Chapter 18

Legal frameworks for security schemes in wireless communication systems

Abdulwaheed Musa[1,2]

Abstract

Wireless communication is one of the very successful technologies that have found applications in our daily lives. It has drawn the attention of researchers, standard bodies, and organizations who have continuously proposed and developed different standards and regulations to further advance the communication system. However, one of the major issues and concerns that have been raised in wireless communication is security with its legal frameworks. Security as well as privacy are very crucial schemes in wireless communication because of the transmission of signals over unprotected media, thus exposing signals to security and privacy attacks such as eavesdropping, modification, and data theft, among others. Depending on the type of data being transmitted, security and privacy and the legal frameworks become even more critical, especially with the adoption of new technology such as cloud computing in the healthcare and other sectors. While framework is a structure that combines, in the form of a single hybrid conceptual solution, different but relevant areas together, the legal frameworks are simply a set of standards which can be utilized to deal with a challenge or to decide what to do. Some legal frameworks have been developed, over the years, particularly in the area of healthcare, Artificial Intelligence (AI) and Internet of Things (IoT). However, there are no sufficient legal frameworks for the security and privacy of wireless network, particularly for the envisioned 6G network. Thus, this chapter presents the fundamental factors of legal frameworks for the security and privacy in a wireless communication network with a focus on the 6G network.

Keywords: 6G networks; Wireless communication; Security and privacy; Legal frameworks; Ethics; Compliance; Conflict resolution

[1]Department of Electrical and Computer Engineering, Kwara State University, Nigeria
[2]Institute for Intelligent Systems, University of Johannesburg, South Africa

18.1 Introduction

Wireless communication has a plethora of benefits over its counterpart in terms of flexibility, scalability, increased data transmission rates, and low cost of deployment, among others. As a result, there is a significant number of end-users and applications of the wireless communication systems, like the cordless mobile phones, wireless local area network (WLAN), satellite communication, etc., which have in turn generated more revenue for the service providers [1]. Similarly, the numerous users of wireless systems have drawn the attention of various standard bodies and organizations who have continuously proposed and developed different standards and regulations as well as defined frequency ranges to further advance wireless communication systems. Over the years, the wireless communications have evolved from the pre-cellular era to the first generation (1G) down to the recently developed fifth generation (5G) network [2]. Researchers have started looking into the future which presents the sixth-generation (6G) network that has been envisioned to facilitate a higher data transmission rate as well as support several novel technologies and applications. However, because of the broadcast nature of wireless communication, concerns about security and privacy, as well as legal frameworks, have been raised.

Security and privacy are the two most crucial issues in wireless communication due to the transmission of signals over unprotected media, thus exposing signals to security and privacy attacks such as eavesdropping, modification, and data theft among others [3]. Depending on the type of data being transmitted, these issues of security and privacy become even more critical, especially with the adoption of new technology, such as cloud computing in the healthcare and other sectors [4]. Legal frameworks are simply a set of standards or rules which can be utilized to deal with a challenge or to decide what to do. On the other hand, ethics are a set of moral principles and standards that guide people's actions. Legal frameworks have been developed, over the years, particularly in the area of healthcare [4], Artificial Intelligence (AI), and the Internet of Things (IoT) [5], however, there are no sufficient legal frameworks for the security and privacy of wireless network, particularly for the envisioned 6G network.

Thus, this chapter aims to present legal frameworks for privacy and security schemes in a wireless communication network including the 6G network. The legal frameworks and innovative solutions to address the privacy and security challenges in 6G wireless networks becomes necessary because of increasing scale and complexity of the systems. Key emerging security and privacy legal frameworks to support massive devices and enabling technologies in the context of 6G wireless networks are established. The chapter presents security legal frameworks and principles, including compliance, data protection, quality of service, and conflict resolution, in 6G networks. The chapter underscores the importance of adherence to laws, regulations, and standards to maintain the privacy and security of 6G networks. Also, ethical and moral principles of 6G wireless network security are highlighted in this chapter, with focus, essentially, on protecting the 6G networks and systems from unauthorized access and malicious attacks, while emphasizing the importance of secure transmission, protecting user privacy, data integrity, accountability, monitoring and auditing, and adherence to best-practice security guidelines and standards.

18.1.1 Contributions

In this subsection, the contributions of the chapter are summarized and highlighted. These are in addition to recommendations for future work in the area of study. The contributions include the following:

- Comprehensive reviews of the security and privacy schemes in wireless communication systems from 1G network up to 6G network.
- Discussion of the foundational background on the evolution of various wireless communication systems.
- Presentation of the security schemes and framework requirements.
- New conceptual security legal frameworks in wireless communication systems, including 6G networks are presented.
- Ethics and moral principles for security and privacy in wireless networks, including the 6G network have been treated.

18.1.2 Chapter organization

Aside Section 18.1 which introduces the chapter, the rest of the chapter is structured such that Section 18.2 presents the evolution of wireless networks, including an overview of the 6G networks; while Sections 18.3 and 18.4 review the security and privacy schemes in wireless communication systems from 1G up to 6G networks. Section 18.5 presents the security framework requirements. In Section 18.6, the wireless network security legal frameworks are presented. Sections 18.7 and 18.8 present the legal as well as ethics and moral principles for security and privacy in the 6G network. Limitations of the study are provided in Section 18.9. Section 18.10 concludes the chapter and provides recommendations for further research directions.

18.2 The evolution of wireless networks

In this section, the previous generations of wireless networks are discussed. The section also presents an overview of the envisaged 6G network, the key enabling technology and some applications of the 6G network. Since the development of wireless communication in 1980, it has continually experienced evolution from 1G up to 5G. These generations have been discussed extensively in the literature where it was noted that the 1G network brought about the advent of mobile communication, having to convey users' voices from the source to the required destination. However, it had many challenges such as being very expensive, little or no roaming, no security and privacy, incompatibility among different technologies, limited to voice communication only, very large equipment, among others [2]. These challenges led to the development of second generation (2G) which was digital and supported both voice and data. As a result, numerous numbers of users started utilizing cellular communication networks. Among other advantages, the 2G provided the use of Short Message Signal (SMS), a feature that was not available in the 1G network. Also, the 2G network came with little roaming and compatibility with other technologies, as well as reduced cost compared to the 1G network. However, it had its challenges such as the inability to support video traffic, lower data rate, weak security, etc. [6,7].

The third-generation (3G) network was then launched to improve the 2G network by supporting voice, data, and video communication. The 3G network introduced technology, such as Massive Input Massive Output (MIMO), is not found in the previous generations. However, there were problems with expensive terminals and high-power consumption, among others [2,6]. The fourth-generation (4G) network was then launched to provide a higher data rate than the 3G network and support voice and video over IP networks as well as online streaming. The 4G network introduced new features such as the harmonious utilization of both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) which increased the capacity of the network. There are other advantages of the 4G network such as higher throughput and simpler architecture, but there are still some disadvantages faced, such as the cost, and battery duration of devices, among others [8].

