Array 18 (2023) 100290

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/locate/array

A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions

Abdul Ahad [a], Zahra Ali [a], Abdul Mateen [a], Mohammad Tahir [b,*], Abdul Hannan [c], Nuno M. Garcia [d,e], Ivan Miguel Pires [d,f,**]

[a] Knowledge Unit of Systems and Technology (KUST), University of Management and Technology, Sialkot, 51040, Pakistan
[b] Department of Computing, University of Turku, FI-20014, Turun Yliopisto, Finland
[c] AAxis Technology solution group, Islamabad, 04403, Pakistan
[d] Instituto de Telecomunicações, Universidade da Beira Interior, 6200-001, Covilhã, Portugal
[e] Universidade de Lisboa, 1749-016, Lisboa, Portugal
[f] Polytechnic Institute of Santarém, 2001-904, Santarém, Portugal

ARTICLE INFO

Keywords:
Smart healthcare
5G
Security
Artificial intelligence
Block chain

ABSTRACT

Healthcare is experiencing a fast change from a hospital-centric and specialist-focused model to one that is dispersed and patient-centric. Numerous technological advancements are driving this fast evolution of the healthcare sector. Communication technologies, among others, have permitted the delivery of customized and distant healthcare services. The present 4G networks and other wireless communication technologies are being utilized by the healthcare industry to create smart healthcare applications. These technologies are continuously evolving to meet the expectations and requirements of future smart healthcare applications. At the moment, current communication technologies are incapable of meeting the dynamic and complex demands of smart healthcare applications. Thus, the future 5G and beyond 5G networks are expected to support smart healthcare applications such as remote surgery, tactile internet and Brain-computer Interfaces. Future smart healthcare networks will combine IoT and advanced wireless communication technologies that will address current limitations related to coverage, network performance and security issues. This paper presents 5G-based smart healthcare architecture, key enabling technologies and a deep examination of the threats and solutions for maintaining the security and privacy of 5G-based smart healthcare networks.

1. Introduction

Healthcare is undoubtedly a necessary component of lives. However, current healthcare systems are under a great deal of difficulty due to the growing elderly population and the accompanying rise in chronic illness [1], having a high demand for resources, including doctors and nurses as well as hospital beds [2]. A solution is required to reduce the burden on healthcare systems without compromising the quality of care for the most vulnerable patients. The Internet of Things (IoT) and 5G have already been widely highlighted as prospective solutions for reducing constraints on healthcare systems [3] and are given considerable attention by researchers to solve various challenges to provide smart health solutions. For example, solving challenges related to the observation of patients afflicted with certain disorders, such as Parkinson's disease [4], and diabetes [5]. Additional research is being carried out to target specific goals, such as aiding in rehabilitation by continually monitoring the progress of a patient [6]. Emergency healthcare has also been suggested as a potential in related papers [7–9] although it is not investigated in detail. Previous research has looked into certain subjects and technologies related to IoT healthcare. In [10], a comprehensive survey, with an emphasis on currently possible solutions, various applications, and unresolved challenges, is presented. Each subject is examined independently rather than as part of a whole system. In [11], data mining, storing, and evaluation are discussed but do not provide a discussion of their integration into a system. In [12], a comparison of several sensors, emphasizing communications, is presented. Unfortunately, it is not easy to construct a picture of a whole system from this study. Finally, the paper [13] focuses only on sensing and massive data handling, with less concern for the network that will enable communications.

New cellular technology known as fifth generation (5G) wireless seeks to improve communication speeds and responsiveness across 5G wireless networks [14]. With the introduction of new technologies, 5G

[*] Corresponding author.
[**] Corresponding author at: Instituto de Telecomunicações, Universidade da Beira Interior, 6200-001, Covilhã, Portugal.
E-mail addresses: tahir.mohammad@utu.fi (M. Tahir), impires@it.ubi.pt (I.M. Pires).

https://doi.org/10.1016/j.array.2023.100290
Received 26 January 2023; Received in revised form 2 May 2023; Accepted 3 May 2023
Available online 8 May 2023

Table 1
Existing survey on 5G-based smart healthcare.

