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

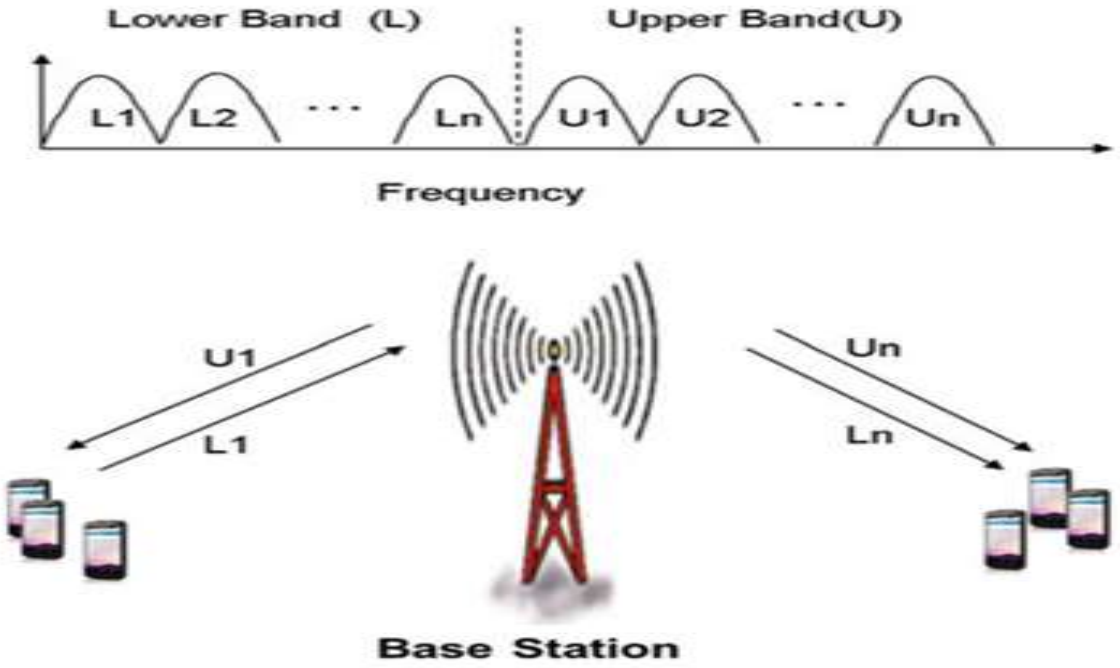

Fig. 2 The 2G cellular TDMA communication system[23]

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.

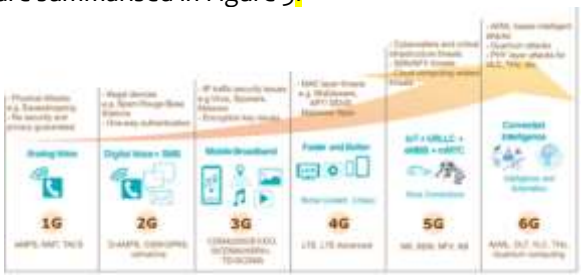

Fig. 3 The security evolution of mobile communications from 1G to the predicted future 6G[44].

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].

