]. Overall, it is clear that network security will

https://doi.org/10.31436/ijpcc.v9i2.405

continue to be a critical issue as mobile networks evolve and advance into the future.

There are also security improvements in 5G networks. In terms of security and authentication procedures, 5G is an enhancement over 4G. Devices can switch between several network types without having to reauthenticate thanks to the adoption of a universal authentication scheme. 5G utilises a Subscription Concealed Identifier (SUCI) during authentication to enhance network security and prevent the transfer of unencrypted data [64,65]. However, the complexity and shortcomings of 5G could lead to security issues. For instance, a hacker might charge another user for network access by taking advantage of the unbounded route between serving and home networks.[66] Additionally, even if 5G-Authentication and Key Management (5G-AKA) defeats International Mobile Subscriber Identity IMSI-catcher assaults, user tracking in 5G is still feasible. Paging users with less than 10 calls and tricking a device into disclosing its Subscription Permanent Identifier (SUPI) by displaying a fictitious pre-authentication notice are two additional ways to locate users [67,68].

In conclusion, all generations of networks contain flaws, and updating the most fundamental protocols might be difficult, leaving vulnerabilities. In older security architectures, supported services, functionality, and known security issues are highlighted. Signalling denial-of-services (DoS), distributed denial-of-service (DDoS), user tracking and energy depletion attacks are all types of 6G security attacks [69]. Poor authentication and resource limitations are problems that affect all network generations and are difficult to fully address.

B. Network vision and essential research projects

Multi-access Edge Computing (MEC), Software-Defined Networking (SDN), Network Function Virtualization (NFV), and network slicing are examples of technologies that were launched with 5G and are still applicable in the context of 6G networks. As a result, the security concerns related to them will still be taken into account when designing safe 6G networks. The possibility of flaws in the SDN controller, interfaces, and application platforms is one of the most important security issues relating to SDN. The scattered nature of 6G networks, distributed denial-of-service (DDoS) assaults, and physical dangers are all threats to MEC [70].

These risks could materialise as a result of the deployment of numerous devices with various levels of embedded security. 6G networks are anticipated to accommodate a wide range of sectors, each with various security requirements, in contrast to local 5G networks that cater to specialised industries. As a result, 6G networks with insufficient security measures could give attackers a chance to attack the network and its devices. The risk of assaults is anticipated to rise as more tiny cells with high-density connections are deployed as part of 6G networks [71]. A hierarchical security mechanism that distinguishes communication security at the sub-network level from sub-network to comprehensive area network security is presented to address the security issues with 6G networks. Furthermore, the usage of Zero Touch Network and Service Management (ZSM) architecture and zero-touch networking in 6G networks could pose serious security vulnerabilities [72]. Data privacy protection in zero-touch networks is difficult due to strict automation requirements with no human interaction, and the rise of attacks in closed-loop systems could be encouraged by complete automation combined with self-learning [73]. To prevent potential attacks and guarantee data privacy, it is essential to adopt strong security measures in 6G networks.

C. The role of blockchain in supporting 6G technologies

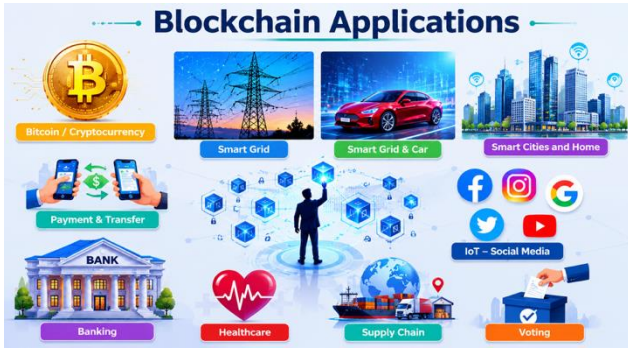

Fig. 1 Blockchain Application in 6G Technology

Figure 1 shows an example for blockchain implementation. Blockchain is currently employed in numerous application fields, such as smart grids, cars, and IoT, after initially exclusively being used in cryptocurrency. [5]. The key technology in the 6G applications of blockchain to support technologies like Reconfigurable Intelligent Surfaces (RIS), Tera Hertz (THz) connectivity, Artificial Intelligence (AI), and tiny cell networks will be necessary to meet the demanding network performance needs of these applications [12]. Dense network deployment is required towards more infrastructure and more complicated network deployment [4]. Network decentralisation is required to give the requisite transparency and trustless in the decentralised network via blockchain to ease network implementation [6]. Very strict security is required of future communication systems because of their in-built security features [16]. Due to the requirements of the applications, the decentralised security and the scalability

https://doi.org/10.31436/ijpcc.v9i2.405

of the blockchain can be found by the selection of appropriate blockchain components [6].