References	Contributions of authors
Ahad et al. [19]	The authors of this review article presented the architecture and taxonomy of a 5G-based smart healthcare network in this study, which included communication protocols, objectives, performance metrics, and requirements. Second, the author provided a comprehensive description of many methodologies, such as scheduling, congestion control, clustering and routing, that may be used to accomplish the various objectives and needs of smart health care. Finally, the author discussed unresolved issues and challenges associated with intelligent smart healthcare.
Dhanvijay et al. [20]	The authors of this review article provided a review of several IoT smart healthcare systems for WBAN that allow data transmission and receiving. Second, the author comprehensively examined privacy protection, power efficiency, strategic planning, and resource management in IoT smart healthcare.
Mahmoud et al. [21]	The authors of this review paper explored the concept of the Cloud of Things (CoT) and how it may be used in the development of smart medical applications. Second, the author extensively analyzed various topics, including using CoT for smart healthcare applications, including energy efficiency.
Tariq et al. [22]	The authors of this review article presented an integrative study comparing currently available state-of-the-art surveys on security and safety, challenges and open issues in patient information exchange, vulnerabilities in existing solutions, and privacy promises about block-chain attach in smart healthcare. The main contribution of this review is to provide a brief explanation of the critical security requirements for smart healthcare systems. Additionally, the authors address the advantages of blockchain adoption in terms of security and its usefulness in smart healthcare by analyzing several blockchain-based solutions for securing healthcare data against possible security breaches.
Qi et al. [23]	The author of this review article investigates numerous IoT applications for smart health care from a variety of perspectives (i.e., monitoring of blood pressure, heartbeat, oxygen saturation etc.). Second, the author reviewed the various enabling IoT technologies available for smart healthcare applications, including network connectivity, processing of data, and sensing technologies.
Algarni et al. [24]	The authors of this review article demonstrate the distribution of recent work on the security and privacy for smart healthcare classified by publishing venue and year. It comprises classifications of the articles included in this article, arranged according to their aim, approaches, security method, and applications. Second, the authors highlighted the most often stated security attacks in smart healthcare systems and the recommended solutions against such attacks. Third, the authors explain how current research addresses security and privacy issues in smart healthcare systems, highlight research issues in privacy and security in smart healthcare systems, and provide recommendations for future research.
Baker et al. [25]	The authors of this review article presented a smart healthcare model for health monitoring in this study, which may be utilized for worldwide tracking and monitoring of unique human conditions. Second, the authors provided an overview of the state-of-the-art for each part of the suggested model (i.e., blood pressure monitoring sensors and smart wearables which monitor various conditions of the body and vital signs). Third, the author discussed various communication protocols for intelligent smart healthcare.
Ahad et al. [26]	The authors of this review article presented a taxonomy of intelligent smart healthcare, which covers communication technologies, various networks, services, applications, needs, and features. Second, the authors presented numerous possibilities for 5G-enabled smart health care and associated requirements. Third, the authors presented critical enabling technologies to fulfill the 5G smart healthcare criteria and unresolved issues and challenges.

wireless networks can provide low latency with a high data rate and a wide coverage area, enhancing global communication. Its deployment can be accelerated over the next few years to meet the growing use of mobile and Internet-connected devices [15]. Cyber-physical systems (CPS) and the IoT are examples of Internet-oriented infrastructure that may be employed in smart healthcare [16,17], and 5G will provide them with ultra-reliable, low-cost broadband access. The 5G network is not a novel idea; it is an evolution of the 4G network. 5G technology is defined as the deployment of the novel, innovative techniques to meet the increasing demands of network congestion and future services via IoT devices for different applications such as smart healthcare [18]. With these needs in mind, 5G enables a variety of communication modes, including device-to-device (D2D), machine-to-machine (M2M) and human-to-machine (H2M). Security is the primary objective of 5G-based smart healthcare.

