Role of Blockchain and AI in Security and Privacy of 6G

Hany F. Atlam, Muhammad Ajmal Azad, Manar Altamimi, and Nawfal Fadhel

Abstract In the coming era, 6G is expected to bring a new reality that contains billions of things, humans, connected cars, robots and drones that will produce Zettabytes of digital data. 6G is mainly used to design an inclusive digital and physical environment, which is able to sense it, understand it and programme it. Several countries around the world are competing to own 6G infrastructures and solutions since this new technology provides huge capabilities that will reshape how enterprises operate. Although 6G provides several advantages over existing technologies, security and privacy issues still need to be addressed. This is because 6G provides automatization of most critical processes, which produce a more wide and complex attack surface. Also, with 6G, the network becomes more vulnerable not only to direct security attacks but also to misbehaviour of automated processes that require to be recognized, and their effect should be minimized. This chapter provides a discussion of security and privacy issues in 6G and how the integration of blockchain and Artificial Intelligence (AI) with 6G can provide possible solutions to overcome these issues. The chapter starts by providing an overview of wireless communications technologies from 0 to 6G. This is followed by discussing the main security and privacy issues in 6G networks. Then, the integration of blockchain with 6G will be discussed by highlighting possible solutions to overcome security and privacy issues associated with 6G. The integration of 6G with AI will be also discussed by highlighting

H. F. Atlam (✉) · M. A. Azad
Department of Engineering and Technology, University of Derby, Derby D22 1GB, UK
e-mail: h.atlam@derby.ac.uk

M. A. Azad
e-mail: m.azadh.atlam@derby.ac.uk

H. F. Atlam
Computer Science and Engineering Dept, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt

M. Altamimi · N. Fadhel
School of Electronics and Computer Science, University of Southampton, Southampton, UK
e-mail: m.m.m.altamimi@soton.ac.uk

N. Fadhel
e-mail: Nawfal@soton.ac.uk

M. Dutta Borah et al. (eds.), *AI and Blockchain Technology in 6G Wireless Network*, Blockchain Technologies, https://doi.org/10.1007/978-981-19-2868-0_5

the importance of AI in 6G and how AI with 6G can provide better and effective security and privacy solutions. In the end, healthcare with 6G is presented as a use case by highlighting security issues and discussing the role of AI and blockchain in providing effective security solutions in the healthcare sector.

Keywords 6G · Security · Privacy · Security and privacy · Blockchain · AI · Blockchain with 6G · AI with 6G

1 Introduction

Although the fifth generation or 5G of mobile communication network is not fully implemented, several studies started to talk about 6G (Sixth Generation) and its potentials. 6G is anticipated to enable unprecedented Internet of Everything (IoE) applications with enormously varied and challenging demands. 6G is intended as a space-aerial-terrestrial-ocean interconnected three-dimension network with multiple sorts of parts enabled by new technologies and standards to make the system more intelligent and flexible to meet varied requirements efficiently [1]. Some people argue that 6G networks will be just a faster version of 5G, but the reality is 6G, is a new improved version of 5G in almost all aspects. For instance, unlike the 5G network, coverage will not be confined to the ground level. Instead, it should cover the entire undersea surface area. Artificial Intelligence (AI) capabilities also will be substantially higher on the 6G network [2].

6G provides new attractive characteristics that will integrate capabilities of previous mobile communication technologies such as high reliability, massive connectivity, high throughput and network densification. 6G can be able to provide several benefits to various applications such as autonomous vehicles, sensing, implants, computing reality devices, smart wearables, and 3D mapping [3, 4]. 6G will also improve performance and maximize user Quality of Service (QoS). 6G is predicted to offer 1000 times faster wireless connectivity than 5G. Additionally, 6G is projected to enable ultra-long-range communication with a latency of less than 1 ms [5].

Although 6G provides unlimited advantages for various applications due to the huge capabilities it provides, security and privacy are the major issues that 6G need to address. The integration of AI in 6G can be used to develop safer and secure systems, but it can also be used to create more dangerous attacks. Physical layer security measures can also be used as the first line of defence for safeguarding network portions that haven't been thoroughly explored. Therefore, there is a need for effective solutions to security and privacy challenges in 6G networks.

Adopting one of the Distributed Ledger Technologies (DLTs) such as blockchain is one of the solutions for overcoming security and privacy challenges in 6G. Blockchain is distributed, decentralized, and trustless network by eliminating the centralized authority. This improves transparency by sharing the transaction details between the participants in the network, provides rigorous security to prevent cyber-attacks

such as Denial of Service (DoS) and privacy to protect sensitive information and prevent data manipulation [6]. Blockchain is also capable of storing data across the network immutably and securely. This eliminates the single point of failure and data manipulation [7].

Another technology that can provide an effective solution for security and privacy issues in 6G is AI. The integration of AI with 6G will bring several benefits for overcoming 6G's security and privacy issues. Multi-layered intrusion detection and prevention employing deep reinforcement learning and Deep Neural Networks (DNN) can protect 6G against IP spoofing attacks, flow table overloading attacks, Distributed Denial of Service (DDoS) attacks, control plane saturation attacks, and host location hijacking attacks. Machine learning (ML) techniques like Decision Trees and Random Forest can be also beneficial for detecting DDoS attacks in SDN systems because of their speed and accuracy.

This chapter aims to provide a discussion of security and privacy issues in 6G and how the integration of blockchain and AI with 6G can provide effective solutions to overcome these issues. The chapter starts by providing an overview of wireless communications technologies from 0 to 6G. This is followed by discussing the main security and privacy issues in 6G networks. Then, the integration of blockchain with 6G will be discussed by highlighting possible solutions to overcome security and privacy issues associated with 6G. The integration of 6G with AI will also be discussed by highlighting the importance of AI in 6G and how AI with 6G can provide better and effective security and privacy solutions. In the end, healthcare with 6G is presented as a use case by highlighting security issues and discussing the role of AI and blockchain in providing effective security solutions in the healthcare sector.

The remainder of this chapter is organized as follows: Sect. 2 presents an overview of mobile communication generations from 0 to 6G; Sect. 3 discusses security and privacy issues of 6G; Sect. 4 presents the integration of blockchain with 6G; Sect. 5 discusses the integration of AI with 6G; Sect. 6 presents use case of healthcare with 6G, and Sect. 7 is the Conclusion.

2 From 0G to 6G: An Overview

The evolution of mobile communication technologies passed through different phases. This section provides an overview of these different phases by highlighting the main advantages and drawbacks introduced by each generation. The discussion started from 0G or pre-cellular mobile telephony in 1970 to 6G that expected to be implemented in 2030.

0G or Zero Generation refers to the pre-cellular mobile telephony technology used in the 1970s such as Radio telephones and the telephone in cars, which was introduced before the invention of cell phones. 0G utilized technologies including IMTS (Improved Mobile Telephone Service), OLT (Norwegian for Offentlig Landmobil Telefoni), PTT (Push to Talk), AMTS (Advanced Mobile Telephone System), and MTS (Mobile Telephone System) [8]. Early example that utilized 0G technology was

Autoradiopuhelin (ARP), which was introduced by Finland in 1971 and become the first public commercial mobile phone network. Also, Germany introduced B-NetZ in 1972 as a public commercial mobile phone network [9].