The recently developed 5G network utilizes new technologies, which include Visible Light Communication (VLC), Network Function Virtualization (NFV), Device-to-Device (D2D) communication, Software-Defined Network (SDN), Heterogenous Network (HetNet), massive MIMO (mMIMO), higher frequencies, network slicing, among others, to significantly improve data throughput, energy efficiency, connection density and reliability [9]. The key 5G use cases are ultra-reliable low latency communications (URLLC), enhanced mobile broadband (eMBB) and massive machine type communication (MTC). eMBB may provide high data speeds of 1G bits/s to mobile users, but URLLC deals more with communication reliability (99.999%) and latency (in milliseconds), particularly for applications such as IoT and vehicle-to-everything (V2X). Massive Machine-Type Communications (mMTC) emphasizes the number of interconnected devices in IoT deployment up to a million connections/km^2 [1,9]. This demonstrated the vast potential of the 5G network.

Figure 18.1 presents a summary of the evolution of wireless communication systems. Some essential features of different wireless generations, 1G to 5G, are shown in Table 18.1.

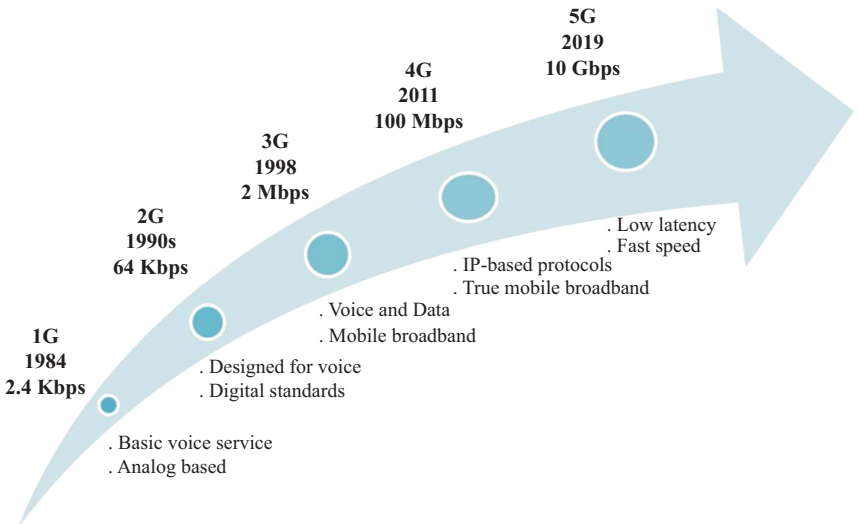


Figure 18.1 Evolution of wireless communication systems [10]

Table 18.1 A comparative of cellular generations

Generations	1G	2G	3G	4G	5G
Deployment	1979	1991	2001	2009	2018
Switching techniques	Circuit switching	Circuit switching	Circuit and packet switching	Packet switching	Packet switching
Access techniques	FDMA	GSM, TDMA, CDMA	WCDMA, UMTS, CDMA 2000, HSUPA/HSDPA	LTEA, OFDMA, SC-FDMA, WiMAX	BDMA, NOMA, FBMC
Application	Voice	Voice and data	Voice, data, and video calls	Voice, data, video calls, HD TV, etc.	Voice, data, video calls, Ultra HD video, VR application
Core network	PSTN	PSTN & packet	Internet	Internet	Internet
Data rate	2.4 kbps	14.4 kbps	384 kbps to 2 Mbps	100 Mbps to 500 Mbps	10 Gbps to 50 Gbps
Frequency band	800 MHz	800 MHz, 900 MHz, 1,800 MHz, 1,900 MHz	800 MHz, 900 MHz, 1,800 MHz, 1,900 MHz, 2,100 MHz	2–8 GHz	1.8 GHz, 2.6 GHz, 30–300 GHz
Merits	Mobility	Digital voice call, low power consumption	Better Internet experience, supports both voice and video calls	High data rate, body area network	Low latency, higher data rate, wider coverage
Demerits	Poor security, low capacity, low coverage	Low data rate, inability to support video transmission	Expensive terminals and high-power consumption	Expensive and high power consumption	Requires many small cell antennas

Recently, researchers have started envisioning the 6G network to improve the traditional wireless communications systems, increase service quality, and support massive data traffic demands. 6G networks seek to maximally increase data rates, minimize energy consumption, improve coverage and broadband connectivity, increase link dependability, reduce latency, and attain cognitive communication. 6G may offer exceptionally high data rates of over 100 Gbps with an end-to-end delay of less than 1 ms [11,12]. 6G is also projected to attain extraordinarily high communication dependability levels. The 6G criteria can be met by employing new advanced and intelligent communication systems. For instance, reconfigurable intelligent surfaces, new spectrum, extra-large MIMO, holographic radio communications, full-duplex wireless communications, modulation and multiple access are all crucial strategies for improving data rates. Furthermore, backscatter and energy harvesting techniques are both essential and required to improve energy efficiency. The merging of terrestrial and non-terrestrial communications and cell-free massive MIMO systems are viable methods for increasing connectivity and providing full coverage. AI and machine learning (ML) are critical strategies for attaining intelligence. Edge computing and holographic teleportation (telepresence) effectively create low-latency and ultra-reliable communications. Finally, quantum communication and blockchain are efficient strategies for increasing communication security, secrecy, and privacy [12–14].

18.3 Privacy and security schemes in wireless communication systems

This section presents the various security and privacy schemes in wireless communication systems from 1G to the envisioned 6G. Due to the broadcast nature of the wireless communication network, it is vulnerable to different security and privacy threats and attacks. These have drawn the attention of researchers, standard organizations and other stakeholders to continuously proffer countermeasures to these challenges. With the advancement of technology, there is a corresponding advancement in the security and privacy threats and attacks as summarized as follows.

One of the major limitations of the 1G wireless network, apart from being analog-based, was the lack of security as well as privacy. The cellular systems lacked authentication and cryptography which made call interception and impersonation attacks easy to conduct [15]. The 2G wireless network, being digital-based, addressed the security and privacy challenges witnessed in the 1G. However, it was susceptible to threats and attacks such as spamming, session hijacking, and fake base stations [16]. Other vulnerabilities witnessed in the 2G include the inability of the operators to be verified by the mobile stations, i.e. one-way authentication [15]. The 3G wireless network advanced from the 2G network and incorporated voice, video, and data, but it was susceptible to attacks and threats, such as denial-of-service, eavesdropping, location update spoofing,

identity theft, man-in-the-middle attacks which infringe on the privacy of the users as the attacker accesses confidential information [17]. The 4G was IP-based and was developed to facilitate a higher data transmission rate than the 3G as well as other novel features, such as supporting high-dimension television (HD TV). However, this advancement of technology allowed for even greater security and privacy risks and challenges as the 4G network suffered from eavesdropping, transmission control protocol (TCP) flooding, denial-of-service, intrusion, address spoofing, man-in-the-middle, user identity theft, and malware spreading and authentication delay attacks [18].