1.1. Our contribution

There are several attempts to examine 5G-smart healthcare from a wider perspective. The contributions of 5G-smart healthcare research papers that have been published are summarized in Table 1. To the best of our knowledge, this is the first research to examine the security of 5G-based smart healthcare networks.

Our research study makes the following significant contributions:

- We present a 5G-based smart healthcare architecture, taking into account certain enabler technologies (small cells, D2D communication, advanced MIMO, software-defined networking (SDN), mmWaves, NOMA, Network function virtualization (NFV), and edge computing for 5G smart healthcare.
- Discussion on major security concerns, such as security threats (i.e., authentication, confidentiality, availability, non-repudiation, integrity) and attacks that exist in 5G-based networks for smart healthcare.
- A summary of pre-existing solutions for the security issues and presented possible emerging technologies and solutions for 5G-based smart healthcare network security.
- Finally, we discuss several research issues and potential future research directions for 5G-based smart healthcare security.

1.2. Organization of this paper

This paper is organized as follows: In Section 2, a brief overview of 5G smart healthcare architecture and key enabling technologies are presented. Section 3 presented a taxonomy for 5G smart healthcare security, covering security threats, attacks, and existing security approaches. Section 4 presents security solutions for 5G-based smart healthcare networks, including Blockchain, Artificial intelligence, Cyber-physical system (CPS) and Quantum cryptography. Section 5 presents open issues and future research direction for 5G smart healthcare. Finally, the conclusion is presented in Section 6.

2. 5G smart healthcare architecture and key enables technologies

The term "5G" refers to the fifth generation of wireless mobile networks, which will complement existing 4G networks before ultimately replacing it. This section discusses 5G design, features, and performance improvements. The architecture of 5G smart healthcare is shown in Fig. 1.

2.1. Architecture of 5G

5G networks will make use of a large number of small cells to build an ultra-dense network. These small cells are radio access nodes that operate on a low power level and have a diameter ranging from a few meters to one mile. Applications for 5G smart healthcare can benefit significantly from utilizing a wide variety of small cells. Since smart healthcare applications demand high data rates (for instance, remote