1G or First-Generation technology for cellular networks was presented in the 1980s. Nippon Telephone & Telegraph (NTT) in Tokyo, Japan, introduced the world's first cellular system in 1979. Also, Nordic Mobile Telephone (NMT) and (TACS) in 1980 started to introduce their cellular systems across Europe [8]. 1G was mainly designed for voice services in which it uses analogue signals to transmit information [10]. 1G was the first step in the road to provide public and commercial mobile telephony. Although all 1G systems provided handover and roaming capability, the interoperability between countries was the major issue that faced 1G. This allows users to make voice calls only in one country. Also, 1G suffered from the lack of security and privacy as voice calls were transmitted back to the radio towers, which make these calls susceptible to various attacks. Also, since voice calls are not encrypted, the data transmission and calls can neither be secure, nor private. 1G also suffered from poor voice links and low capacity and unreliable handoff [11].

2G or Second-Generation technology was introduced in the early 1990s. The first 2G system was introduced by Finland in 1991. 2G is mainly based on digital modulation techniques, which enable both voice and short message services [12]. GSM (Global System for Mobile Communications) is the most well-known and commonly utilized 2G mobile communication system [13]. GSM overcomes the limitation of 1G by allowing international roaming between phone providers, which enable users to utilize their phones in different places around the globe. Compared to 1G, 2G provides better security and privacy since the encryption is applied on all text messages, which provide better security and allow only interned receiver to obtain messages and read it. Although 2G provides better security over 1G, it still has some issues such as crypto flaws, eavesdropping attack, SIM attack, fake base station (BS), absence of replay protection and DOS attack.

3G or Third-Generation technology of mobile communication was first introduced in 2000. It was the first wireless communication technology that enables data transfer of 2 Mbps [14]. 3G provides several advantages over 2G technology in which it provides faster communications that enable sending and receiving a large amount of data and enable high-speed video conferencing and 3D games. Also, with increased bandwidth and broadband capabilities with 3G, this allows web-based applications and audio and video streaming to work efficiently. On the other hand, 3G presents some challenges or drawbacks. One of the major issues is energy efficiency in which 3G consumes significantly more power than 2G, so 3G needs different devices and drivers. This makes building an infrastructure for 3G more challenging. Also, 3G needs high bandwidth requirements and costly fees for 3G licenses and agreements [15]. UMTS (universal mobile telecommunications service) or what was called W-CDMA is the primacy technology in 3G. It represents the recessive that is compatible with prior generations of wireless technologies through its heterogeneity with the legacy GSM and AMPS technologies. The evolution of UMTS into high-speed packet access (HSPA) and advanced HSPA (HSPA +) allowed for greater end-to-end

network efficiency and eventually led to the advancement of the next generation of networks [16].

4G or Fourth-Generation technology of mobile communication was first introduced in Stockholm in 2009. 4G represents the communication standard that delivers demands for broadband data transmission and broadcasting. 4G was the main driver for the Internet of Things (IoT) that enables users and physical objects to connect anytime, anywhere using any network path. 4G is the successor of 3G that is produced to overcome limitations associated with 3G and enable broader bandwidth, better security and privacy and high-speed internet access. According to the ITU union, 4G provides a data rate of 100 Mbps [17]. 4G is mainly based on the invention of LTE (Long-Term Evolution), which provides an IP-based invention for data transmission. LTE provides seamless mobility, QoS, and low latency for packet-switched traffic. 4G provides high-speed data rates up to 1Gbps, which provide high quality for audio and video streaming applications and online games. 4G also provides better security and privacy. On the other hand, 4G introduces some issues in which 4G consumes more power and need complicated and expensive hardware for implementation [8].

5G or Fifth-Generation technology of mobile communication was first introduced in the late 2010s. The demands for considerably faster data rates for users, and the exponentially growing IoT applications and services have meant the telecom industry has had to evolve around these pressures. 5G can satisfy the demands of the public and companies by creating a truly mobile and wired connected community. This will only be achieved by improving the radio access interface, which requires a new larger range of frequency, expanded bandwidth for the increasing user base, and support for the ever-expanding IoT [18]. There are various advantages to 5G. It transports a world with much improved mobile data broadband, ultra-responsiveness, ultra-reliability, ultra-low latency, ultra-fast data rates, and huge IoT capabilities. 5G can support around one million per square kilometre while 4G can only support about 4,000 devices. This can enable more video and audio streaming without disruption. Massive MIMO (Multiple Input Multiple Output) is a new digital technique used in 5G that uses multiple targeted beams to highlight and follow users throughout a cell site. Coverage, speed, and capacity are all improved as a result [19]. 5G is extremely compatible with WWWW (Wireless World Wide Web), which will create several applications using the high capabilities it provides.

6G or Sixth-Generation technology of mobile communication attracted the attention of several researchers, although 5G coverage is not yet being provided completely. The research has been started in 2019 to develop the 6G wireless technology. 6G provides new attractive characteristics that will integrate capabilities of previous mobile communication technologies such as high reliability, massive connectivity, high throughput and network densification. 6G with new capabilities will be able to provide several benefits to various applications such as AI, smart wearables, implants, autonomous vehicles, computing reality devices, sensing, and 3D mapping [3, 4]. 6G will improve performance and maximize user QoS. 6G is predicted to offer 1000 times faster wireless connectivity than 5G. Additionally, 6G is projected to enable ultra-long-range communication with a latency of less than

1 ms [5]. The average experienced downlink (DL) data rates for 6G are expected to be 100 Gbps and the number of devices per km^2 will be 10^9.

The development of mobile communication technologies passed through various stages with each generation provided added capabilities, as shown in Fig. 1. The evolution started with supporting only voice calls with 1G and over the time the next generation focused on increasing bandwidth and speed of data transmission that allowed the appearance of novel web and internet applications. The developments continued to generate 5G that is the main driver for massive broadband and various IoT applications and services. The expectation talks about 6G and how it can change how businesses work by allowing automation and AI and creating a connected world.

Table 1 provides a summary of the advantages and disadvantages of each mobile communication technology that was previously introduced. Besides, a comparison of various features of 4G, 5G and 6G is presented in Table 2.

3 Security and Privacy Issues in 6G

Although 6G provide countless benefits by providing ubiquitous access and connectivity to various applications, security and privacy are still major issues that need to be addressed to provide more trust for the customers. This section discusses some of the security and privacy threats that are presented by 6G.

3.1 Security Issues in 6G

The old generation of mobile communication technologies (i.e., 1G, 2G, 3G) did not consider the security and privacy of users in their priorities. This makes these technologies suffer from severe security and privacy issues including cloning, eavesdropping, authentication and authorization issues. Because of the execution of wireless applications, 4G began to consider security, although it faced numerous security and privacy issues [20]. Then, 5G and 6G did the same but with security threats that need to be handled to take all the benefits of 6G wireless networks. Looking at the security in 6G should be combined with AI as 5G and 6G have almost fully integrated with AI, which led to what is called security automation. At the same time, adversaries with the power of AI have become more powerful and intelligent that makes detecting their attacks not an easy task.