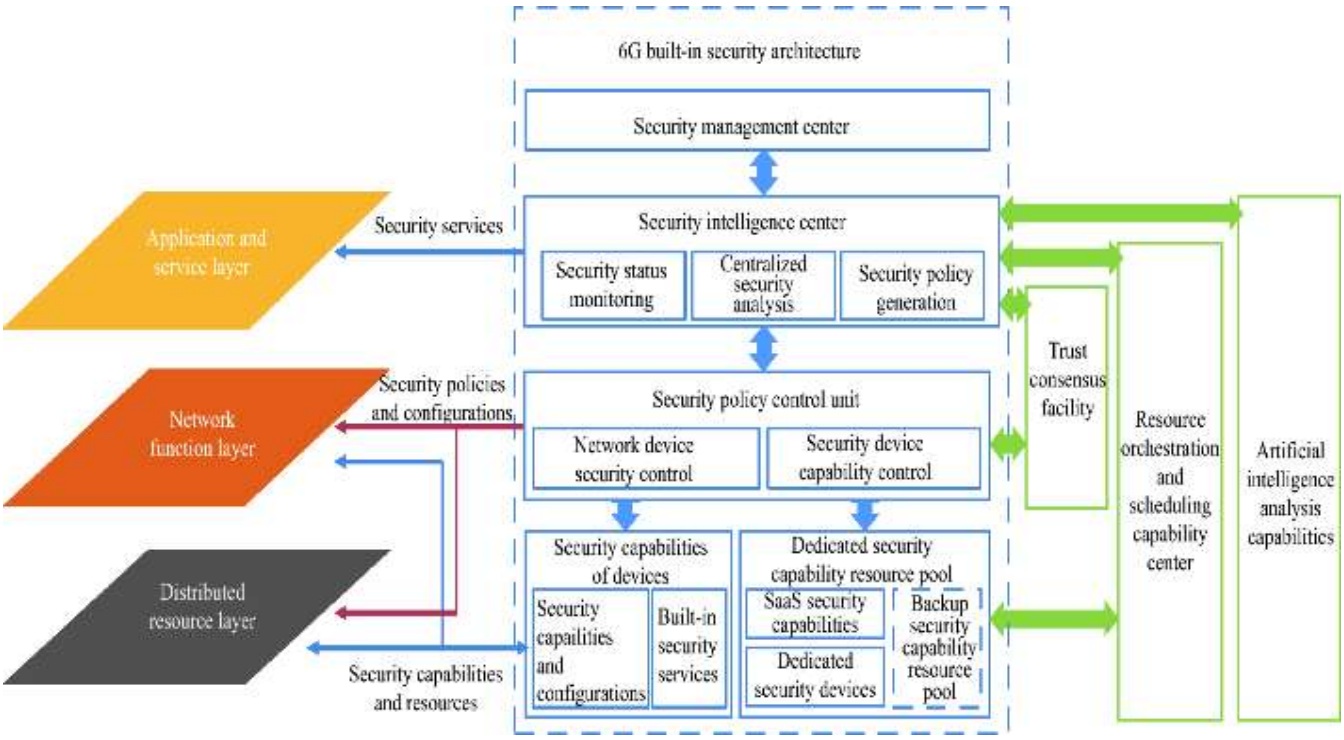

Fig. 4 The security evolution of mobile communications from 1G to the predicted future 6G[57]

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.

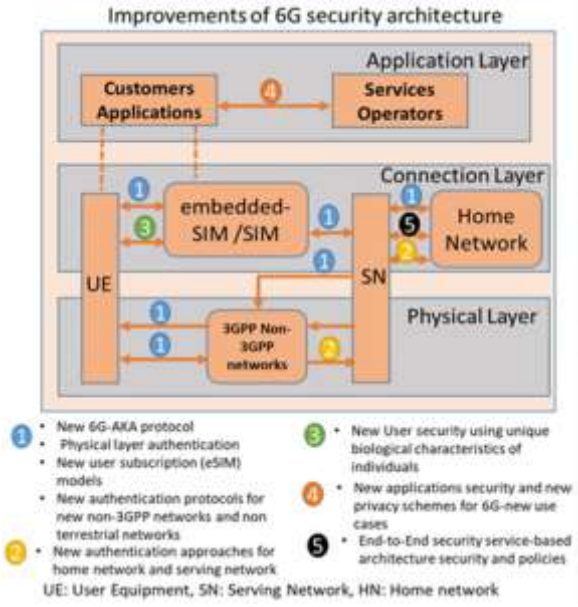

Fig. 5 The new improvements of 6G security architecture[44]

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].

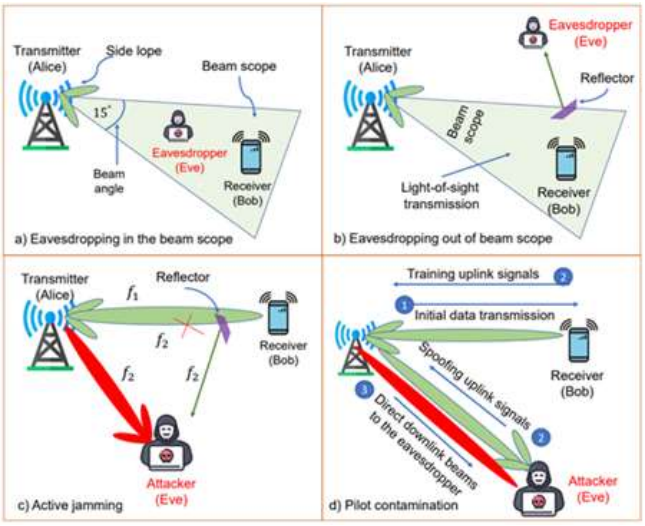

Fig. 6 Illustration of the methods to mitigate eavesdropping/jamming threats for 6G physical layer.