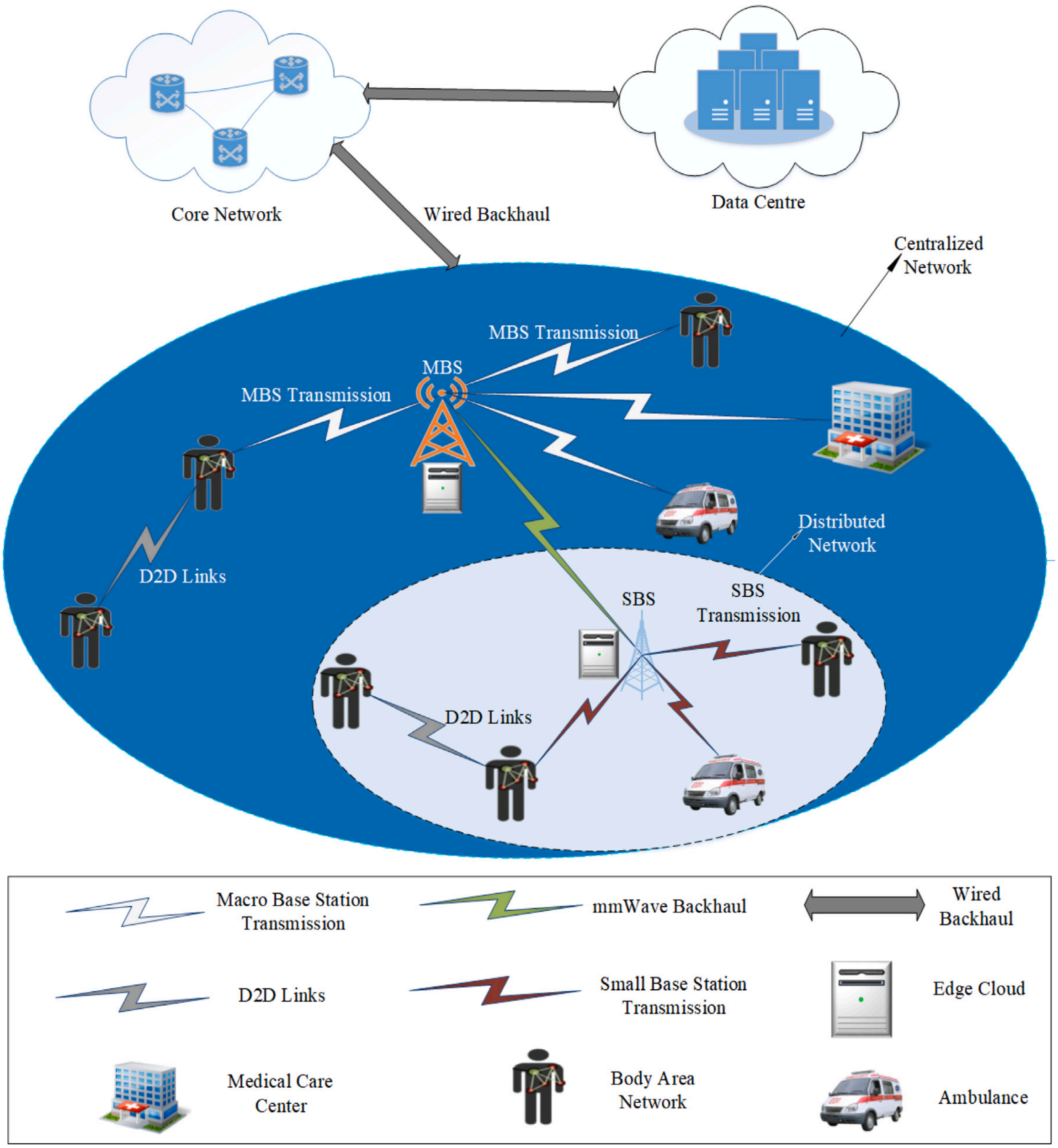

Fig. 1. A general architecture of 5G based smart healthcare.

surgery requires data rates ranging from 137 Mbps to 1.6 Gbps [27]), one approach is to employ small cells [28]. Small cells are classified into three categories, ranging in size referred to as femto, pico, and microcells. These are considered small cells compared to the macro cell, which has a range of around 20 miles. Femtocells are often used to expand capacity and coverage in a limited area, such as a hospital or residence. It comes with a support of 30 users across the 0.1-km range. Picocells increase capacity and coverage, supporting up to 100 users on a 1-km scale. Picocells are often used to increase the coverage of cellular and wireless networks within a limited area. The key differences between microcells and picocells are the coverage area and the capacity to support more users. Within a two-kilometre range, microcells may accommodate up to 2000 users. In cellular networks, Marco cell technology offers radio coverage over a wide area of mobile network access. It covers a large area and delivers a high-efficiency output. [29]. A microcell is deployed in a station with high output power. It accommodates around 2000 users within a 30-km radius. By deploying small cells, the network may improve area spectrum efficiency through spectrum sharing. Additionally, in small cells, the control plane and user plane operate independently, the control plane providing connection and mobility and the user plane providing data transmission [30]. The user equipments (UEs) must thus be connected to macro- and small-cell base stations simultaneously. Macro-cell base stations use lower frequencies to provide connectivity and mobility (control plane). On the other hand, small-cell base stations function at a higher frequency to facilitate high-throughput data transmission. [31]. Heterogeneous networks (HetNets) typically include cellular networks with macro, micro, pico, and femto base stations. They are utilized for efficient spectrum usage and adaptable coverage. Table 2 summarizes the contents of small cells.

2.2. 5G features and enable technologies

2.2.1. D2d communication

D2D is a technique for two devices to communicate directly over a network that does not need a base station (BS). D2D communications

Table 2
Summary of small cells.