Flash network traffic is one of the common vulnerabilities in both 5G and 6G networks. With the growing amount of IoT devices, the network capacity has to reach a demand fast. Wireless local area networks or even Femtocells, for example, are preferred when trying to increase the capacity of a network; However, transmitted information intended for the certified user equipment is more vulnerable to eavesdroppers and unauthorized users. This is because of broadcasting features of

Table 1 Summary of advantages of different mobile communication technologies from 1 to 6G

Technology	Advantages	Disadvantages
1G	The first technology to provide public and commercial mobile telephony Allows voice calls Use analogue signal	Unable to interoperate between countries Low spectral efficiency Major security and privacy issues Limited capacity Large phone size Poor handoff reliability
2G	Use digital signals Allows services including text messaging, image messages, and MMS Provides better quality and capacity Better response time. 10 times better than 3G	Unable to support internet and e-mail services Limited data rates Security and privacy issues Unable to handle complex data such as videos Require strong digital signals
3G	Provide high-speed network communication for data transmission Faster than previous networks Provide very good voice call and huge MMS	Failure of WAP for internet access Consumes more power Require installing new 3G equipment Require different handsets Require closer base stations
4G	Very high voice quality High bandwidth 10 times faster than 3G Support interactive multimedia and other broadband services Easily access the Internet and other services	Require new complicated and expensive hardware as it uses new frequencies Consumes more power High cost for users Previous components are not compatible with 4G
5G	Low latency capabilities Increased speed and bandwidth Increased connectivity and access to various online services Provides energy efficiency plans Improved WAN connection Data bandwidth of > 1 Gbps Dynamic information access	Limited coverage as it is not yet implemented fully Security and privacy issues Higher expensive and complicated hardware equipment Not compatible with previous technologies, so need new equipment
6G	Provide ultra-broadband internet services Very low latency capabilities Support higher number of users per km^2 Higher downlink data rate that is expected to be 100Gbps Uses visible lights which leverage the benefits of LEDs Uses THz (Terahertz) frequencies, which has several benefits Support home automation and other IoT applications	Need expensive and complicated hardware equipment Security and privacy issues Since it uses THz frequencies, it will face issues of THz, which is more dangerous for the environment Lack of information control Since it uses light, it will face issues of VLC Require new expensive equipment

Table 2 Comparison of 4G, 5G and 6G

Feature	4G	5G	6G
Development period	2009	2018	2030
End-to-end (E2E) latency	100 ms	10 ms	1 ms
Mobility support	Up to 350 km/hr	Up to 500 km/hr	Up to 1000 km/hr
Satellite integration	No	No	Fully
Per device peak data rate	1 Gbps	10 Gbps	1 Tbps
XR	No	Partial	Fully
THz Communication	No	Limited	Widely
Haptic Communication	No	Partial	Fully
Maximum spectral efficiency	15 bps/Hz	30 bps/Hz	100 bps/Hz
Architecture	MIMO	Massive MIMO	Intelligent surface
Maximum frequency	6 GHz	90 GHz	10 THz
AI	No	Partial	Fully
Autonomous vehicle	No	Partial	Fully
Service level	Video	VR, AR	Tactile
Applications	High-speed applications, mobile TV, wearables	High-resolution video streaming, remote control of cars, robots and medical procedures	AI, smart wearables, implants, autonomous vehicles, computing reality devices, sensing, and 3D mapping

wireless communications and open system architecture. The traffic from servers to machines must be protected to prevent traffic sniffing attacks [21].

DoS and DDoS are other common security threats in 6G. It is one of the most obvious attacks that occur to any device connected to the network and can damage the system as a whole. The use of various radio access network technologies is another security threat. Different radio access network technologies are starting to be integrated with 6G, these include mmWave, Wi-Fi, NB-IoT and Li-Fi. There are potential risks with the integration of these technologies and could pose a risk to the 5G network when systems are not tested or trailed to see whether or not they have any unknown/known vulnerabilities [22].

Integrity-based attack is one of the common attacks in 6G networks. This type of attack is implemented using a fake eNodeB, when consumer equipment is convinced to connect to the network, this is known as a malicious relay. This malicious relay is using the network as a Man-in-the-Middle attack. Because there is no integrity defence on this channel the attacker can take advantage of this, the intruder, who has

Table 3 Summary of some of security attacks/threats in 6G

Security threat in 6G	Description
Flash network traffic	Transmitted information needed for the intended user is vulnerable to eavesdroppers and unauthorized users. This is because of broadcasting features of wireless communications and open system architecture
Poisonous attack in AI	This attack is performed by tampering with malicious samples in the training data, which affect the learning outcomes of the AI system, which result in misclassification or incorrect regression outcomes
DoS and DDoS	DoS and DDoS attacks are carried out by continuously injecting fake heavy load in virtual network functions (VNFs)
Evasion attack in AI	This attack is similar to the poisonous attack but with tampering with the testing data instead to affect the result of the AI model
AI/ML frameworks	Most AI models use existing or traditional AI/Machine Learning (ML) frameworks that have several vulnerabilities that can be used as a way to hack or attack the integrity of data
51% attack	Controlling the public blockchain with at least 51% of its mining power allows the attacker to gain control over the blockchain and manipulate its blocks and transactions
Quantum collision	In a quantum environment, a quantum collision occurs when two entirely independent inputs of a hash function produce the same result/output
Access control	Access control policies are broken, data or user credentials are stolen, and unauthorized resources or system parameters are accessed or modified by adversaries
Eavesdropping	Although transmissions in narrow beams with strong directionality are resistant to interception attacks, rogue nodes can still intercept the signal

access to the intended user's encrypted communications, manipulates or changes the transmitted information such that the attacker fabricates the message that enters the intended receiver [23]. Other security attacks in 6G are summarized in Table 3.

3.2 Privacy Issues in 6G

6G is expected to provide ubiquitous access to various devices, objects, sensors, and autonomous applications. This will enable various devices in different IoT applications to share a huge quantity of data between various applications. However, this type of data can be personal data including financial data, habits, etc. [24]. For instance, although a smart light, which turns on and off as you move, provides an effective way of utilizing the energy, it can be used to identify the pattern of life in your house to identify which room you use and when and if there are other people in the house. Although the energy service provider can utilize your data to provide more efficient lighting service, for example, and create more customized and individually

Table 4 How blockchain can address the challenges of 6G

6G Issues	How blockchain can address the challenge
Availability and transparency	The data in the blockchain network do not rely on centralized authority. Instead, the blockchain stores and distributes data across the network, where all the information are accessible across the blockchain network [42]. Additionally, smart contracts in the blockchain can provide reliable data exchange between the users [36]
Data integrity	The data in the blockchain have a unique encrypted hash to guarantee its integrity [43]
Access control	Smart contracts are capable of providing direct access between requestors and data centres with no need for a central authority [36]
Authentication	The blockchain-based public-key infrastructure is capable to identify entities in the network [7]
Privacy	The blockchain is capable of providing better and effective privacy in many forms. Firstly, the data are stored in a time-stamped and immutable mode to prevent data modification. In terms of data exchange across the network, smart contracts can protect data from malicious users by providing user authenticity [44]. Also, blockchain could enforce user data privacy policies using smart contracts by tracking and log the transaction across the network [42]
Scalability	The blockchain improves scalability through its ability to share the services between edge nodes across the network, interoperability across devices, and the link between IoT devices with no need for trusted intermediaries [38]
Security	The blockchain is a decentralized and distributed ledger in which transactions are added to the network and confirmed by a majority of the nodes participating in the network. SHA-256 hash was then used to link the new block to the preceding one. As a result, the blockchain provides a secure and immutable environment [36]

personalized services based on personal preference, privacy is still the nightmare to customers and how service providers can leak their data and identifying the amount and type of information to be collected by these devices or services [25].