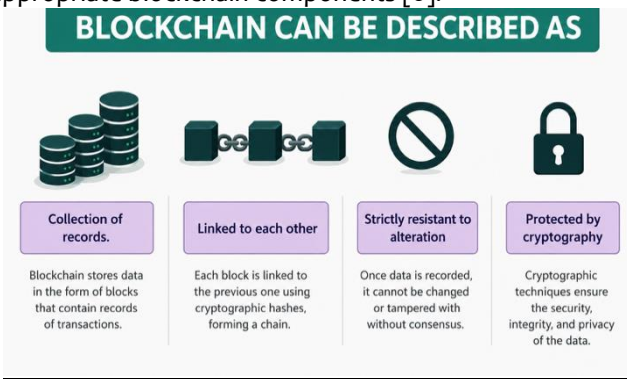

Fig.2 The characteristic definition of a blockchain

Figure 2 shows the simple characteristics definition of a blockchain. The applications of blockchain in 6G networks can enhance security in terms of personal information, data integrity and service accessibility and enable massive scalability [6]. This shows that blockchain technology can increase the security of the 6G network in several aspects such as providing a very secure and tamper-proof way of sharing and storing the data that help to protect against the cyber-attacks [12]. It is to earn the trustworthiness of the user as the privacy of their data can be controlled by their own and decide who can access it [6]. The adaptability of blockchain technology makes it suitable for various applications, and it can provide desired levels of data integrity, non-repudiation, and auditability [7]. Blockchain has the potential to significantly improve secure access control, trusted data interaction, and privacy protection in the context of current 5G and upcoming 6G networks. [13]. By leveraging blockchain's capabilities, 5G and 6G networks can benefit from tracing, certification, and supervision functionalities [14]. These features enable the verification and tracking of data and transactions, ensuring the integrity of information exchanged within the network. Blockchain's decentralised nature also helps in enhancing the security of access control mechanisms, preventing unauthorised access, and ensuring data privacy [7].

Blockchain technology can effectively tackle the challenges of softwarization, decentralisation, and open systems in upcoming 6G networks. It provides a secure and transparent framework to handle software updates, maintain network integrity, and establish trust among network components. As 6G networks heavily rely on software-defined networking (SDN) and network function virtualization (NFV), blockchain offers a promising solution. [20]. Decentralisation is another key aspect of future 6G networks, aiming to reduce reliance on centralised entities and promote distributed decision-making. Blockchain's distributed ledger technology (DLT) architecture aligns well with the decentralised nature of 6G networks, allowing multiple stakeholders to participate and contribute to network operations while maintaining transparency and trust [20]. Finally, open systems are crucial in enabling innovation and collaboration in future 6G networks. Blockchain technology can facilitate the creation of open, interoperable platforms where multiple stakeholders can engage and share resources securely. Smart contracts, a feature of blockchain, can automate the execution of agreements and transactions between different network entities, fostering efficient and transparent interactions [8].

III. LITERATURE OVERVIEW

This literature overview provides a brief summary of at least 15 papers published from 2018 onward of key sources on the IoT and blockchain technology application in networking systems. The table shows a few previous articles related to blockchain in 6G communication.

https://doi.org/10.31436/ijpcc.v9i2.405

Table 1: Survey of blockchain in 6G communication.

Articles	Key Findings / Argument	Supporting Evidence / Sample Characteristics / Methods	Strength / Limitations	Significance / Implications
Research Question: IoT Blockchain application in the network system.				
[5]	The article investigates the uses of blockchain technology outside of cryptocurrencies.	The article provides examples and case studies showcasing the implementation of blockchain technology in diverse industries and sectors.	The strengths lie in the versatility of blockchain technology and potential for enhancing security and transparency, while limitations include scalability challenges and regulatory consideration	The article highlights the significance of blockchain technology in revolutionising industries such as supply chain, healthcare, and finance, with implications for improved efficiency, trust, and data management.
[16]	The significance of security and privacy in 6G networks is covered in the article.	Analysing the flaws in current network topologies and protocols, the authors analyse the possible security and privacy issues in 6G networks.	The article includes a thorough investigation of security issues in 6G networks; nevertheless, since these networks have not yet seen widespread deployment, one weakness could be the absence of empirical evidence.	To safeguard user data and maintain network integrity, which is essential for the successful deployment and adoption of 6G technology, this article emphasises the necessity for stringent security and privacy measures in the development and implementation of 6G networks.
[4]	The article identifies AI techniques for 6G communication networks.	The extensive analysis of existing literature, research papers and empirical studies on AI techniques applied to 6G communication networks.	Potential biases in the book selection process, the evolution of AI technology, and the use of 6G communication networks.	The impacts for rational decision-making, resource management, overall network performance, and network optimisation.
[6]	The potential of the blockchain technology to enhance security and communication in 6G networks	Blockchain's distinctive properties, include decentralisation, immutability, and transparency	In-depth exploration of potential applications and benefits of integrating blockchain technology into 6G networks, highlighting security-enhancing capabilities.	The widespread use of blockchain technology in 6G networks can meet the new security challenges and improve communication by maintaining data integrity, boosting privacy, and providing a decentralised architecture for secure transactions.
[7]	The article explores the application of blockchain mechanisms for enhancing protection in the Internet of Things (IoT) network system.	The article discusses various use cases and applications where blockchain can improve security in IoT, such as secure data sharing, identity management, access control, and tamper-proof auditing.	The article provides a comprehensive overview of the application of blockchain mechanisms for IoT security, covering various use cases and potential benefits.	The insights provided can guide researchers, practitioners, and policymakers in understanding the benefits, challenges, and considerations when implementing blockchain mechanisms in IoT security.