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

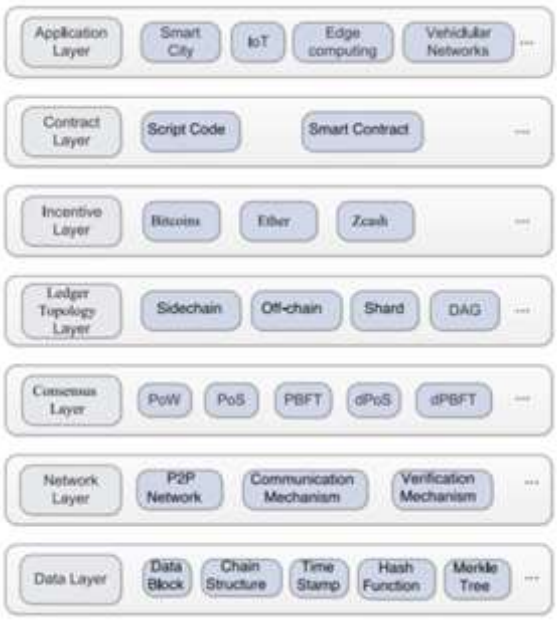

Fig. 7 General Architecture of blockchain

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

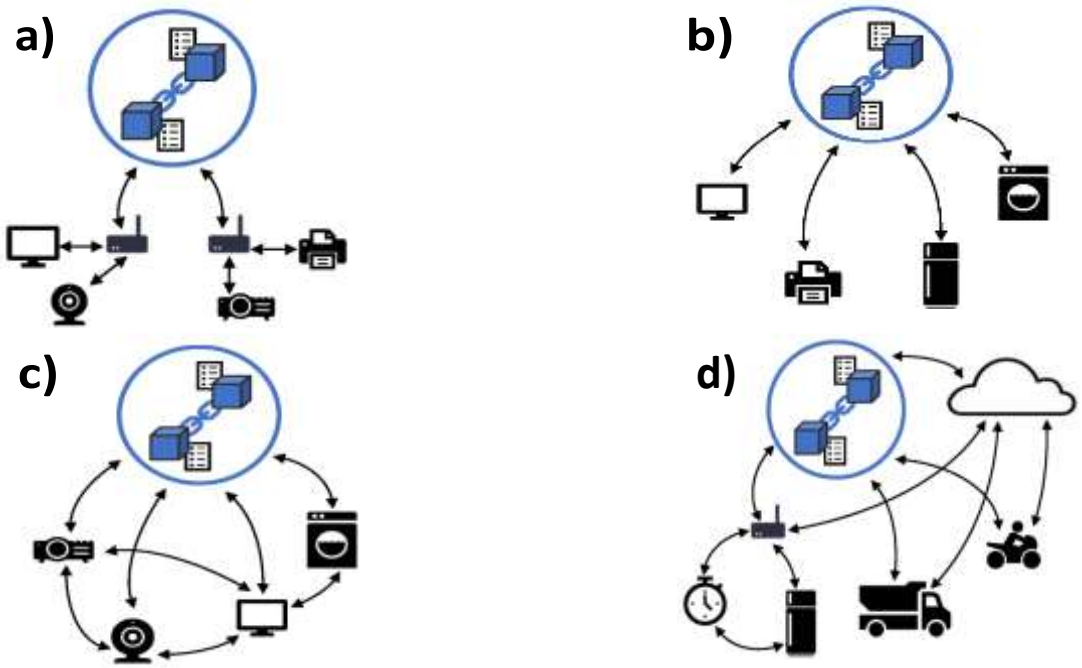

Fig. 8. A Gateway device as end-points to the blockchain, Fig. 8. b IoT edge devices as transaction issuers to the blockchain, Fig. 8.c Interconnected edge devices as end-points to the blockchain and Fig. 8.d A hybrid cloud/blockchain approach.

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.