With the increase of adoption of AI-enabled smart applications that need situational and context-aware services, the traditional privacy-preserving techniques will not provide the required functionality due to various privacy issues encountered with 6G. Therefore, there is a need to adopt new technologies that provide better security and privacy. One of these technologies is Distributed Ledger Technology (DLT) such as blockchain, which provides more effective security solutions and provides privacy-preserving data sharing using DLT security features such as integrity, immutability, accountability and traceability [26, 27]. Other privacy-preserving techniques like Privacy protection using differential privacy (DP) also can provide an effective privacy-preserving solution for 6G wireless applications. Before sending the final

output to the specified server, DP disturbs the actual data using fake design random noise functions. This eliminates the need for statistical analysis of the data collected and the inference of any personal information [28]. These approaches can be a solution to the privacy nightmare in 6G, but this does not change the fact that there is a need for new privacy-preserving technologies that can provide effective privacy solutions with the ubiquitous access and connectivity provided by 6G.

4 Blockchain for 6G

Adopting one of the technologies of DLT such as blockchain can provide better security and privacy for 6G. Blockchain provides effective security solutions utilizing immutability, tamper-proof, integrity, and accountability features. This section presents the integration of blockchain with 6G. It begins by outlining blockchain and its characteristics, benefits/advantages, integration with 6G and how this integration can utilize various features of blockchain in 6G.

4.1 Overview of Blockchain

Blockchain technology is relatively a recent technology that has been grasped by several scholars to explore more after success in the financial sector, cryptocurrency. In 2009, an anonymous person namely Satoshi Nakamoto published a white paper that solved a double-spending problem in an electronic cash transaction. It allows individuals to receive or send online payments without financial intuition using blockchain technology [29].

Blockchain is defined as distributed and decentralized ledger in which each node in the network contributes to managing transactions. The transactions are encrypted and stored in a block. Each block is time-stamped and encompasses a hash function of the preceding blocks to link the blocks together. The time-stamp and hash functions are used to protect the integrity and immutability of the transactions that are distributed across the network. To keep the network secure, the majority of the nodes in the network should agree to add a block to the chain through a mechanism called a consensus algorithm. The consensus verifies and authenticates the transactions without a central authority [30].

4.2 Benefits of Blockchain

The structure of building a blockchain network gives its own benefits that would not be found in other technologies. Although blockchain is one of the common

DLT technologies, it has its key benefits. This section provides the key benefits of blockchain including:

- **Persistency**: After validating and adding a block into the chain by the agreement of the majority of participant nodes in the blockchain network, data could not be modified or deleted because each block contains a timestamp of creating the block and hash function of all blocks in the chain. This maintains the integrity of the data [31].
- **Auditability**: The auditability in blockchain comes from the fact that each block stores the hash value of the previous block, which allows the current block to be connected with the previous block. This allows the data to be verified and tracked back [31].
- **Availability**: Because the data are shared among all nodes in the blockchain network, it can be accessed from other nodes even if one node is down.
- **Decentralized Management**: The automation of management comes from using a consensus protocol where each node in the network must follow the protocol to run the network. The consensus is an agreement between the nodes to validate the transaction and adding the block to the chain [32].
- **Transparency:** Because all data are shared throughout the network nodes, every participant node has access to it, blockchain provides a high level of transparency [33].
- **Privacy**: Privacy could be a great challenge in the blockchain because of the transparency factor [32]. However, with Public Key Infrastructure (PKI) and adding smart contracts in the blockchain network, privacy could be enhanced. PKI provides each user with their unique public key to represent their identity whereas, smart contracts could be used to add access to the data, enforce privacy policy, and add automation network tracking.
- **Security**: Blockchain provides a high level of security in two forms: PKI and cryptographic. Every user in the network has its own unique public key to represent the identity that protects them from malicious attacks. The cryptographic is used to encrypt data using SHA-256 that protects the data from being deleted or modified [32].

4.3 Integration of Blockchain with 6G

Despite the recent development of the 5G mobile network, academia and industry have commenced envisions in the next generation; the 6G mobile network by reviewing the development of the 5G [34], and highlighting the requirements in the 6G [22]. The requirements of 6G will enhance in terms of data rate, high system capacity, efficient high spectrum, lower data delay, and expected wider and deeper coverage. These requirements are a response to the emergence of new technologies, such as the Internet of Vehicles and the Internet of Everything that require high convergence of a massive number of sensors and devices, which are far beyond the capability of 5G [35].

The envisioned 6G mobile network would enable system services beyond 5G. However, the limitation in the technology adopted in 5G could not enable to reach expectation on 6G because of the extraordinary explosive growth in mobile traffic [36]. The growth has led to perceptible challenges in developing the next-generation mobile network. These challenges are not only related to the massive connectivity but are related to security and privacy [36]. The unprecedented in increasing mobile users, machine-to-machine and device-to-device connections, and the number of transactions, scalability, minimize latency, higher throughput of the network are main challenges in the future generation network [37]. These challenges rise series of security and privacy against cyber-attacks, protecting the massive data transmission between devices, and preventing unauthorized manipulation [38]. Therefore, integration with enabler technologies is essential to address the challenges.

5G provides network services through several underlying technologies, such as cloud computing. Although cloud computing paved the 5G to its objectives such as unlimited storage and communication power, the centralized architecture remains an obstacle to response to the massive amount of data and IoT devices [34, 36]. The challenges in centralized cloud computing remain unsolved in terms of security and privacy. Single point of failure and cyber activities lead to failure in security services such as data availability, privacy, and data integrity. Additionally, cloud services are provided through cloud service providers and users' data are stored in the cloud. These raise an issue in privacy services such as the method used to access the data, and the personal information of the users [36].

The integration with other enabler technologies such as decentralized architecture such as blockchain will bring the prospect to tackle the challenges. Blockchain is distributed, decentralized, and trustless network that operates without a centralized authority. This could improve transparency by sharing the transaction details between the participants in the network, provides rigorous security to prevent cyber-attacks such as DoS and privacy to protect sensitive information and prevent data manipulation [6].