https://doi.org/10.31436/ijpcc.v9i2.405

[8]	The article explores the applications, challenges, and future trends of blockchain smart contracts.	Provide examples and case studies showcasing the potential use of blockchain smart contracts in different industries, including IoT applications.	The article provides a comprehensive overview of blockchain smart contracts, covering their applications, challenges, and future trends, incorporates insights from existing literature and includes examples and case studies to support the arguments.	The information presented can be valuable for researchers, practitioners, and policymakers interested in understanding the applications, challenges, and future directions of blockchain smart contracts, including their relevance to IoT systems.
[20]	The article discusses key technological directions for the development of 6G networks.	Discusses various aspects of 6G networks, including communication technologies, network architecture, spectrum management, and energy efficiency.	Wraps a wide range related to 6G networks, discussing various technologies and their potential implications.	Although it does not directly discuss IoT blockchain applications, the integration of IoT and blockchain is considered an important aspect of future network systems.
[21]	The authors review existing literature and provide insights into the potential requirements and challenges of 6G wireless communications.	Elaborates on the potential applications and requirements of 6G, highlighting the need for advanced technologies to support emerging use cases.	The article does not specifically focus on IoT blockchain applications in the network system. It provides a broader perspective on the vision and potential techniques for 6G wireless communications.	The integration of IoT and blockchain is seen as a key part of future network systems, and the article helps to comprehend the vision and prospective methodologies for 6G wireless communications even though it does not directly mention IoT blockchain applications.
[27]	Emphasises the need to address scalability, latency, energy consumption, consensus mechanisms, interoperability, and security as key challenges.	Debate on the technical aspects, limitations, and requirements for integrating blockchain technology in the context of 6G networks.	The article addresses the research challenges associated with the implementation of blockchain in 6G networks, providing insights into potential areas of improvement.	Instead of concentrating just on IoT blockchain applications in the network system, this study addresses the research challenges of integrating blockchain in 6G networks.
[14]	The article argues that blockchain are decentralised, secure, and transparent transactions, fostering trust and collaboration among different stakeholders in the 6G ecosystem.	The article may include case studies, conceptual discussions, or analysis to support its arguments.	The strengths and limitations of the article are not explicitly mentioned.	The article highlights the potential role of blockchain in shaping the business models and ecosystem of 6G networks. It suggests that blockchain can enhance trust, security, and collaboration among stakeholders, fostering innovation and value creation.

https://doi.org/10.31436/ijpcc.v9i2.405

[22]	The article provides a summary of the current state of research and development in 6G vehicular technology.	The article is a survey paper, so it likely summarises existing research, studies, and literature related to 6G vehicular technology.	The article concentrates on the potential of blockchain technology in transforming 6G networks towards open ecosystem business models.	Highlights the importance of reliable and efficient communication for enabling advanced vehicular services, such as autonomous driving, connected vehicles, and smart transportation systems.
[13]	The article examines the potential benefits and challenges of leveraging edge caching and blockchain in enhancing the performance and efficiency of data delivery in 6G networks.	The articles must provide research papers and academic studies, case studies, and previous surveys to make the article more consistent.	The strengths of the article include its innovative approach that combines blockchain technology and physical layer security, which demonstrates creativity and relevance in the context of emerging 6G networks.	The article explores how edge caching can reduce latency and improve content delivery in 6G networks by bringing data closer to end-users. It discusses how blockchain technology can provide decentralisation, transparency, and trust in the management and operation of edge caching systems.
[15]	The article deals with the inclusion of the smart contract in the blockchain. Smart contracts are positioned to revolutionise	Blockchain smart contracts leverage the capabilities of a blockchain to enable secure and reliable execution of contracts without the need for intermediaries.	Blockchain smart contracts offer automated and secure contract execution on a decentralised network. Their strengths lie in providing trust, transparency, automation, and	The article emphasises how blockchain technology can be used to implement smart contracts, which are self-executing contracts with the terms of the agreement directly written into the code. The authors highlight
	various industries like finance, healthcare, energy, etc.		eliminating intermediaries. They enhance efficiency, reduce errors, and ensure the integrity of data.	the potential benefits of using blockchain smart contracts in various industries, particularly in the context of Industry 4.0 and the Industrial Internet of Things (IIOT).
[10]	The essay explores whether the Internet of Things (IoT) is strengthened by the blockchain.	Incorporating Blockchain into IoT Security, Identity and Access Management Systems, Cloud versus Blockchain Models, and Ensuring Supply Chain Security are a few examples of the different types of IoT systems that are discussed in the article.	The article's strengths are the benefits of blockchain, such as immutability, decentralised structure, and auditability, in addressing security challenges associated with IoT, including IP spoofing and data manipulation.	The article highlights the measure taken to set a new standard for securing IoT applications using blockchain technology. By leveraging blockchain, they intend to enhance the security of IoT ecosystems by providing a standardised framework for building secure IoT devices, applications, and networks.

https://doi.org/10.31436/ijpcc.v9i2.405

[11]	The core concepts of Consistency, Availability, and Partition Tolerance are presented in the article.	The review analyses the advantages and disadvantages of several consensus algorithms, including Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), in terms of establishing consistency, availability, and	For terms of strengths, the article may emphasise that combining edge caching and blockchain technology can lead to enhanced content availability, faster access to data, and improved network efficiency.	The articles accentuate the potential of utilising edge caching, a technique that brings content closer to end-users, combined with blockchain technology in the context of 6G networks.			partition tolerance.		