Cell types	Cells radius (km)	Users	Locations
Femto cell	0.010 to 0.1	1 to 30	Indoor
Pico cell	0.25 to 1.0	30 to 100	Indoor/Outdoor
Micro cell	0.2 to 2.0	100 to 2000	Indoor/Outdoor
Macro cell	8 to 30	More than 2000	Outdoor

may be used to tackle difficulties in the highly-dense networks [32]. In D2D communication, each terminal has the option of direct communication to exchange data or exchange radio access connections. D2D communication may help decrease interference, especially in unlicensed frequency bands [33]. The concept of D2D communication does not exist in a 4G network. The gateway and base station are used to handle all communications. This method is inefficient, as it creates a bottleneck at the base stations. Direct communication can be more beneficial when a significant number of devices are involved in the machine-to-machine paradigm. Ad-hoc networking technologies, such as Bluetooth and WLAN, allow devices to communicate in an unlicensed spectrum outside of the cellular network. However, These links are susceptible to interference. But, when links are properly managed, licensed spectrum assures the quality of services. To achieve connectivity, these D2D communications require base stations to ignore intra-cell interference [34].

2.2.2. Advance massive MIMO

The spectral efficiency and data rate may be increased by using modern massive MIMO. MIMO is an acronym for multiple-input, multiple-output. 5G-based smart healthcare network capacity may be increased by increasing the number of sending and receiving antennas [35]. Multiple transmitting and receiving antennas may be utilized concurrently to manage massive amounts of data traffic generated by healthcare devices in the network. In a 4G network, a base station has twelve ports for processing cellular communications (MIMO). Eight of the twelve are for broadcast, while four are for receiving. In 5G, this number increases to around 100 ports per base station, resulting in massive MIMO communication [36].

2.2.3. Software defined network

SDN is a dynamic, controllable, adaptable, and cost-effective architecture that enables the delivery of high bandwidth demanded by various applications [37]. SDN integrates many network technologies to make the network more flexible and adaptable to manage virtualized servers and storage infrastructure. SDN networking is a methodology for constructing, developing, and managing networks that distinguish network forwarding planes and control planes [38]. SDN can fulfill a variety of smart healthcare requirements in 5G. Depending on the operator's policies, certain use cases can be handled in the cloud, while those that need a quick response and virtual services can be handled in the edge cloud.

2.2.4. NOMA

The term "NOMA" refers to non-orthogonal multiple access. It is a technique that facilitates multiple users while using the same time and frequency resources but different energy resources [39]. The use of various transmission levels accomplishes multiplexing of the same frequency. Unlike previous generations, the power domain is used for multiple access, when Code Division Multiple Access (CDMA), Orthogonal Frequency-division multiplexing (OFDMA), Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) domains served many users in 1G, 2G, 3G, and 4G, respectively. NOMA contributes to the enhancement of spectrum efficiency and connection density. Additionally, it allows flexibility between strong and weak users and mitigates the effects of multiple access interference [40].

2.3. Network function virtualization

NFV is a rapidly evolving networking technique that permits the replacement of high-cost specialized hardware devices, such as routers and firewalls, with network tools based on software and runs as virtual machines on standard servers [41]. 5G must allow D2D communication in smart healthcare, which is expected to create a vast amount of data. It is not feasible to process all produced data at the centralized data centre. Furthermore, future applications will be highly dynamic and demanding, which requires the network to be flexible. The NFV enables data to be processed according to QoS requirements by strategically placing the required networking components. NFV allows the creation of network slices, which enables the orchestration of virtualized network environments that are tailored for particular healthcare applications, including telemedicine or remote monitoring. This enables healthcare providers to provide priority to traffic for crucial healthcare applications, cut down on latency, and guarantee QoS. NFV can also be used to implement virtualized security tools like firewalls and intrusion detection systems that can scale up and down based on traffic patterns and threat levels. This can assist healthcare practitioners in protecting patient data privacy and security, which is essential in the healthcare sector.

By offering a more flexible, scalable, and economical network infrastructure, NFV can significantly improve the delivery of healthcare services.