Many studies have shown that blockchain could address the limitations associated with 6G [37–40]. Blockchain is capable of storing data across the network immutably and securely. This eliminates the single point of failure and data manipulation by malicious attacks, which ensures data availability and data integrity [7]. Additionally, blockchain is used to enhance the accessibility and authentication of data using smart contracts [27, 41]. Smart contracts can add restrictions to access data through decentralized rules.

Maintaining data transparency is a critical issue regarding data modification, user personal information, and access control, however, blockchain technology has the capability of maintaining data transparency while considering the security and privacy of data. This is due to many reasons. Firstly, every transaction on the blockchain network is approved through a consensus mechanism and agreed upon by the majority of the nodes in the network. These transactions are stored in a block and add blocks to the previous ones using SHA-256 encryption. Additionally, every user in the network has their public key to represent their identity and keep their personal

information anonymity. Lastly, smart contracts are capable of providing restrictions to whom to access the data and can enforce privacy policies to access the data [36].

Moreover, integration of 6G with blockchain would enhance the network performance and increase scalability with low-latency services. The scalability improvement would be enhanced through the integration of the blockchain with mobile edge computing. Instead of centralized computing, a distributed structure would enable to share of reliable resources between edge nodes. Accordingly, the interoperability across devices could be improved because of the structure of the blockchain [38].

4.4 Blockchain for Better Security in 6G

Security issues are critical when it comes to mobile communication networks. It could be range from DoS, single point of failure, data tampering, and data leakage. Many studies illustrated that security issues still existed in the deployment of 5G [22, 36]. However, 6G is expected to work with trillions of devices and millions of mobile users. Investigation of these security issues and tackle them before developing the 6G is vital.

DoS attack is one of the challenging threats in 6G. Although many solutions have been proposed to mitigating the issue such as using AI techniques to detect the DoS, this issue is going to be crucial challenging in the 6G due to the massive connectivity. This threat could result in low latency to mobile uses, affect the scalability, and availability of the network [45].

The single point of failure threat is a result of the dependency on centralized systems. Even though the centralized systems in the computing model, edge computers, and others provide services that could not be available in previous networks such as on-demand and minimized the management efforts [36], the expansion of mobile uses and IoT devices would not be met. This threat could affect the performance and the security services in the network [39].

Data tampering threat concerns are about modifying the data by malicious attacks across the mobile network. Because the network services are remote communication between many actors, IoT devices, and intermediate provider services, providing data integrity is important. Although many cryptographic tools are used to protect the data integrity such as keyless signature infrastructure (KSI) or using a third party to validate data, these techniques would not be efficient with the massive increase in connectivity [7]. Data leakage threat is highly vulnerable in data sharing in the networks because of the cyber-attacks. This could lead to losing valuable customer personal information in the mobile networks, or location information of cars in vehicular networks. Data leakage is high-risk in centralized systems where data are stored in a single location. This model put the entire database at risk [46].

Blockchain is one of the promising technologies to tackle security threats. Blockchain features such as data sharing, the protocol to preserve the data, and access control are innovative features to enhance security. Firstly, instead of relying on a single point, blockchain is decentralized distributed ledgers across a network

of nodes. This structure provides robustness and availability of data stored in the blockchain network. Additionally, the data in the network are immutable, which could not be changed or modified since each block is hashed with time-stamped and linked to the previous ones in such a way that could not modify the content of the blocks. Furthermore, the users in the network are using PKI to recognize their identities. Lastly, the network is not controlled by a single entity. Instead, the network is autonomous management using a consensus mechanism that provides a guarantee for agreement between participant nodes [47].

The integration of 6G with blockchain would help to tackle the limitations in network security. The decentralized and distributed structure would help to overcome the single point of failure and DoS. The immutability of data increases the integrity of the data and prevents it from being changed by malicious attacks [7].

5 AI for 6G

Because AI can learn to achieve self-configuration, self-optimization, self-organization, and self-healing, and therefore improve feasibility, intelligence is a vital element of 6G networks. This section discusses the integration of AI with 6G and how this integration can overcome security and privacy issues associated with 6G.

5.1 An Overview of AI

AI is an emerging and rapidly developing technology. Its applications are becoming more prevalent with every passing day. AI is an exciting emerging technology with many possible applications that could revolutionize society. It is predicted that the number of AI digital voice assistants will surpass Earth's human population by 2024 and hit 8.4 billion units [48]. AI can play games, aid healthcare, drive cars, assist law enforcement, and possibly control autonomous weapons. Considering its potentially powerful applications, AI, therefore, must be developed to ensure it is safely implemented. Some experts argue that confidentiality, integrity, and availability (CIA) are key security requirements for AI [49]. Ensuring the integrity of AI output is a clear issue and of huge importance, because AI can interfere with digital media [50].

AI is defined as "*computers that are able to perform tasks typically carried out by humans*" [50]. Due to the exponential growth of computing performance outlined by Moore's Law, some predict that computers with human general intelligence could exist within the next twenty years [51]. The concept of AI has been known for at least 80 years. The 1950 paper by Alan Turing, considered the possibility of real thinking machines. Turing devised a test for assessing a machine's ability to think. A benchmark was proposed that if a computer can fool an interrogator at least 30% of the time, then the test is passed.

A significant subset and evolution of AI is ML. Key developments were made in the 1950s–1970s [51]. ML can be described as a process of complicated computation involving intelligent decision-making and automated pattern recognition based on training sample data. It is considered a supervisory method because it requires initial data to be supplied by human users. ML plays a role in cybersecurity, for example, the use of Artificial Neural Networks (ANNs) in misuse/signature detection systems [52].

5.2 Integration of AI with 6G for Effective Security

Implementing 6G networks needs AI to empower autonomous networks. Hence, security attacks on AI systems particularly ML techniques will impact 6G. This includes poisoning attacks, logic corruption data injection, model inversion, model evasion, and membership inference attacks [53]. However, the integration of AI with 6G will provide several advantages to overcome security and privacy challenges in 6G. For example, IP spoofing, flow table overloading, DDoS, control plane saturation, and host location hijacking attacks can all be prevented by multi-layered intrusion detection and prevention employing deep reinforcement learning and Deep Neural Networks (DNN) [54]. Furthermore, because of their speed and precision, DDoS attacks in SDN systems can be detected using machine learning techniques such as Decision Trees (DT) and Random Forest (RF). ML-based adaptive security techniques are also effective against SDN/NFV threats, as 6G networks presume dynamic deployment of virtual services on-demand [55].

In contrast to current centralized cloud-based AI systems, 6G will rely heavily on edge intelligence. In the vast device and data regime, the distributed nature facilitates the implementation of edge-based federated learning to ensure communication efficiency [56]. 6G network architecture envisions connected intelligence and AI at multiple levels of the network structure. AI has the potential to prevent DoS attacks on cloud servers at the cellular level [57]. Also, in a mesh network, a device's multi-connectivity allows numerous base stations to utilize AI classification algorithms to analyse the device's behaviour and use weighted average ways to collectively decide on its authenticity [58].