https://doi.org/10.31436/ijpcc.v9i2.405

IV. Methodology for Blockchain -Based Security And Trust For Iot Ecosystems

Internet of Things (IoT) and Blockchain technology can completely change how we manage and safeguard IoT ecosystems [6-10]. Utilising blockchain's distinctive qualities to build a decentralised and secure environment for IoT platforms, devices, and applications is how these two technologies are being integrated [1]. We can address the issues of security, privacy, trust, and scalability in the ever-expanding IoT ecosystem by integrating the capabilities of IoT and blockchain [14]. We will look at many ways that IoT and blockchain might work together in this post to open up new opportunities and improve the overall effectiveness, security, and translucency of IoT systems [19].

IoT devices connected to the internet can use blockchain technology to build impenetrable records of shared transactions [15]. IoT devices can safely transfer their data to be stored on the blockchain by using private blockchain networks. Due to the permission nature of these private networks, only authorised users can connect and validate transactions [3]. By doing this, it is made sure that the data is reliable and trustworthy. It is quite challenging for any unauthorised person to tamper with or edit the records once the data is posted to the blockchain because it becomes part of an immutable and transparent ledger [7][5]. The tamper-resistant features of blockchain, which provides a high level of data integrity, enable IoT [18].

A potent method to improve security and transparency in IoT ecosystems is the integration of blockchain technology with IoT devices [10]. IoT devices can securely store and share data in a decentralised, tamper-resistant manner thanks to blockchain. Blockchain protects data from unauthorised access and alteration by enforcing its integrity and confidentiality through the use of cryptographic algorithms. Blockchain's distributed architecture does away with the requirement for a central authority, lowering the possibility of a single point of failure and boosting the security of the IoT network as a whole [7]. Furthermore, stakeholders may independently confirm the legitimacy and data integrity thanks to blockchain's transparent and irreversible nature, which also creates a clear audit trail of all transactions. This openness encourages trust among participants and makes it possible to track and trace IoT devices and the data they generate effectively. Blockchain enables direct peer-to-peer interactions between devices, accelerating the IoT sector's efficiency and removing the need for middlemen. As a whole, blockchain equips IoT devices to improve security, guarantee data integrity, and offer transparency to IoT ecosystems, creating the groundwork for a more reliable and secure IoT infrastructure [25].

By doing away with the requirement for a third-party mediator in IoT networks, blockchain-based smart contracts provide a revolutionary solution. "Smart contracts" are self-executing agreements with specified terms and conditions that are recorded on a blockchain [15]. These agreements do away with the requirement for manual intervention by automatically starting specific actions when specific criteria are met. They function as digital agents that, in place of middlemen, check, authorise, or disapprove agreements depending on predetermined criteria. This not only simplifies the procedure but also lowers costs and boosts productivity. IoT devices can use smart contracts to autonomously carry out trusted forms including ownership transfers, resource sharing, and payment execution without relying on a central authority.

IoT systems, applications, and devices can substantially benefit from the scalable and decentralised environment that blockchain technology offers [10]. The enormous amount of data created by IoT devices is frequently too much for traditional centralised systems to handle, which causes bottlenecks and poor performance. IoT networks can divide data processing and storage over several nodes using blockchain's decentralised architecture, doing away with the need for a single central authority. This decentralised strategy boosts the IoT ecosystem's resilience and fault tolerance in addition to scalability [4]. With blockchain, IoT devices can interact and transact with one another directly, doing away with the need for middlemen and cutting down on latency. Peer-to-peer communication has been streamlined, which speeds up transactions and lowers the price of involving third parties. The decentralised nature of blockchain adds an additional layer of security by eliminating single points of failure, making it more challenging for malicious actors to compromise the IoT network [1]. In conclusion, IoT devices, platforms, and applications may operate more effectively, safely, and seamlessly in the quickly changing IoT ecosystem thanks

https://doi.org/10.31436/ijpcc.v9i2.405

to the decentralised environment provided by blockchain technology.

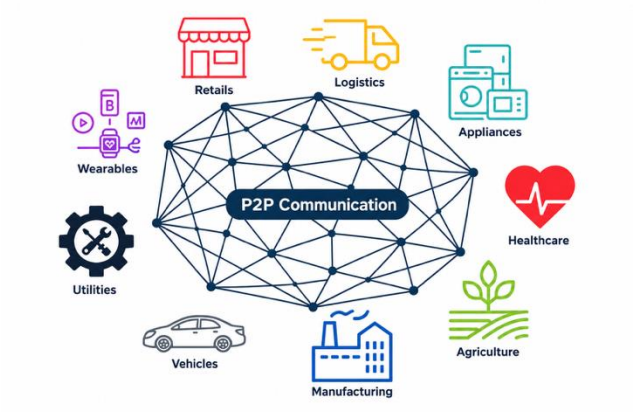

Fig. 3 decentralisation of management using blockchain.