2.3.1. mm-waves

Radio waves that fall between 20 and 300 GHz are known as mmWave. 5G must operate in the mmWaves band, especially between 20 and 90 GHz, because the spectrum below 3 GHz is scarce [42]. However, the mmWaves suffer high path loss which limits the coverage area. The problem of excessive path loss can be solved by combining mmWaves with small cells [43], which covers a small area and provide high bandwidth due to the use of mmWave. Such a combination is useful for various applications, including smart healthcare. In several field trials, the mmWaves are shown to be feasible and are being used in a broad variety of use cases. The mmWave increases wireless communication beyond the capabilities of existing radio technology to provide high throughput while complementing the low-frequency transmission.

2.3.2. Edge computing

Edge computing is a distributed technology architecture in which data is handled at the edge of the network near the point of origin. Devices are anticipated to make decisions and react accordingly to tasks in the future smart healthcare application to reduce latency enabling real-time applications. Edge computing has the potential to completely change the way healthcare is provided by enabling remote monitoring, personalized treatment, and faster and more accurate diagnosis. In these circumstances, where a quick decision is more crucial, edge computing is essential, especially in 5G networks [44]. Furthermore, by keeping sensitive patient data inside the hospital or on the device itself, edge computing can offer improved data security while lowering the risk of data breaches and cyberattacks.

3. Taxonomy

5G will bring a revolutionary shift in mobility and accelerate the Internet of Medical Things growth. 5G, consisting of software-defined networks and network slices, would enable evolutionary algorithms to create unique applications for diverse network levels. According to the literature review, 5G enables low latency, flexibility, pervasive mobility, reliability, dependability, and fog computing, which are necessary for extremely large-scale Internet of Things applications [45–47]. Fig. 2 shows the taxonomy of 5G smart healthcare security.