Furthermore, utilizing AI-powered predictive analytics, attacks on the blockchain, such as 51% attacks, can be predicted before they happen. A quantum computer might jeopardize asymmetric key cryptography. They can, however, provide exponential speedups for AI/ML techniques, know how to complete previously impossible jobs much faster. As a consequence, quantum machine learning for network security can be a valid strategy against quantum computer-based attacks [59].

Also, in Visible Light Communication (VLC) systems, intelligent beamforming approaches based on RL give the best beamforming plan to protect from eavesdropper threats. Also, a possible option for detecting jamming attacks is anomaly-based detection systems using AI. Node compromise attacks can also be prevented with AI-based authentication and authorization systems [60].

AI also can provide better solutions for privacy issues in 6G. For instance, edge-based ML approaches can be utilized to detect privacy-preserving routes dynamically and transmit data over the highest rank privacy-preserving routes. Also, federated learning, as compared to cloud-based centralized learning, maintains data close to the user, enhancing data privacy and location privacy. Furthermore, due to the vast variety of applications in 6G and the massive data collection required to feed intelligent models, customers will demand varying levels of privacy on different applications. AI-based service-oriented privacy-preserving policy changes could enable fully automated 6G networks with retained privacy [61].

6 Use Case: Healthcare with 6G

Healthcare is one of the major applications that 6G can provide numerous advantages. 6G communication technology is projected to dramatically transform healthcare, with healthcare being wholly reliant on communication technology [62]. Telesurgery will be performed more efficiently thanks to high-speed communication provided by 6G. Also, 6G will provide numerous benefits in health monitoring with smart wearable devices [63]. 6G will also play a vital role in the development of the Intelligent Internet of Medical Things (IIoMT), which are mainly AI-driven intelligent machines that make their own decisions using communication technologies. 6G can also be utilized in the development of precision medicine, which can allow more precise and customized healthcare [64].

6.1 Security Issues in Healthcare with 6G

Although 6G provide numerous benefits in the healthcare domain, security is still one of the major issues that need to be addressed. Some security threats in healthcare include:

- **Data Integrity**: Protecting the integrity of patients' data is the priority for any healthcare provider. However, due to the high accessibility and connectivity provided by 6G, maintaining data integrity will be one of the main challenges in the healthcare system.
- **Phishing**: It is a popular method of stealing personal information, particularly employee information from healthcare firms. The phishing approach is a social engineering technique that manipulates people into sharing personal information. For example, a hacker may create a website that imitates an official website to obtain access to employee information and thus patient information [65].
- **DoS and DDoS**: These attacks are used to block authorized users from accessing the healthcare system by overloading the healthcare system with a flood of fake

traffic that shut down all healthcare services. DoS and DDoS will be serious attacks that target healthcare systems with 6G.

- **Social Engineering**: Humans are always the weakest point in the security chain. By using various social engineering attacks, hackers can deceive employees including doctors, nurses, etc. to steal sensitive information thanks to their lack of security awareness.
- **Eavesdropping**: With the use of 6G in healthcare, eavesdropping will be one of the security issues that result from signal interception due to the nature of wireless communication.
- **AI-based Attacks**: Although 6G utilize AI to provide several automation services in the healthcare sector, this can create several security vulnerabilities that can be used as a way to hack or attack the integrity of data.
- **Blockchain and AI for Effective Security in Healthcare with 6G**

Integrating blockchain with 6G in the healthcare system can provide effective security solutions to overcome most security challenges in the healthcare sector. Blockchain can overcome security issues associated with data integrity by gathering patient data and storing them in an internal catalogue. Then, smart contracts can be utilized to access patient data controlled by patients and their suitable policies. As a result, a patient can share his or her medical information on his or her own terms [66]. Patients can also have access control thanks to blockchain cryptographic keys. Each patient has a "master" key that allows them to "unlock" their health data and share a copy with healthcare providers as needed. Patients can limit their actions to reading or writing information, and they can revoke keys if the device on which the key is stored becomes hacked [67].

Also, blockchain stores data in a time-stamped and immutable mode to prevent data modification. Furthermore, with the help of AI with 6G, DoS and DDoS attacks can be detected and provide availability and accessibility of healthcare services 24/7 for authorized users. As blockchain is a distributed and decentralized ledger, a single point of failure associated with centralized systems will not exist and data can be accessed from any node in the blockchain network. The combination of 6G with AI can also provide an effective security solution to social engineering and phishing attacks by utilizing multi-layered intrusion detection and prevention techniques [68].

7 Conclusion

Although 6G provides unlimited advantages for various applications due to the huge capabilities it provides, security and privacy are the major issues that 6G need to address. Blockchain technology can play an important role to resolve some of these issues. The integration of 6G with blockchain can help to tackle the limitations in network security. The decentralized and distributed features can help to overcome the single point of failure and DoS attacks. The immutability of data can also increase data integrity. In the same regard, intelligence is a key feature of 6G networks, as

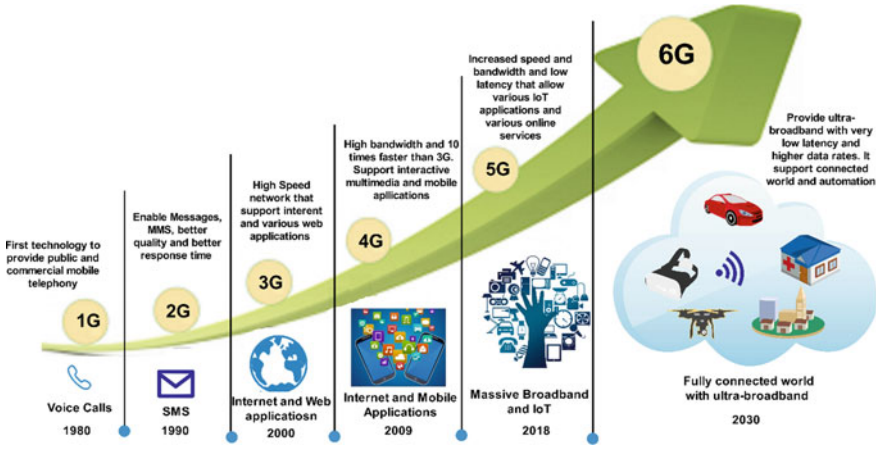

Fig. 1 Development of wireless communication technologies from 1 to 6G

the integration of AI with 6G networks can learn to achieve self-configuration, self-optimization, self-organization, and self-healing, and ultimately improving feasibility. The integration can also provide several advantages to overcome security and privacy challenges in 6G. For instance, multi-layered intrusion detection and prevention employing deep reinforcement learning and DNN can protect 6G against DDoS, flow table overloading, control plane saturation, IP spoofing, and host location hijacking attacks. The chapter provided an overview of 6G by discussing the main security and privacy issues in 6G networks. Then, the integration of blockchain with 6G was discussed by highlighting possible solutions to overcome security and privacy issues associated with 6G. The integration of 6G with AI was presented by highlighting the importance of AI in 6G and how AI can provide better and effective security and privacy solutions in 6G. In the end, healthcare with 6G was presented as a use case by highlighting security issues and discussing the role of AI and blockchain in providing effective security solutions in the healthcare sector.