Figure 3 shows the decentralisation of management using blockchain. Blockchain The traceability of food products could be revolutionised by IoT technologies, ensuring accountability and transparency across the supply chain. A food product's entire path from fields to grocery shops to homes may be tracked and validated using blockchain technology on a decentralised, unchangeable database. IoT gadgets, such as sensors and Radio-Frequency Identification (RFID) tags, can be included in the supply chain to gather real-time information on the place of origin, the standard of food, and how it was handled. This data can be safely saved on the blockchain along with other pertinent information like temperature, humidity, and transportation information. With this knowledge, consumers may trace a food product's complete lifecycle and learn more about its origin, manufacturing processes, and history of distribution [40].

Vendors are already striving to integrate the IoT and blockchain in a variety of ways. Trust-building, cost-savings, quicker information exchanges, and scaled security are the four ways that IoT can benefit from blockchain technology, according to a recent whitepaper from Tata Consultancy Services. But there are still a lot of operational and compatibility problems that need to be addressed, much alone fixed. IoT and blockchain pairings have brought up legal and compliance challenges that need to be addressed [37].

By enabling IoT devices to safeguard data and increase industry openness, blockchain technology improves security and transparency in IoT ecosystems. Data security can be improved by using blockchain, which is one of its main benefits. IoT devices are susceptible to cyberattacks because they produce and send enormous amounts of sensitive data [16][46]. Blockchain offers numerous security solutions to address this. First of all, data entered into the blockchain is immutable, which means that once it is done, it cannot be changed or tampered with. It is very safe against unauthorised differences appreciations to this function, which guarantees the integrity and validity of IoT data. To provide another level of protection in a blockchain, data is indeed hashed, but not necessarily before being stored on the blockchain. Instead, data is hashed and included as part of the transaction block [17].

V. RECOMMENDATIONS

Innovating 6G network and application security requires a collaborative and forward-thinking approach that involves detailed research, collaboration between academia and industry, and a comprehensive assessment of potential threats and risks. Strengthening privacy and data protection mechanisms through encryption, anonymization techniques, and strict access controls is essential. Leveraging AI and machine learning can enhance real-time threat detection and mitigation capabilities.

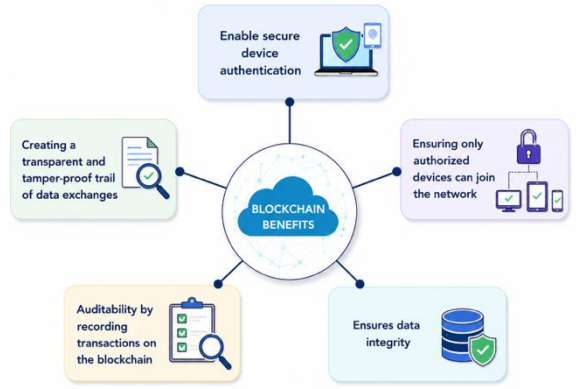

Fig. 4 The idea of a suggested or detailed strategy for innovation.

Figure 4 shows a suggested or detailed strategy for innovation. It visually represents the idea suggested in the innovation process. The implementation of zero-trust architecture, exploration of blockchain technology, and emphasis on secure application development is vital for enhancing security in the 6G environment. Incorporating security automation, continuous monitoring, and staying updated with threat intelligence is key to addressing arising risks. Furthermore, the utilisation of IoT Blockchain applications in 6G networking systems offers significant advantages. IoT Blockchain enables secure device authentication, ensures data integrity and audibility, facilitates decentralised firmware updates, and provides decentralised access control mechanisms.

The blockchain's smart contracts automate secure interactions and improve supply chain security. Collaboration and research between academia and industry are essential for successfully implementing IoT Blockchain applications in 6G networks while considering scalability and interoperability challenges. By embracing ongoing innovation, research, and collaboration, a secure and resilient 6G ecosystem can be built.

From this evaluation, this paper offers a comprehensive analysis of the integration of blockchain technology into IoT networking systems, presenting insightful insights into the benefits and challenges associated with this amalgamation. Nevertheless, it is crucial to recognise that this study does have certain limitations. The absence of a comprehensive technical analysis pertaining to the incorporation of blockchain technology into IoT networking systems presents a challenge in understanding the fundamental mechanisms involved. Moreover, the lack of a comparative analysis of various blockchain-based solutions for IoT networking systems impedes the capacity to evaluate the most effective approaches. Although the paper offers a valuable overview of the subject matter, it is imperative to undertake further research to address these limitations and comprehensively explore the potential transformative impacts of blockchain technology in IoT networking systems in future endeavours.

VI. Conclusion

In summary, the forthcoming implementation of 6G networks by the year 2030, accompanied by robust security protocols and the seamless incorporation of blockchain technology into the IoT infrastructure, presents significant potential for transforming the realm of communication and data administration. By placing emphasis on enhancing authentication, encryption, access control, and threat detection mechanisms, 6G networks are positioned to effectively address the increasing requirements of forthcoming technologies, thereby facilitating a highly interconnected ecosystem. The integration of blockchain technology into the Internet of Things (IoT) networking introduces a novel phase characterized by secure and decentralized data storage, automated interactions, and enhanced trust. These technological advancements present significant prospects in various industries, such as energy management, smart cities, healthcare, and supply chain logistics. However, the presence of obstacles such as scalability, energy efficiency, and interoperability require ongoing investigation and advancement in order to fully exploit the capabilities of IoT blockchain applications.