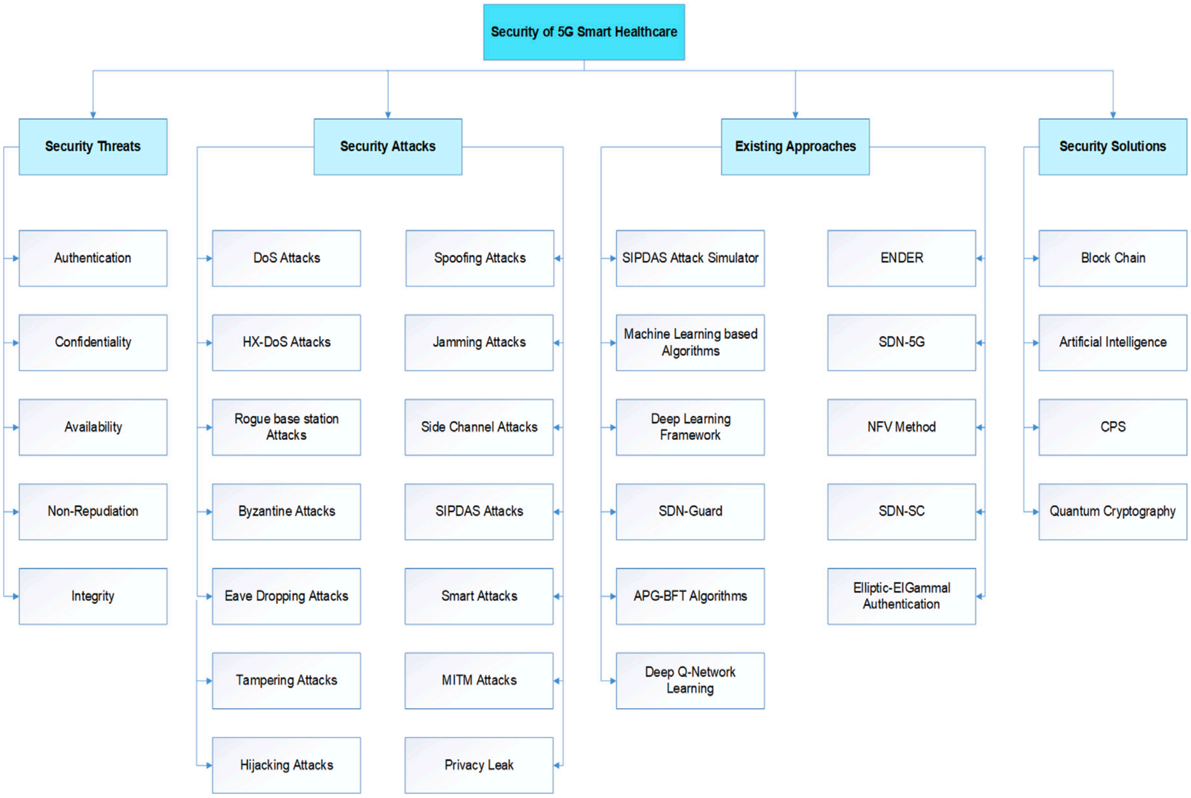

Fig. 2. Taxonomy of 5G smart healthcare security.

3.1. *Security threats*

Threats are an effort to obtain illegal access to information, assets, services, cause loss and harm to information systems. Table 3 presents the summary of different security threats and attacks relevant to 5G smart healthcare.

3.1.1. *Authentication*

Authentication is a critical concept in 5G-based smart healthcare network security because it allows the verification of user identities within the network. Numerous mechanisms are employed in the 5G-based smart healthcare network for data authentication. It is divided into two sections: primary and secondary authentication. Primary authentication enables mutual authentication of medical devices and networks in both networks 5G and 4G [48]. However, primary authentication in a 5G-based network has several issues, including knowledge control, and the call of device authentication is insufficiently supported. These difficulties are addressed via the usage of Authentication Protocol Privacy (5G-AKA) and flexible authentication schemes. Primary authentication is compatible with technologies other than Third Generation Partnership Project (3GPP). Secondary authentication is used beyond the domain of the mobile operator and is based on the 3GPP standard. Secondary authentication is possible via Extensible Authentication Protocol (EAP) based linked techniques [49].

3.1.2. *Confidentiality*

Confidentiality is a security attribute. Confidentiality ensures that an authorized person can only access the information about the sender. The key needed by the secondary next-generation base node (SgNB) is created and provided by the master base node (MeNB) before any secure new radio (NR) transmission; the UE likewise generates and sends the same key [50]. Signals for radio resource control (RRC) can be sent between the secondary next-generation base node (SgNB) and user equipment (UE). As a result, the keys are utilized to ensure the authenticity and privacy of user plane (UP) data and RRC messages. Although 5G networks allow integrity protection for UP data, they cannot be implemented in the EUTRA-NR Dual Connectivity (EN-DC) scenario. Both UP and RRC allow for the usage of confidentiality.

3.1.3. *Availability*

The 5G-based smart healthcare network benefits from cloud resources, which helps develop cost-effective infrastructure. However, security threats like cyberattacks threaten the reliability of the network. DDoS attacks require physical and logical resources at the edge and cloud levels, which has an influence on network-slicing processes. Jamming attacks cause problems on radio access facilities, preventing users from accessing cellular services [51]. Attacks on 5G resources, including the support system, control plane, and radio, can disrupt the smart healthcare network.

3.1.4. *Non-repudiation*

The capacity to demonstrate the validity and reliability of a message or transaction and prohibit the sender from denying their involvement in the communication is known as non-repudiation. The deniability of users cannot be stopped by authentication alone. However, as it is vital to distinguish between different users or UEs to generate safe data transfer, authentication is necessary to ensure non-repudiation [52]. 5G networks can make use of digital signatures to ensure non-repudiation. Digital signatures use a cryptographic technique to create a unique code that is added to the message, which can be used to prove the authenticity and integrity of the message. This makes it difficult for the sender to deny their involvement in the communication.

3.1.5. *Integrity*

A security measure in the 5G network is user plan integrity protection between next-generation node B (gNB) and IoT devices. It is consistent with gNB's and IoT devices' use of encryption. Integrity protection is a resource-intensive feature that IoT devices cannot implement at a high data rate due to their limitations [53]. Thus, the

Table 3
Summary of different security threats and attacks in 5G smart healthcare.