The recently developed 5G wireless network facilitated a very high data transmission rate as well as other novel applications and technologies that have significantly advanced the wireless communication system as an entity. The network has a plethora of advantages and has found several applications in various sectors of our daily lives. However, it is also vulnerable to attacks and threats due to numerous applications and technologies it supports. Such threats include eavesdropping, hijacking, denial-of-service, network slice theft, configuration, man-in-the-middle, malware spreading, jamming, and hacking attacks [16,19–21]. The 6G wireless network is expected to be an AI-based autonomous network that would not only facilitate ultra-high data rate transmission with very low latency but also incorporate both space and underwater communication to form a ubiquitous network. However, similar to the 5G network, the 6G network would be susceptible to several threats and attacks such as eavesdropping attacks, jamming attacks, access control attacks, data modification attacks, 51% attacks, and Sybil attacks [22–25]. There are also some identified privacy challenges such as data theft and the misuse of users' data. Table 18.2 presents the taxonomy of some of the attacks and threats in cellular communication systems.

Table 18.2 Taxonomy of threats and attacks in cellular communication systems

Threats	**1G**	**2G**	**3G**	**4G**	**5G**
Eavesdropping	✓	✓	✓	✓	✓
Jamming	×	×	×	✓	✓
Impersonation or identity theft	✓	×	✓	✓	×
Spamming	×	✓	×	×	×
Fabricated BS	×	✓	✓	×	×
Spoofing	×	×	✓	×	✓
TCP flooding	×	×	×	✓	✓
Malware	×	×	×	✓	✓
Hijacking	×	×	×	×	✓
Configuration	×	×	×	×	✓
Network Slice theft	×	×	×	×	✓
Penetration	×	×	×	×	✓
Injection	×	×	×	×	✓
Sniffing	×	×	×	×	✓

Several schemes have been proposed to defend against these threats in all the cellular generations. Schemes, such as voice scrambling, were utilized to provide some level of protection against eavesdropping attacks in the 1G network. However, it does not have very strong encryption, making it possible for attackers to penetrate the network and perform call interception and other malicious activity [17]. Since the 2G network was digital, cryptography schemes, such as COMP128 and A5 cryptographic, were supported. They were used to provide radio-path encryption and user authentication, respectively, but they both have shown weaknesses [25]. For the 3G network, the 3G Partnership Project (3GPP) designed an Authentication and Key Agreement (AKA) scheme which was utilized for mutual authentication of a mobile station (MS) with the network, thus addressing the one-way authentication experienced in the 2G network [26].

Similarly, in the 4G network, the AKA protocol was also utilized to mutually authenticate users and the network as well as the combination of Internet Key Exchange (IKE) and Internet Protocol Security (IP-Sec) was utilized to protect the transmission between the core network and the base station (BS) [27,28]. As mentioned earlier, the overall 5G network vulnerabilities are linked to the vulnerabilities of the key enabling technologies. Thus, some privacy and security schemes have been proposed to secure these enabling technologies, and improve the privacy and security of the 5G network. Some of the schemes include enhanced version of the AKA scheme commonly known as the 5G-AKA, Physical Layer Security (PLS), Transport Layer Security (TLS), and Session Layer Security (SLS) which are used to control channel communication [29]. Furthermore, encryption schemes that were developed for the 5G network include the Elliptic Curve Integrated Encryption Scheme (ECIES) to protect users' identities and International Mobile Subscriber Identity (IMSI) encryption to defend against IMSI catchers [29].

The brief review has shown that security and privacy challenges have been the major concern in wireless communication systems which has attracted the attention of many researchers and stakeholders who have proposed schemes to defend against the threats and attacks. However, a wireless network cannot be completely secured as advancement in technology presents further vulnerabilities, thus there is a need for continuous development and evaluation of security and privacy schemes for wireless communication systems.

18.4 6G wireless network security schemes

The merging use cases for the envisioned 6G wireless network are shown in Figure 18.2. Although the deployment of the 5G radio networks with assured low latency, extraordinary dependability, and mass connectivity, is almost completed [30,31], the network will not be able to satisfy most needs, especially after 2030.

Thus, the impacts of the 6G network include but not limited to the following: an integrated air-ground-space-sea network (SAGIN) through implementation of both terrestrial and non-terrestrial networks [32,33]; increased data speed and network traffic capacity as a result of new radio bands, such as millimeter wave,

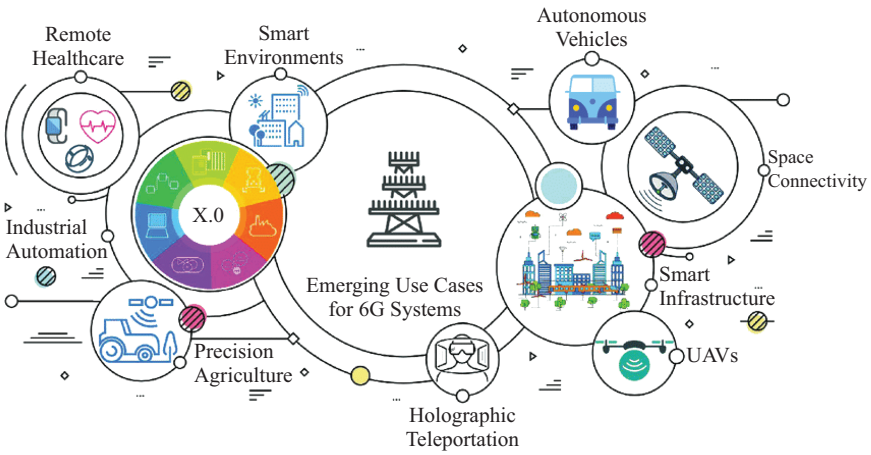


Figure 18.2 6G emerging use cases for 6G [1]

sub-6 GHz, and terahertz (THz); novel intelligent services and applications using AI and big data technologies [34–37]; and improved network security and privacy [38].

Although the privacy and security threats or attacks of the envisioned 6G network are somewhat similar to the 5G network, the 6G network technology is expected to come with better security and more spectrum coverage while using less energy. Using novel technologies, such as waveform design, multiple accesses, channel coding methods, network slicing, cloud edge computing, and various antenna technologies, 6G networks will be able to meet these demands [31].