Acknowledgement

We would like to extend our utmost appreciation to the Computer Network course for its invaluable contribution in enhancing our understanding of IoT security and Blockchain. The knowledge acquired from studying this subject has played a pivotal role in shaping our comprehension of these pivotal domains and has provided us with the essential resources to effectively investigate and utilise the capabilities of these technologies. We express our sincere gratitude to our esteemed professors and educators for their unwavering commitment and diligent endeavours in imparting this indispensable knowledge, facilitating our progress in enhancing our proficiency and understanding in the domain of Computer Networking, IoT security, and Blockchain technology.

Conflict of Interest

The authors declare that there is no conflict of Interest

References

[1] M. S. Ali, M. Vecchio, G. D. Putra, S. S. Kanhere, and F. Antonelli, "A Decentralized Peer-to-Peer Remote Health Monitoring System," *Sensors*, vol. 20, no. 6, p. 1656, Mar. 2020, doi: 10.3390/s20061656.

[2] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A Survey on Space-Air-Ground-Sea Integrated Network Security in 6G," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 1, pp. 53–87, 2022, doi: 10.1109/COMST.2021.3131332.

[3] 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.

[4] K. Sheth, K. Patel, H. Shah, S. Tanwar, R. Gupta, and N. Kumar, "A taxonomy of AI techniques for 6G communication networks," *Comput. Commun.*, vol. 161, pp. 279–303, Sep. 2020, doi: 10.1016/j.comcom.2020.07.035.

[5] 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.

[6] A. H. Khan *et al.*, "Blockchain and 6G: The Future of Secure and Ubiquitous Communication," *IEEE Wirel. Commun.*, vol. 29, no. 1, pp. 194–201, Feb. 2022, doi: 10.1109/MWC.001.2100255.

[7] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet Things*, vol. 1–2, pp. 1–13, Sep. 2018, doi: 10.1016/j.iot.2018.05.002.

[8] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer--Peer Netw. Appl.*, vol. 14, no. 5, pp. 2901–2925, Sep. 2021, doi: 10.1007/s12083-021-01127-0.

[9] I. Acharjamayum, R. Patgiri, and D. Devi, "Blockchain: A Tale of Peer to Peer Security," in *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, Bangalore, India: IEEE, Nov. 2018, pp. 609–617. doi: 10.1109/SSCI.2018.8628826.

[10] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017, doi: 10.1109/MITP.2017.3051335.

[11] G. R. Carrara, L. M. Burle, D. S. V. Medeiros, C. V. N. De Albuquerque, and D. M. F. Mattos, "Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking," *Ann. Telecommun.*, vol. 75, no. 3–4, pp. 163–174, Apr. 2020, doi: 10.1007/s12243-020-00751-w.

[12] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," *Sustain. Cities Soc.*, vol. 63, p. 102364, Dec. 2020, doi: 10.1016/j.scs.2020.102364.

[13] W. Sun, S. Li, and Y. Zhang, "Edge caching in blockchain empowered 6G," *China Commun.*, vol. 18, no. 1, pp. 1–17, Jan. 2021, doi: 10.23919/JCC.2021.01.001.

[14] S. Yrjola, "How Could Blockchain Transform 6G towards Open Ecosystemic Business Models?," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, Dublin, Ireland: IEEE, Jun. 2020, pp. 1–6. doi: 10.1109/ICCWorkshops49005.2020.9145223.

[15] S. Munirathinam, "Industry 4.0: Industrial Internet of Things (IIOT)," in *Advances in Computers*, Elsevier, 2020, pp. 129–164. doi: 10.1016/bs.adcom.2019.10.010.

[16] 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.

[17] 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.

[18] 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.

[19] C. De Alwis *et al.*, "Towards 6G: Key technological directions," *ICT Express*, p. S2405959522001485, Oct. 2022, doi: 10.1016/j.icte.2022.10.005.

[20] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G Wireless Communications: Vision and Potential Techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul. 2019, doi: 10.1109/MNET.2019.1800418.

[21] G. Kirubasri, S. Sankar, D. Pandey, B. K. Pandey, H. Singh, and R. Anand, "A Recent Survey on 6G Vehicular Technology, Applications and Challenges," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India: IEEE, Sep. 2021, pp. 1–5. doi: 10.1109/ICRITO51393.2021.9596147.

[22] W. Li, Z. Su, R. Li, K. Zhang, and Y. Wang, "Blockchain-Based Data Security for Artificial Intelligence Applications in 6G Networks," *IEEE Netw.*, vol. 34, no. 6, pp. 31–37, Nov. 2020, doi: 10.1109/MNET.021.1900629.

[23] H. Viswanathan and P. E. Mogensen, "Communications in the 6G Era," *IEEE Access*, vol. 8, pp. 57063–57074, 2020, doi: 10.1109/ACCESS.2020.2981745.

[24] S. Zhang, J. Liu, H. Guo, M. Qi, and N. Kato, "Envisioning Device-to-Device Communications in 6G," *IEEE Netw.*, vol. 34, no. 3, pp. 86–91, May 2020, doi: 10.1109/MNET.001.1900652.