References

1. Yang P, Xiao Y, Xiao M, Li S (2019) 6G Wireless Communications: Vision and Potential Techniques. IEEE Netw 33(4):70–75. https://doi.org/10.1109/MNET.2019.1800418
2. Letaief KB, Chen W, Shi Y, Zhang J, Zhang A (2019) The Roadmap to 6G: AI Empowered Wireless Networks. IEEE Commun Mag 57(8):84–90. https://doi.org/10.1109/MCOM.2019.1900271
3. David K, Berndt H (2018) 6G Vision and requirements: Is there any need for beyond 5g? IEEE Veh Technol Mag 13(3):72–80. https://doi.org/10.1109/MVT.2018.2848498
4. Elmeadawy S, Shubair RM (2019) 6G wireless communications: future technologies and research challenges. In: 2019 international conference electrical Comput. Technol. Appl. https://doi.org/10.1109/ICECTA48151.2019.8959607.

5. F. Clazzer, A. Munari, G. Liva, F. Lazaro, C. Stefanovic, P. Popovski (2019) From 5G to 6G: Has the Time for Modern Random Access Come?, Accessed: Aug. 10, 2021. https://arxiv.org/abs/1903.03063v1.
6. H. F. Atlam, A. Alenezi, M. O. Alassafi, G. B. Wills (2018) Blockchain with Internet of Things: Benefits, challenges, and future directions, Int. J. Intell. Syst. Appl., vol. 10, no. 6, doi: https://doi.org/10.5815/ijisa.2018.06.05.
7. Salman T, Zolanvari M, Erbad A, Jain R, Samaka M (2019) Security services using blockchains: A state of the art survey. IEEE Commun. Surv. Tutorials 21(1):858–880. https://doi.org/10.1109/COMST.2018.2863956
8. Meraj M, Mir I, Kumar S (2015) Evolution of Mobile Wireless Technology from 0G to 5G. Int. J. Comput. Sci. Inf. Technol. 6(3):2545–2551
9. Lopa M, Vora J (2015) Evolution of mobile generation technology: 1G to 5G. Int. J. Mod. Trends Eng. Res. 02:281–291
10. Wang M, Zhu T, Zhang T, Zhang J, Yu S, Zhou W (2020) Security and privacy in 6G networks: New areas and new challenges. Digit. Commun. Networks 6(3):281–291. https://doi.org/10.1016/j.dcan.2020.07.003
11. J. H. Schiller (2003) Mobile Communications. 2nd Edition, Pearson Education Limited.
12. Stojmenovic I (2002) Handbook of Wireless Networks and Mobile Computing. John Wiley & Sons Inc.
13. J. G. Shinde, P. Shamuvel, K. Sunil (2018) Review Paper on Development of Rice Transplanter, IRE Journals 2(5), pp. 94–100
14. A. K. Pachauri, O. Singh (2021) G Technology—Redefining wireless Communication in upcoming years, Int. J. Comput. Sci. Manag. Res., 1(1)
15. Nguyen VG, Brunstrom A, Grinnemo KJ, Taheri J (2017) SDN/NFV-Based Mobile Packet Core Network Architectures: A Survey. IEEE Commun. Surv. Tutorials 19(3):1567–1602
16. Gupta A, Jha RK (2015) A Survey of 5G Network: Architecture and Emerging Technologies. IEEE Access 3:1206–1232. https://doi.org/10.1109/ACCESS.2015.2461602
17. Nitesh GS, Kakkar A (2016) Generations of Mobile Communication. Int. J. Adv. Res. Comput. Sci. Softw. Eng. 6(3):320–324
18. Karla B, C. DK, (2014) A comparative study of mobile wireless communication network: 1g to 5g. Int. J. Comput. Sci. Inf. Technol. Res. 2:430–433
19. Eluwole OT, Udoh N, Ojo M, Okoro C, Akinyoade AJ (2018) From 1G to 5G, what next? IAENG Int J Comput Sci 45(3):413–434
20. Porambage P, Gur G, Osorio DPM, Liyanage M, Gurtov A, Ylianttila M (2021) The Roadmap to 6G Security and Privacy, IEEE Open. J. Commun. Soc. 2:1094–1122. https://doi.org/10.1109/OJCOMS.2021.3078081
21. Wang HM, Zheng TX, Yuan J, Towsley D, Lee MH (2016) Physical Layer Security in Heterogeneous Cellular Networks. IEEE Trans Commun 64(3):1204–1219. https://doi.org/10.1109/TCOMM.2016.2519402
22. De Alwis C (2021) Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research, IEEE Open. J. Commun. Soc. 2:836–886. https://doi.org/10.1109/OJCOMS.2021.3071496
23. V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, A. Rezaki (2020) Security and trust in the 6G era, NOKIA Bell Labs.
24. Ahmad I, Shahabuddin S, Kumar T, Okwuibe J, Gurtov A, Ylianttila M (2019) Security for 5G and beyond. IEEE Commun. Surv. Tutorials 21(4):3682–3722. https://doi.org/10.1109/COMST.2019.2916180
25. Y. Section, A. Gurtov, L. Mucchi, I. Oppermann (2020) 6G-White-Paper-Trust-Security-Privacy.
26. Atlam HF, Walters RJ, Wills GB (2018) Fog Computing and the Internet of Things: A Review, big data Cognitive. Computing 2(2):1–18
27. H. F. Atlam, G. B. Wills (2018) Technical aspects of blockchain and IoT, In Role of Blockchain Technology in IoT Applications, Advances in Computers, pp. 1–35.