To maintain secure communications, new security protocols must be developed to protect sensitive data and communications within these technologies. The 6G wireless network security scheme is a critical aspect of the development of 6G technology, which aims to provide a secure, reliable and fast wireless communication infrastructure for various applications. The security of a wireless network is essential to prevent unauthorized access, protect user data and privacy, and ensure the integrity of communication. In this context, several conventional security schemes such as encryption, authentication, and access control have been proposed for 6G networks. Other schemes that have been proposed to secure most of the technologies and applications in the 6G network include PLS-based schemes, quantum cryptographic schemes, Distributed Ledger Technology (DLT), and distributed AI-based security schemes. These schemes have been proposed as potential solutions to the privacy and security challenges in the 6G network and beyond [25,39,40].

The most crucial problems in 6G networks are thought to be threat detection, data processing, data encryption and traffic analysis. Security requirements for 6G use cases are more stringent than those for 5G use cases. It will be more difficult to operate and implement distributed AI security and privacy solutions as a result of the Internet of Everything's (IoE) large range of capabilities and services.

An important challenge in the development of a 6G security scheme is the integration of various security mechanisms that can provide comprehensive security solutions. For instance, encryption is an essential mechanism that ensures the confidentiality of user data, while authentication ensures that only authorized users can access the network. Similarly, access control is necessary to prevent unauthorized access to sensitive network resources [41]. The 6G wireless network security scheme should also consider the complex and dynamic nature of the network's environment [42]. For example, 6G networks are expected to be more diverse than previous generations, including different devices, users, and services. Also, the mobility of users and devices in 6G networks poses significant challenges to the security scheme, as it requires effective mechanisms to protect against unauthorized access [43].

To address these challenges, recent research has proposed the use of advanced security techniques, such as AI, ML, and blockchain. For example, ML algorithms can be used to detect and prevent security threats in real-time, while blockchain technology can provide secure and transparent data sharing between multiple parties. Additionally, the use of network function virtualization (NFV) and software defined networks (SDN) can give more efficient and flexible security solutions for 6G networks.

In summary, a secure and reliable 6G network security scheme is a critical challenge that needs a multi-disciplinary approach. The integration of various security mechanisms and the use of advanced technologies can provide comprehensive security solutions for 6G networks. However, more research is needed to tackle the specific security requirements and challenges of 6G networks, including the protection of user data and privacy, the integration of different security mechanisms, and the mitigation of security threats.

18.5 Security framework requirements

To protect sensitive information and critical systems from unauthorized access, theft, and damage, there is a need for set of guidelines, policies, and standards to ensure wireless networks security. The security framework requirements for wireless networks are crucial for ensuring the integrity, confidentiality and availability of information transmitted over the networks. The requirements include the implementation of various technical and organizational measures to prevent unauthorized access, modification, or destruction of data. The author of [44] provided an overview of the security framework requirements for wireless networks. The study highlights the need for risk assessment, threat modeling, and continuous security monitoring to ensure the security of wireless networks. It also highlights the need for organizations to adopt a proactive approach in identifying potential security threats and implementing appropriate security measures to mitigate the risks.

The security framework requirements aim at protecting the privacy and confidentiality of data transmitted over wireless networks and maintain the reliability and availability of the network services. These requirements also safeguard against

unauthorized access and protect against potential security threats to networks. The framework requirements are a mandatory collection of policies and procedures that must be put in place to secure the confidential information of customers, subscribers, network operators, service providers, and public authorities. Subscribers and network service providers who require security to protect their devices, operation and business interests all need networks and asset protection. Some of the criteria that are important and required to protect data and information from threats are as highlighted.

18.5.1 Customers and subscribers

Customers and subscribers need to comply with certain security framework requirements to protect their data and devices. The author of [45] discussed the importance of customer education and awareness in securing wireless networks, and posited that customers should be aware of the security risks associated with wireless networks and should be provided with the necessary tools and information for security. This includes regular security updates, secure password management, and the use of anti-virus software. However, the requirements also include the implementation of secure authentication and access control measures to safeguard customer information and privacy, comprehensive encryption and safe storage of customer data, secured protocols for transmitting customer data, implementation of industry standard authentication procedures for secure customer account access, as well as monitoring and blocking malicious activity. Furthermore, subscribers can defend themselves against security risks by implementing multi-factor authentication on their accounts to greatly reduce the likelihood hacking. Also, subscribers must be cautious before clicking any links and use secure passwords since significant cases of successful cyber-attacks start with phishing.

18.5.2 Network service providers

To ensure the security of wireless networks, network operators and service providers have a significant responsibility in the design, deployment, and maintenance of the networks. They must ensure that the networks are secure and meet standards. The author of [46] highlighted security framework requirements for network operators and service providers to include the use of secure protocols, encryption, and secure authentication mechanisms. In addition, it is important to conduct regular security audits, monitor network activities, and respond promptly to security incidence. The following requirements are also necessary for wireless security: implementing secure authentication and access controls, data encryption and secure data storage for operator information, adopting secure protocols for transmitting data during transit, implementing industry standard authentication procedures for secure network access, monitoring and blocking malicious activities, as well as detecting and responding to network threats.

18.5.3 Public authorities

Public authorities play a crucial role to ensure the security of wireless communication networks by developing and enforcing legal frameworks that promote

security. The author of [47] analyzed the security framework requirements for public authorities, including the development of data protection laws and regulations, the establishment of security standards, and the enforcement of penalties for security breaches. It also emphasized the importance of collaboration between public authorities and network operators and service providers to ensure the effective implementation of security framework requirements. As highlighted under subscribers and service providers' requirements, implementing secure authentication and access controls of public information, data encryption and secure data storage of public data, adopting secure protocols for transmitting public data, implementing industry standard authentication procedures for secure network access to public records, monitoring and blocking malicious activities, as well as robust incident response capabilities to effectively address security breaches are also necessary to promote the security legal frameworks for public authorities.

18.6 Legal frameworks for wireless network security

The extensive adoption of wireless networks has made the wireless network security to become a critical aspect. The widespread use of the network could be hampered by the lack of integrity, confidentiality, and security of data [48]. The security of wireless networks presents legal as well as ethics and moral issues. To address these issues and the increasing complexity of the wireless networks, such as the increasing threat of cyber-attacks, it is important for various stakeholders, including government, industry, and academia to collaborate for wireless networks security. Also, the implementation of standards, such as those established by the Institute of Electrical and Electronics Engineers (IEEE), and the management of third-party risk can play a crucial role to ensure the security of wireless networks. Nevertheless, legal frameworks play a key role in ensuring the security of wireless networks by providing guidelines on how to manage security risks and protect their networks and data.