[25] N. M. Nasir, S. Hassan, and K. M. Zaini, "Evolution Towards 6G Intelligent Wireless Networks: The Motivations and Challenges on the Enabling Technologies," in *2021 IEEE 19th Student Conference on Research and Development (SCOReD)*, Kota Kinabalu, Malaysia: IEEE, Nov. 2021, pp. 305–310. doi: 10.1109/SCOReD53546.2021.9652750.

[26] T. Sharma, S. K. Prasad, and V. Sharma, "Research challenges of Blockchain in 6G Network," in *2022 IEEE Delhi Section Conference (DELCON)*, New Delhi, India: IEEE, Feb. 2022, pp. 1–7. doi: 10.1109/DELCON54057.2022.9753098.

[27] 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.

[28] S. Chen, Y.-C. Liang, S. Sun, S. Kang, W. Cheng, and M. Peng, "Vision, Requirements, and Technology Trend of 6G: How to Tackle the Challenges of System Coverage, Capacity, User Data-Rate and Movement Speed," *IEEE Wirel. Commun.*, vol. 27, no. 2, pp. 218–228, Apr. 2020, doi: 10.1109/MWC.001.1900333.

[29] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.

[30] D. C. Nguyen *et al.*, "6G Internet of Things: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, Jan. 2022, doi: 10.1109/JIOT.2021.3103320.

[31] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A Survey of Blockchain-Based Strategies for Healthcare," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–27, Mar. 2021, doi: 10.1145/3376915.

[32] P. Singh, Z. Elmi, Y. Lau, M. Borowska-Stefańska, S. Wiśniewski, and M. A. Dulebenets, "Blockchain and AI technology convergence: Applications in transportation systems," *Veh. Commun.*, vol. 38, p. 100521, Dec. 2022, doi: 10.1016/j.vehcom.2022.100521.

[33] S. Najjar-Ghabel, S. Yousefi, and H. Karimipour, "Blockchain Applications in the Industrial Internet of Things," in *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*, H. Karimipour and F. Derakhshan, Eds., Cham: Springer International Publishing, 2021, pp. 41–76. doi: 10.1007/978-3-030-76613-9_4.

[34] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain Applications in Smart Grid–Review and Frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019, doi: 10.1109/ACCESS.2019.2920682.

[35] A. H. Mohsin *et al.*, "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Comput. Stand. Interfaces*, vol. 64, pp. 41–60, May 2019, doi: 10.1016/j.csi.2018.12.002.

[36] T. R. Gadekallu *et al.*, "Blockchain for Edge of Things: Applications, Opportunities, and Challenges," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 964–988, Jan. 2022, doi: 10.1109/JIOT.2021.3119639.

[37] R. Jayaraman, A. Srivastava, and M. Kumar, "Blockchain technology for protection of biomedical documents in healthcare society," *Int. J. Internet Technol. Secur. Trans.*, vol. 12, no. 6, p. 566, 2022, doi: 10.1504/IJITST.2022.126470.

[38] M. Krichen, M. Ammi, A. Mihoub, and M. Almutiq, "Blockchain for Modern Applications: A Survey," *Sensors*, vol. 22, no. 14, p. 5274, Jul. 2022, doi: 10.3390/s22145274.

[39] G. Zhao *et al.*, "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions," *Comput. Ind.*, vol. 109, pp. 83–99, Aug. 2019, doi: 10.1016/j.compind.2019.04.002.

[40] A. Hasankhani, S. Mehdi Hakimi, M. Bisheh-Niasar, M. Shafie-khah, and H. Asadolahi, "Blockchain technology in the future smart grids: A comprehensive review and frameworks," *Int. J. Electr. Power Energy Syst.*, vol. 129, p. 106811, Jul. 2021, doi: 10.1016/j.ijepes.2021.106811.

[41] S. Al-Megren *et al.*, "Blockchain Use Cases in Digital Sectors: A Review of the Literature," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada: IEEE, Jul. 2018, pp. 1417–1424. doi: 10.1109/Cybermatics_2018.2018.00242.

[42] P. Bhattacharya *et al.*, "Coalition of 6G and Blockchain in AR/VR Space: Challenges and Future Directions," *IEEE Access*, vol. 9, pp. 168455–168484, 2021, doi: 10.1109/ACCESS.2021.3136860.

[43] Y. Zuo, "Making smart manufacturing smarter – a survey on blockchain technology in Industry 4.0," *Enterp. Inf. Syst.*, vol. 15, no. 10, pp. 1323–1353, Nov. 2021, doi: 10.1080/17517575.2020.1856425.

[44] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512–529, Aug. 2019, doi: 10.1016/j.future.2019.02.060.

[45] B. Wan, C. Xu, R. P. Mahapatra, and P. Selvaraj, "Understanding the Cyber-Physical System in International Stadiums for Security in the Network from Cyber-Attacks and Adversaries using AI," *Wirel. Pers. Commun.*, vol. 127, no. 2, pp. 1207–1224, Nov. 2022, doi: 10.1007/s11277-021-08573-2.