28. Wang Q, Chen D, Zhang N, Ding Z, Qin Z (2017) PCP: A Privacy-Preserving Content-Based Publish-Subscribe Scheme with Differential Privacy in Fog Computing. IEEE Access 5:17962–17974. https://doi.org/10.1109/ACCESS.2017.2748956
29. S. Nakamoto (2009) Bitcoin: A Peer-to-Peer Electronic Cash System, DOI: https://doi.org/10.1007/s10838-008-9062-0.
30. Atlam HF, Wills GB (2019) Intersections between IoT and distributed ledger, In Role of Blockchain Technology in IoT Applications. Adv Comput 115:2019
31. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017:557–564. https://doi.org/10.1109/BIGDATACONGRESS.2017.85
32. Tt K, He K, O.-M. L, (2017) Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 24(6):1211–1220. https://doi.org/10.1093/JAMIA/OCX068
33. H. F. Atlam, M. O. Alassafi, A.Alenezi, R.Walters, G. B. Wills (2018) XACML for Building Access Control Policies in Internet of Things, In Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), pp. 253 -260.
34. Chen S, Liang YC, Sun S, Kang S, Cheng W, Peng M (2020) Vision, Requirements, and Technology Trend of 6G: How to Tackle the Challenges of System Coverage, Capacity, User Data-Rate and Movement Speed. IEEE Wirel Commun 27(2):218–228
35. Zong B, Fan C, Wang X, Duan X, Wang B, Wang J (2019) 6G Technologies: Key Drivers, Core Requirements, System Architectures, and Enabling Technologies. IEEE Veh Technol Mag 14(3):18–27. https://doi.org/10.1109/MVT.2019.2921398
36. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2020) Blockchain for 5G and beyond networks: A state of the art survey. J Netw Comput Appl 166:102693. https://doi.org/10.1016/J.JNCA.2020.102693
37. T. Hewa, G. Gur, A. Kalla, M. Ylianttila, A. Bracken, M. Liyanage (2020) The role of blockchain in 6G: Challenges, opportunities and research directions, 2nd 6G Wirel. Summit 2020 Gain Edge 6G Era, 6G SUMMIT 2020, doi: https://doi.org/10.1109/6GSUMMIT49458.2020.9083784.
38. Chowdhury MZ, Shahjalal M, Ahmed S, Jang YM (2020) 6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions, IEEE Open. J. Commun. Soc. 1:957–975
39. Jiang W, Han B, Habibi MA, Schotten HD (2021) The Road Towards 6G: A Comprehensive Survey, IEEE Open. J. Commun. Soc. 2:334–366
40. Xu H, Klaine PV, Onireti O, Cao B, Imran M, Zhang L (2020) Blockchain-enabled resource management and sharing for 6G communications. Digit. Commun. Networks 6(3):261–269. https://doi.org/10.1016/J.DCAN.2020.06.002
41. H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills (2017) An overview of risk estimation techniques in risk-based access control for the internet of things, In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), pages 254–260.
42. A. Banerjee, K. P. Joshi (2017) Link before you share: Managing privacy policies through blockchain, Proc. - 2017 IEEE Int. Conf. Big Data, Big Data, pp. 4438–4447, doi: https://doi.org/10.1109/BIGDATA.2017.8258482.
43. Maksymyuk T (2020) Blockchain-Empowered Framework for Decentralized Network Management in 6G. IEEE Commun Mag 58(9):86–92. https://doi.org/10.1109/MCOM.001.2000175
44. Butt TA, Iqbal R, Salah K, Aloqaily M, Jararweh Y (2019) Privacy Management in Social Internet of Vehicles: Review. Challenges and Blockchain Based Solutions, IEEE Access 7:79694–79713. https://doi.org/10.1109/ACCESS.2019.2922236
45. Amaizu GC, Nwakanma CI, Bhardwaj S, Lee JM, Kim DS (2021) Composite and efficient DDoS attack detection framework for B5G networks. Comput. Networks 188:107871

46. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla (2017) ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability, Proc. - 2017 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput, pp. 468–477, doi: https://doi.org/10.1109/CCGRID.2017.8.
47. M. W. Akhtar, S. A. Hassan, R. Ghaffar, H. Jung, S. Garg, M. S. Hossain, (2020) The shift to 6G communications: vision and requirements, Human-centric Comput. Inf. Sci. 2020 101, vol. 10, no. 1, pp. 1–27, doi: https://doi.org/10.1186/S13673-020-00258-2.
48. D. Silver (2017) Mastering the game of Go without human knowledge, Nat. 2017 5507676, vol. 550, no. 7676, pp. 354–359, doi: https://doi.org/10.1038/nature24270.
49. Bhatnagar S (2018) The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation Authors are listed in order of contribution Design Direction. Cornell Univ, New York
50. Reedy P (2020) Interpol review of digital evidence 2016–2019, Forensic Sci. Int. Synerg. 2:489–520. https://doi.org/10.1016/J.FSISYN.2020.01.015
51. R. Anyoha (2017) The History of Artificial Intelligence - Science in the News, Harvard University, 28 August 2017, 2018. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ (accessed Oct. 09, 2021).
52. Dua S, Du X (2011) Data mining and machine learning in cybersecurity. Taylor & Francis
53. Benzaïd C, Taleb T (2020) AI for beyond 5G Networks: A Cyber-Security Defense or Offense Enabler? IEEE Netw 34(6):140–147. https://doi.org/10.1109/MNET.011.2000088
54. Abdulqadder IH, Zhou S, Zou D, Aziz IT, Akber SMA (2020) Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defence mechanisms. Comput. Networks 179:107364. https://doi.org/10.1016/J.COMNET.2020.107364
55. Santos R, Souza D, Santo W, Ribeiro A, Moreno E (2020) Machine learning algorithms to detect DDoS attacks in SDN. Concurr. Comput. Pract. Exp. 32(16):e5402. https://doi.org/10.1002/CPE.5402
56. Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y (2021) Low-Latency Federated Learning and Blockchain for Edge Association in Digital Twin Empowered 6G Networks. IEEE Trans. Ind. Informatics 17(7):5098–5107. https://doi.org/10.1109/TII.2020.3017668
57. Ma C (2019) On Safeguarding Privacy and Security in the Framework of Federated Learning. IEEE Netw 34(4):242–248
58. H. F. Atlam, M. A. Azad, A. G. Alzahrani, G. Wills (2020) A review of blockchain in internet of things and Ai, Big Data Cogn. Comput., vol. 4, no. 4, doi: https://doi.org/10.3390/bdcc4040028.
59. Biamonte J, Wittek P, Pancotti N, Rebentrost P, Wiebe N, Lloyd S (2017) Quantum machine learning, Nat. 2017 5497671, vol. 549, no. 7671, pp. 195–202, doi: https://doi.org/10.1038/nature23474.
60. Xiao L, Sheng G, Liu S, Dai H, Peng M, Song J (2019) Deep reinforcement learning-enabled secure visible light communication against eavesdropping. IEEE Trans Commun 67(10):6994–7005. https://doi.org/10.1109/TCOMM.2019.2930247
61. M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, M. Ylianttila (2018) 5G Privacy: scenarios and solutions, IEEE 5G World Forum, 5GWF 2018 - Conf. Proc., pp. 197–203. https://doi.org/10.1109/5GWF.2018.8516981.
62. Nayak S, Patgiri R, Member S (2020) 6G Communication Technology: A Vision on Intelligent Healthcare. IEEE Internet of Things Journal.
63. Saad W, Bennis M, Chen M (2019) A vision of 6g wireless systems: Applications, trends, technologies, and open research problems. IEEE Netw 1–9.
64. Reddy B, Hassan U, Seymour C et al (2018) (2018) Point-of-care sensors for the management of sepsis. Nat Biomed Eng 29(2):640–648. https://doi.org/10.1038/s41551-018-0288-9
65. Mohammad RM, Thabtah F, McCluskey L (2015) Tutorial and critical analysis of phishing websites methods. Comput Sci Rev 17:1–24. https://doi.org/10.1016/J.COSREV.2015.04.001
66. Partala J, Nguyen TH, Pirttikangas S (2020) Non-interactive zero knowledge for blockchain: a survey. IEEE Access 8:227945–227961

67. Ji Y, Zhang J, Ma J et al (2018) BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. J Med Syst 42. https://doi.org/10.1007/S10916-018-0998-2
68. Saha A, Amin R, Kunal S et al (2019) Review on "Blockchain technology based medical healthcare system with privacy issues. Secur Priv 2:e83. https://doi.org/10.1002/SPY2.83