Governments around the world, including the United States, United Kingdom, and the EU, have enacted laws and regulations to protect wireless networks [49] and safeguard data and networks [50,51]. These regulations focus on technical and administrative measures such as encryption, authentication protocols, and the responsibilities of the various parties involved in the network. In the United States, the Federal Communications Commission (FCC) implemented specific rules and regulations for wireless network security. These regulations aim to secure users from unauthorized access and interference, protect user data, and ensure the overall security of the network.

The FCC's rules and regulations for wireless network security mandate that all providers of radio frequency (RF) communication services ensure the security of their networks and protect user privacy. This act requires providers to secure the confidentiality, security, and integrity of user data, and to implement authentication and authorization measures such that only authorized users have access to the network [52].

It is also crucial for companies to be aware of the legal regulations governing their wireless networks and to have established policies to secure their networks. Various companies have thus established their own in-house regulations and processes to guarantee the safety of their wireless networks. These guidelines may touch on subjects such as access authorization protocols, user access control, network surveillance, and antivirus software. Thus, it can be concluded that the security of wireless networks is a multi-faceted and dynamic challenge.

The challenge of securing wireless networks is increased by the constrain of resources, thereby making it difficult to easily implement methods for privacy protection and attack mitigation in traditional networks for emerging wireless networks, such as 6G network. Therefore, there is a need for innovative response techniques of wireless network security and the legal frameworks.

18.7 Security legal principles

The concept of legal security underscores the systematization, stability, rule of law, and protection of human rights through the administration of justice. Security legal principles are the foundational laws and regulations that govern the protection of information, communication networks, and other related systems. These principles are designed to ensure the protection of individuals, organizations, and government entities from malicious cyber threats, unauthorized access, data breaches, and other security risks.

Until recently, wireless network security was only talked about to reduce the risks in data and the technical and organizational infrastructure that supported it. But technology advancement and awareness of the concerns over network security have changed that. The advancement has made it possible for individuals, groups, organizations and government to generate, collect, process, transmit, and store data from various sources and for different purposes. Thus, concerns over how secured what is collected are and the possible harm from privacy violations emanating from their unethical uses have also significantly increased. In recent years, the legal landscape for network security has rapidly evolved, and various organizations have published guidance and best practices to help ensure that security standards are up-to-date, consistent and relevant [53].

The IEEE addresses the importance of security legal principles that govern network security and in the development of 6G networks. A study in [46] highlighted the need for security legal principles in the design of 6G networks. It emphasizes the importance of including privacy and security considerations in the design of 6G networks, and of adhering to international privacy and security standards, such as the ISO 27001 and the NIST SP 800-53. Also, the authors of [54] emphasized the need for privacy policies and security measures that are compliant with international privacy laws and regulations, such as the General Data Protection Regulation (GDPR).

The General Data Protection Regulation (GDPR) provides the basic principles that form the framework for data protection. The fundamental tenets have a direct

and indirect effect on the different requirements and restrictions found in the law. Some of the principles contained in the GDPR include the following: Lawful, fair, and transparent processing of personal data. There should be awareness on how personal information is collected, used, or processed. The principle of transparency entails that all information on personal data processing are clear and simple. Second, personal data should only be collected for explicit, specified, and legitimate purposes; this is as determined at the time of gathering of the personal data. Thirdly, processing of personal data must be pertinent and restricted to what is required. Only when there are no other reasonable options for achieving the processing goal can personal data be further processed. Restricting storage of personal data is another (i.e. fourth) principle; a time limitation should be set for deletion or reviews to ensure that data are not stored longer than necessary. Furthermore, processing of personal data should be in such a way that confidentiality and security are ensured, including protection against unauthorized and unlawful use or access, and guarding against accidental loss or damage. Lastly, adhering to the security principles and regulations are very vital, and integral parts.

By establishing appropriate legal measures, as well as security and private policies, the 6G network can be designed and operated to protect the security and privacy of user data. Adherence to security legal principles is a crucial aspect of maintaining the safety and security of data, systems, and networks for companies, governments, and other organizations. Compliance with these laws and regulations forms an integral part of any security plan. This section further pays attention to compliance, data protection, quality of service, and conflict resolution as they relate to the legal security of information.

18.7.1 Compliance

The principle of compliance requires organizations to follow applicable laws, regulations, and industry standards to ensure the safety of their systems and data [47]. This is particularly important for organizations operating in multiple jurisdictions that must comply with the laws of each country they operate in. Organizations should have a clear process for ensuring compliance and procedures for regularly monitoring and updating their efforts [47].

In the context of 6G wireless networks, it is important to consider the adherence to laws, regulations, and standards that organizations must follow to protect sensitive data and maintain the privacy and security of their systems and networks. Compliance with security and privacy regulations as well as national and international laws related to data privacy and cybersecurity, such as the California Consumer Privacy Act (CCPA) and the European General Data Protection Regulation (GDPR) is a critical aspect of any security framework.

Organizations must ensure that their security measures align with industry standards and government regulations to protect sensitive information and maintain customer trust. The author of [55] noted that compliance with regulations can be challenging, as the dynamic nature of IoT-enabled smart cities requires frequent updates to security and privacy measures. To address this challenge, it is suggested that organizations adopt a risk-based approach to compliance, regularly assessing

and updating their security and privacy measures to ensure that they align with the latest regulations and standards.

18.7.2 Data protection

Data protection is another important principle of security legal frameworks [56]. Organizations must ensure that sensitive information is protected from unauthorized access and breach to secure and protect the integrity, confidentiality, and availability of sensitive data stored and transmitted over wireless networks. This includes implementing encryption and other security technologies, as well as establishing policies and procedures for access control, incident response, and risk management. Data protection laws vary by jurisdiction, but organizations must generally handle and store personal data securely and inform customers about data usage [57]. Organizations must also be transparent in their data handling practices and follow applicable regulations or standards [58].

In the 6G wireless networks, it will be important to consider new data protection requirements, such as privacy-enhancing technologies and the management of large amounts of data generated by IoT devices. The work in [59] underscores the importance of data protection in the 6G era and the need for innovative solutions to address the privacy and security challenges, especially as the traditional data management approaches are no more sufficient for the security and privacy requirements of 6G wireless systems due to increasing scale and complexity of the systems. To address these challenges, a blockchain-based subscriber data management protocol is proposed. This leverages the decentralized and secure nature of blockchain technology to protect the security and privacy of subscribers' data. The scheme involves the creation of a distributed ledger that records subscribers' data and transactions in a secure and tamper-proof manner, preventing unauthorized access or manipulation of the data.

18.7.3 Quality of Service

Quality of Service (QoS) is another crucial legal principle in wireless security, particularly for organizations handling sensitive information. It ensures that the security framework provides reliable and efficient performance, especially in mission-critical applications. It is important to consider how security measures may impact QoS and vice versa in the context of 6G wireless networks, as well as how to balance these considerations to provide both high levels of security and acceptable levels of performance for users. This requires an understanding of the potential trade-offs between performance and security, and the development of network design and management strategies that take these factors into account.