[46] A. Jahid, M. H. Alsharif, and T. J. Hall, "The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research

roadmap," *J. Netw. Comput. Appl.*, vol. 217, p. 103677, Aug. 2023, doi: 10.1016/j.jnca.2023.103677.
[47] N. Etemadi, Y. Borbon-Galvez, F. Strozzi, and T. Etemadi, "Supply Chain Disruption Risk Management with Blockchain: A Dynamic Literature Review," *Information*, vol. 12, no. 2, p. 70, Feb. 2021, doi: 10.3390/info12020070.
[48] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, pp. 2384–2428, 2021, doi: 10.1109/COMST.2021.3108618.
[49] C. Brookson, "GSM security: A description of the reasons for security and the techniques," in Proc. IEE Colloq. Secur. Cryptogr. Appl. Radio Syst., London, U.K., Jun. 1994, pp. 2/1–2/4.
[50] M. Arapinis, L. I. Mancini, E. Ritter, and M. Ryan, "Privacy through pseudonymity in mobile telephony systems," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, Feb. 2014.
[51] H. Karjaluoto, "An investigation of third generation (3G) mobile technologies and services," *Contemp. Manage. Res.*, vol. 2, no. 2, p. 91, 2007.
[52] N. Saxena and N. S. Chaudhari, "Secure-AKA: An efficient AKA protocol for UMTS networks," *Wireless Pers. Commun.*, vol. 78, no. 2, pp. 1345–1373, Sep. 2014, doi: 10.1007/s11277-014-1821-0.
[53] N. Jefferies, "Security in third-generation mobile systems," in *Proc. IEE Colloq. Secur. Netw.*, London, U.K., Feb. 1995.
[54] T. F. La Porta, "Security and IP-based 3G wireless networks," in *Proc. 14th Int. Conf. Comput. Commun. Netw.*, San Diego, CA, USA, Oct. 2005, p. 211, doi: 10.1109/ICCCN.2005.1523879.
[55] T. Zahariadis and D. Kazakos, "(R)evolution toward 4G mobile communication systems," *IEEE Wireless Commun.*, vol. 10, no. 4, pp. 6–7, Aug. 2003, doi: 10.1109/MWC.2003.1224974.
[56] A. N. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," *IEEE Secur. Privacy*, vol. 11, no. 2, pp. 55–62, Mar./Apr. 2013, doi: 10.1109/MSP.2012.136.
[57] Y. Park and T. Park, "A survey of security threats on 4G networks," in *Proc. IEEE Globecom Workshops*, Washington, DC, USA, Nov. 2007, pp. 1–6, doi: 10.1109/GLOCOMW.2007.4437813.
[58] P. Goyal, S. Batra, and A. Singh, "A literature review of security attack in mobile ad-hoc networks," *Int. J. Comput. Appl.*, vol. 9, no. 12, pp. 11–15, Nov. 2010, doi: 10.5120/1439-1947.
[59] S. J. Kim, H. Lee, and M. Lee, "A study of 4G network for security system," *Int. J. Adv. Cult. Technol.*, vol. 3, no. 2, pp. 77–86, Dec. 2015, doi: 10.17703/IJACT.2015.3.2.77.
[60] S. K. Mohapatra, B. R. Swain, and P. Das, "Comprehensive survey of possible security issues on 4G networks," *Int. J. Netw. Secur. Appl.*, vol. 7, no. 2, pp. 61–69, Mar. 2015, doi: 10.5121/ijnsa.2015.7205.
[61] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, vol. 18, pp. 64–84, Mar. 2016, doi: 10.1016/j.phycom.2015.10.006.
[62] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the internet of things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018, doi: 10.1109/ACCESS.2017.2779844.
[63] C.-X. Wang *et al.*, "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 122–130, Feb. 2014, doi: 10.1109/MCOM.2014.6736752.
[64] J. Thompson *et al.*, "5G wireless communication systems: Prospects and challenges," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 62–64, Feb. 2014, doi: 10.1109/MCOM.2014.6736744.
[65] D. Soldani and M. Innocenti, "5G communication systems and connected healthcare," in *Enabling 5G Communication Systems to Support Vertical Industries*. New York, NY, USA: Wiley, 2019, pp. 149–177.
[66] G. Liu and D. Jiang, "5G: Vision and requirements for mobile communication system towards year 2020," *Chin. J. Eng.*, vol. 2016, art. no. 5974586, p. 8, 2016, doi: 10.1155/2016/5974586.
[67] T. Mahmoodi, "5G and software-defined networking (SDN)," in *Proc. 5G Radio Technology Seminar: Exploring Technical Challenges in the Emerging 5G Ecosystem*, London, U.K., Mar. 2015.
[68] 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.
[69] S. A. Hakeem, A. A. Hady, and H. W. Kim, "5G-V2X: Standardization, architecture, use cases, network-slicing, and edge-computing," *Wireless Netw.*, vol. 26, no. 8, pp. 6015–6041, Nov. 2020, doi: 10.1007/s11276-020-02419-8.
[70] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016, doi: 10.1109/ACCESS.2016.2601009.
[71] M. Pawlicki, M. Choras, 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.
[72] ETSI ISG ZSM, "ETSI GS ZSM 002: ZSM reference architecture," ETSI, Sophia Antipolis, France, 2019. [Online]. Available: https://www.etsi.org/deliver/etsigs/ZSM/001099/002/01.01.0160/gsZSM002v010101p.pdf
[73] 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.