The European Network and Information Security Agency (ENISA) states that transferring data with minimum disruption and at desired speed and quality is critical to data security [60]. Organizations must ensure quick and secure data transfer to maintain information integrity, and ENISA recommends that they should be able to detect and respond to incidents promptly to efficiently address potential breaches.

18.7.4 Conflict resolutions

Conflict resolution is an important security legal principle that can stem from a variety of sources, including resource allocation, network configuration, and interference from other devices. It is important to ensure that conflicts and disputes between organizations and stakeholders are resolved fairly and successfully. One of the most important key components for a successful conflict resolution framework in 6G networks is the ability to quickly detect and identify conflicts as they occur. This can be accomplished through the use of monitoring and analytics tools that provide real-time visibility into the state of the network. The author of [61] discussed the importance of conflict resolution in the context of the IoT in a smart home environment. The study highlighted the importance of conflict resolution in IoT-enabled smart homes and proposed a rule-based conflict resolution framework to address the challenge of managing multiple devices in a smart home.

The EU General Data Protection Regulation (GDPR) approves that data controllers resolve disputes between themselves and data subjects efficiently [62]. The Global Network Initiative (GNI) promotes a set of principles and guidelines for companies to respect freedom of expression and privacy online, with conflict resolution as a key component [63]. The International Standards Organization (ISO) 27001 requires organizations to have a conflict resolution process in place to address disputes effectively [64].

18.8 Ethics and moral principles

Ethics are a set of moral principles and standards that guide people's actions and behavior. Every user in an organization is required to adhere to certain ethical standards and codes. Less disruption is expected in a company that conducts its activities in accordance with ethical code. Similarly, there will be negative effects on a company that does not uphold ethics. Ethics recognize right from wrong [65]. In computer security for instance, cyber-ethics is what separates security personnel from hackers.

The field of technology, including wireless network security, has a growing importance for ethics and moral principles. As technology continues to rapidly advance, it is important to ensure that its development and deployment align with ethical values. The author of [66] argues that it is important for individuals and organizations to consider ethical and moral considerations when making decisions about the development and deployment of technology and believes that ignoring these principles can have serious consequences, both for individuals and society as a whole. Also, policymakers and regulators must be involved in the development of ethical and moral frameworks, in order to ensure that technology is developed and used in ways that are consistent with the societal values.

The ethical and moral principles of the conventional security schemes and that of 6G wireless network security are similar. Essentially, they focus on protecting data, networks, and systems from unauthorized access and malicious attacks. Both emphasize the importance of protecting user privacy, data integrity, secure

transmission, responsible use of technology, accountability, monitoring and auditing, user education, and adherence to best-practice security guidelines and standards.

The authors of [67–71] examine the various conventional security schemes used in wireless networks and their respective strengths and weaknesses. Conventional security measures, such as encryption, authentication and access control have been utilized to secure and protect networks against malicious attacks and unauthorized access. While these methods have proven to be effective, they are, however, with their limitations and are vulnerable to new and evolving security threats. Thus, with the rapid advancement of technology, there is a growing need for the development of more innovative and sophisticated security protocols and schemes to stay ahead of evolving threats and ensure security of the wireless network systems.

18.9 Limitations of the study

This study is not without limitations some of which are as presented thus. Only papers and resources written in English language have been consulted, thereby limiting the research scope to English literature. Also, it is possible to miss some relevant information, but this was minimized as much as possible. The topic covered in this study is multidimensional and interdisciplinary, and this was evident in unavailability of very rich text in the research context.

Lastly, security and its legal frameworks are rarely at the top of stakeholders' concerns, except to potentially comply with fundamental norms or regulatory obligations. Besides, security and privacy issues are typically addressed after the wireless system has been developed and deployed for use. It is therefore difficult to understand the true security requirements. Thus, explanations on protection mechanisms as a form of design solution are given instead of declarative statements about the protection required, even when security requirements are to be highlighted.

18.10 Conclusion and recommendations

Legal frameworks for security and privacy schemes in wireless communication systems have become a critical aspect of modern technology. The increasing need for real-time information exchange, complexity of wireless networks, threat of cyber-attacks and more have exacerbated the need for wireless network security, privacy and legal frameworks. To maintain secure wireless communication systems, security schemes and legal frameworks have been proposed to protect data and communications within these technologies. Furthermore, ethical and moral considerations must be incorporated into the design of the security schemes.

The requirements for the network security framework emanated from various sources which include the customers (i.e. subscribers), the service providers (i.e. network operators), and the public authorities. The customers require confidence in the wireless network and reliability of the services being offered. The network service providers require security of their business interests and operations, as well

as meeting their customers and the public's obligations. As for the public authorities, they need security by legislation and orders for services availability, fair and free competition, and privacy protection.

It is recommended that the requirements for the security of wireless networks and services should be premised on international security standards. This will increase interoperability and prevent duplication of efforts. There is a need to balance the cost of security measures and the probable financial impacts of breaches in security since the security mechanisms and services are relatively expensive compared to the value of what are being secured and protected. Thus, it is necessary to have a way of customizing the provided security vis-a-vis the protected services.

Also, it is better to consider security profiles covering a range of wireless network services because of the high number of probable security features combinations. Besides, standardization will allow for reuse of solutions and products, as well as faster and low cost security. The economy of scale in component interoperation and product development within wireless networks in terms of security are important benefits of standardization both for the systems dealers and users.

The security services and mechanisms for wireless networks and operators are associated with protection against malicious attacks, such as eavesdropping, denial of service, spoofing, forgery, or tampering with messages in forms of modification, deletion, delay, replay, misrouting, re-routing, or re-ordering. Protection includes prevention, detection and recovery from threats and attacks, as well as management of personal or security-related data and information. Finally, in the framework, provisions to allow lawful and duly authorized interception are also expected.

References

[1] I. F. Akyildiz, A. Kak, and S. Nie, "6G and Beyond: The Future of Wireless Communications Systems," *IEEE Access* 2020, 8, 133995–134030, doi:10.1109/ACCESS.2020.3010896.

[2] M. H. Mahmud, "Cellular Mobile Technologies (1G to 5G) and Massive MIMO," *Int. J. Sci. Res.* 2019, 8, 929–937.

[3] V. L. Nguyen, P. C. Lin, B. C. Cheng, R. H. Hwang, and Y. D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," *IEEE Commun. Surv. Tutorials* 2021, 23, 2384–2428, doi:10.1109/COMST.2021.3108618.

[4] Z. Zandesh, M. Ghazisaeedi, M. V. Devarakonda, and M. S. Haghighi, "Legal Framework for Health Cloud: A Systematic Review," *Int. J. Med. Inform.* 2019, 132, 103953, doi:10.1016/j.ijmedinf.2019.103953.

[5] E. Nehme, H. Salloum, J. Bou Abdo, and R. Taylor, "AI, IoT, and Blockchain: Business Models, Ethical Issues, and Legal Perspectives," In *Internet of Things, Artificial Intelligence and Blockchain Technology*; Springer, 2021; pp. 67–88.

[6] S. Patel, V. Shah, and M. Kansara, "Comparative Study of 2G, 3G and 4G," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* 2018, 3, 1962–1964.

[7] M. Arshad, A. Farooq, and A. Shah, "Evolution and Development towards 4th Generation (4G) Mobile Communication Systems," *J. Am. Sci.* 2010, 6, 6.

[8] N. Rawat, "Future and Challenges of 4G Wireless Technology," *Int. J. Sci. Eng. Res.* 2012, 3, 1–7.

[9] A. Shahraki, M. Abbasi, M. Piran, and A. Taherkordi, "A Comprehensive Survey on 6G Networks: Applications, Core Services, Enabling Technologies, and Future Challenges," 2021, *arXiv Prepr. arXiv2101.12475*.

[10] M. Attaran, "The Impact of 5G on the Evolution of Intelligent Automation and Industry Digitization," *J. Ambient Intell. Humaniz. Comput.*, 2021, 14, 5977–5993, doi:10.1007/s12652-020-02521-x.

[11] X. You, C. X. Wang, J. Huang, *et al.*, "Towards 6G Wireless Communication Networks: Vision, Enabling Technologies, and New Paradigm Shifts," *Sci. China Inf. Sci.* 2021, 64, doi:10.1007/s11432-020-2955-6.

[12] H. H. H. Mahmoud, A. A. Amer, and T. Ismail, "6G: A Comprehensive Survey on Technologies, Applications, Challenges, and Research Problems," *Trans. Emerg. Telecommun. Technol.* 2021, 32, e4233, doi:10.1002/ett.4233.

[13] M. H. Alsharif, A. H. Kelechi, M. A. Albreem, S. A. Chaudhry, M. Sultan Zia, and S. Kim, "Sixth Generation (6G) Wireless Networks: Vision, Research Activities, Challenges and Potential Solutions," *Symmetry (Basel)*. 2020, 12, 676, doi:10.3390/SYM12040676.

[14] FG-NET-2030 Network 2030 – A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond, 2019.

[15] F. Njoroge, and L. Kamau, "A Survey of Cryptographic Methods in Mobile Network Technologies from 1G to 4G," *Jomo Kenyatta Univ. Agric. Technol.* 2018, 10, 1–6.

[16] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and Beyond," *IEEE Commun. Surv. Tutor*. 2019, 21, 3682–3722.

[17] S. Sullivan, A. Brighente, S.A.P. Kumar, and M. Conti, "5G Security Challenges and Solutions: A Review by OSI Layers," *IEEE Access* 2021, 9, 116294–116314, doi:10.1109/ACCESS.2021.3105396.

[18] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on Threats and Attacks on Mobile Networks," *IEEE Access* 2016, 4, 4543–4572, doi:10.1109/ACCESS.2016.2601009.

[19] A. Celik, J. Tetzner, K. Sinha, and J. Matta, "5G Device-to-Device Communication Security and Multipath Routing Solutions," *Appl. Netw. Sci.* 2019, 4, 102, doi:10.1007/s41109-019-0220-6.

[20] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G Security: Analysis of Threats and Solutions," in *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017* 2017, pp. 193–199, doi:10.1109/CSCN.2017.8088621.

[21] A. Sharma, V. Balasubramanian, and A. Jolfaei, "Security Challenges and Solutions for 5G HetNet," in *Proceedings – 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*; 2020; ISBN 9781665403924.

[22] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," in *Joint 30th European Conference on Networks and Communications and 3rd 6G Summit, EuCNC/6G Summit 2021*; 2021; ISBN 9781665415262.

[23] P. Porambage, G. Gur, M. Osorio, M. Livanage, and M. Ylianttila, "6G Security Challenges and Potential Solutions," in *Proceeding of the of the Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*; 2021; ISBN 9781665415262.

[24] M. R. Islam, M. M. Rahman, M. Mahmud, M. A. Rahman, M. H. S. Mohamad, and A. H. Embong, "A Review on Blockchain Security Issues and Challenges," in *Proceedings of the 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC),* Shah Alam, Malaysia; 2021; ISBN 9781665440110.

[25] 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. Networks* 2020, 6, 281–291, doi:10.1016/j.dcan.2020.07.003.

[26] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols," *Proc. Priv. Enhancing Technol.* 2019, 2019, 108–127, doi:10.2478/popets-2019-0039.

[27] H. Omerani, and T. Mazri, "4G and 5G: Security and Privacy Analysis," in *Proceedings of the ACM International Conference Proceeding Series*; ACM: New York, NY, October 23, 2019; pp. 1–4.

[28] K. A. Alezabi, F. Hashim, S. J. Hashim, and B. M. Ali, "An Efficient Authentication and Key Agreement Protocol for 4G (LTE) Networks," in *Proceedings of the IEEE TENSYMP 2014 – 2014 IEEE Region 10 Symposium*; 2014; pp. 502–507.

[29] R. Khan, P. Kumar, D. N. K. Jayakody, and M. A. Liyanage, "Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Commun. Surv. Tutor.* 2020, 22, 196–248, doi:10.1109/COMST.2019.2933899.

[30] R. Khan, P. Kumar, D. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Commun. Surv. Tutor.* 2020, 22, 196–248.

[31] S. S. Ranasinghe and U. M. U. Jayawardena, "6G Wireless Networks: Key Drivers and Research Challenges," *IEEE Access* 2020, 8, pp. 154213–154230.

[32] A. Yazar, S. Dogan-Tusha, and H. Arslan, "6G Vision: An Ultra-flexible Perspective," *ITU. J. Future Evol. Technol.* 2020, 1, 121–140.

[33] C. Alwis, A. Kalla, Q. Pham, *et al*., "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," *IEEE Open J. Commun. Soc.* 2021, 2, 836–886.

[34] P. Ray, N. Kumar, and M. Guizani, "A Vision on 6G-Enabled NIB: Requirements, Technologies, Deployments, and Prospects," *IEEE Wirel. Commun.* 2021, 28, 120–127.

[35] H. I. Obakhena, A. L. Imoize, F. I. Anyasi, *et al.*, "Application of Cell-Free Massive MIMO in 5G and Beyond 5G Wireless Networks: A Survey," *J. Eng. Appl. Sci.* 2021, 68, 13, https://doi.org/10.1186/s44147-021-00014-y

[36] A. L. Imoize, O. Adedeji, N. Tandiya, and S. Shetty, "6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap," *Sensors* 2021, 21, 1709, https://doi.org/10.3390/s21051709

[37] K. Sheth, K. Patel, H. Shah, S. Tanwar, R. Gupta, and N. Kumar, "A Taxonomy of AI Techniques for 6G Communication Networks," *Comput. Commun.* 2020, 161, 279–303.

[38] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, "Artificial-Intelligence-Enabled Intelligent 6G Networks," *IEEE Netw.* 2020, 34, 272–280.

[39] M. B. Gracia, V. Malele, S. P. Ndlovu, T. E. Mathonsi, L. Maaka, and T. Muchenje, "6G Security Challenges and Opportunities," in *IEEE 13th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT)*; Cape Town, South Africa, 2022; pp. 339–343.

[40] 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.* 2021, 2, 1094–1122, doi:10.1109/OJCOMS.2021.3078081.

[41] Y. F. Xiaoli Liu, "Towards 6G Networks: Key Technologies, Applications, and Open Issues," *IEEE Commun. Mag.* 2020, 58(6), 66–72.

[42] Y. Zheng Li, "Security and Privacy Issues in 6G Wireless Networks: Challenges and Solutions," *IEEE Commun. Mag.* 2020, 58(12), 50–57.

[43] W. Yuhang Zhang, "6G Wireless Networks: Vision, Requirements, Challenges, and Solutions," *IEEE Commun. Mag.* 2021, 59(1), 128–135.

[44] R. S. A. K. K. Kumar, "Securing Wireless Networks through Framework Requirements: A Review," *IEEE Trans. Depend. Secure Comput.* 2020, 17(4), 721–736.

[45] Y. L. Yajuan Zhang, "A Comprehensive Overview of Wireless Network Security," *IEEE J. Selected Areas Commun.* 2020, 37(9), 1925–1932.

[46] X. S. Jianfeng Chen, "Security Framework Requirements for Network Operators and Service Providers," *IEEE Trans. Mobile Comp.* 2022, 21(7), 1467–1475.

[47] Y. Liu, Y. Su, and Y. Yang, "Security Legal Principles in Cloud Computing: A Systematic Literature Review," *Int. J. Network Secur. Appl.* 2018, 10(6), 95–108.

[48] A. Kanuparthi, K. Ramesh, and S. Addepalli, "Hardware and Embedded Security in the Context of Internet of Things," in *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*, Berlin, Germany, November 2013, pp. 61–64.

[49] M. A. S. Zeki, "Wireless Network Security Legal Frameworks: An Overview," *Int. J. Comput. Netw. Commun.* 2018, 10(3), 1–9.

[50] G. M. Anaya, "Wireless Network Security: Legal Frameworks," *IEEE J. Commun. Netw. Secur.* 2017, 2(1), 1–10.

[51] E. I. Chuang and H. S. Hwang, "The Internationalization of Network Security Regulations: An Overview of Related Laws and Regulations," *IEEE Commun. Mag.* 2010, 48(8), 82–88.

[52] Federal Communications Commission, "Communications Act of 1934," § 222, https://www.fcc.gov/General/communications-act-1934.

[53] Y.-C. L. S.-Y. C. Hsien-Cheng Chen, "Security Framework Requirements for Public Authorities," *IEEE Commun. Mag.* 2023, 61(5), 96–103.

[54] J. L. Liu Xiong, "Privacy and Security Considerations in 6G Wireless Networks," *IEEE Commun. Mag.*2021, 59(2), 102–108.
[55] J. L, J. A. Hernandez-Ramos and V. S. M. A. V. N. A. F. S. G. B. Martinez, "Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and Future Directions," *IEEE Secur. Privacy* 2020, 19(1), 12–23.
[56] M. Khan, *Data Protection: A Practical Guide to UK and EU Law*. London: Kogan Page; 2015.
[57] B. Hutchinson, C. Mitchell, and P. Regan, *Data Protection Law*, London: Sweet & Maxwell, 2017.
[58] H. Zhang, H. Zhang, and Z. Deng, *Data Protection Law and Practice: An International Approach,* Cambridge: Cambridge University Press, 2019.
[59] X. A. W. Y. M. Z. J. W. Xueqiang Yan, "A Blockchain-based Subscriber Data Management Scheme for 6G Mobile Communication System," in *2021 IEEE Globecom Workshops (GC Wkshps)*, Madrid, Spain, 2021.
[60] ENISA, Quality of Service (QoS), 2018. https://www.enisa.europa.eu/topics/network-and-information-security/network-security/quality-of-service-qos.
[61] M. N. S. S. K. D. T. R. C. Y. L. Thinagaran Perumal, "Rule-Based Conflict Resolution framework for Internet of Things Device Management in Smart Home Environment," in *2016 IEEE 5th Global Conference on Consumer Electronics*, Kyoto, Japan, 2016.
[62] A. Khan, *Conflict Resolution in the Age of the GDPR*, 2019, https://www.itgovernance.co.uk/blog/conflict-resolution-in-the-age-of-the-gdpr.
[63] Global Network Initiative, *GNI Principles & Implementation Criteria*, 2018, https://globalnetworkinitiative.org/principles-implementation-criteria/
[64] ISO, ISO/IEC 27001:2013, 2020. https://www.iso.org/standard/57867.html.
[65] S. Rahman, "Ethics and Philosophy of Security," in J. McPherson (Ed.), *Security and Privacy: Foundations, Technologies and Applications*, IGI Global, pp. 24–52, 2020.
[66] W. James Alexander Hughes, "We Are Not Pontius Pilate: Acknowledging Ethics and Policy," in *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, Canberra, ACT, Australia, 2021.
[67] V. B. Kumaravelu, A. L. Imoize, F. R. C. Soria, *et al*., "Outage Probability Analysis and Transmit Power Optimization for Blind-Reconfigurable Intelligent Surface-Assisted Non-Orthogonal Multiple Access Uplink," *Sustainability* 2022, 14, 13188, https://doi.org/10.3390/su142013188.
[68] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks," *IEEE Commun. Mag.* 2019, 57, 84–90.
[69] 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.* 2020, 27, 126–132. "Conventional Security Schemes in IoT: A Survey," 2021.
[70] S. Saxena, "Security Techniques in Wireless Networks," *Wireless Commun. Mobile Comput.*2005, 5(6), 563–576.
[71] M. Alsabah, M. A. Naser, B. M. Mahmmod, *et al.*, "6G Wireless Communications Networks: A Comprehensive Survey," *IEEE Access* 2021, 9, 148191–148243, doi:10.1109/ACCESS.2021.3124812.