Security attacks	Security threats					Target components
	Authentication	Confidentiality	Availability	Non-repudiation	Integrity	
DoS attacks			✓		✓	Cyber physical cloud
Spoofing attacks	✓	✓				Physical layer
HX-DoS attacks			✓			Cyber physical cloud
Jamming attacks			✓			Radio interface
Rogue base station attacks	✓	✓				Centralized control elements
Side channel attacks		✓	✓		✓	Network Slices
Byzantine general attacks					✓	Distributed computing
SIPSAS attacks			✓			Cyber physical cloud
Eaves dropping attacks		✓				Fog/Edge computing
Smart attacks	✓	✓	✓	✓	✓	Centralized control elements
Tampering attacks		✓				Cloud and Fog computing
Hijacking attacks			✓			SDN controller
Privacy leak		✓				User equipments

5G-based smart healthcare network architecture must include protocols that ensure network integrity. For example, 5G networks may use cryptographic algorithms such as Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) to create a unique code that is added to the data, which can be used to verify the integrity of the data. This ensures that the data has not been modified or tampered with during transmission.

3.2. Security attacks

This subsection presents the numerous security concerns in 5G-based smart healthcare networks, as illustrated in Table 4.

3.2.1. DoS attack

In a denial of service (DoS) attack, the attacker makes an attempt to send a large volume of bogus data targeted towards nodes of the network. This large number of requests may consume power, bandwidth and time, etc. causing the node to crash or be unable to respond to legitimate requests. When many computers on a network are utilized to initiate a distributed denial of service attack (DDoS), the security of several of those computers and networks may be breached.

3.2.2. Spoofing attacks

Spoofing is a vulnerability that allows an attacker to intercept genuine interactions on a 5G network. Spoofing attacks include injecting false signals using a fake identity to get unlawful advantages and launch additional malicious attacks such as man-in-the-middle and denial of service attacks [54]. Spoofing attacks are a risk in wireless communications used for 5G-based smart healthcare because of the vulnerability of wireless communication to physical layer attacks.

3.2.3. HX-DoS attack

In the Cyber-Physical Systems (CPS) architecture, this attack combines eXtensible Markup Language (XML) and Hyper Text Transfer Protocol (HTTP) messages the attacker sends to overflow scripts and damages the cloud service provider's communication channel capability. These attacks might be easily deployed in the CPS cloud environment using web services such as Software as a Service (SaaS), platform as a service (PaaS), and Infrastructure as a Service (IaaS) [55]. While these attacks are quickly mitigated, they might cause complications if they occur often.

3.2.4. Jamming attack

The performance of the 5G network can be affected by malicious cyberattacks, which are possible to launch against the network. Because control channels are necessary to operate the radio interface effectively, wireless communication in 5G-based smart healthcare networks is vulnerable to cyberattacks that jam the radio interface. By jamming certain control channels with high-powered signals, an attacker might cause damage to the frequency bands. If an attacker compromises many devices and establishes a botnet, the intensity of the jamming attacks improves. Collectively, these hijacked bot mobile medical devices may act as jamming devices [56,57].

3.2.5. Rogue base station attacks

Automation of network optimization and setup for optimal network management resulted in the emergence of a new threat called rogue base stations (RBS) [58]. In order to conduct unauthorized and illegal monitoring for any potential communication disturbances, an attacker impersonates a real base station. An attacker tries to learn the identities of users by monitoring the International Mobile Subscriber Identity (IMSI) of the user's device using fake base stations.

3.2.6. Side-channel attack

Multiple slices of 5G-based smart healthcare networks use the same physical infrastructure and resources, enabling 5G network slice side-channel attacks. When a translator is capable of inferring particular physical patterns and features, such as power management, in order to obtain confidential data, this type of assault is known as a side-channel attack. In comparison to earlier network generations, 5G networks are more susceptible to this kind of attack since they are based on network slicing, allowing an attacker to isolate and assess a particular slide's performance easily.

3.2.7. Byzantime general attack

In this strategy, the adversary stops transmitting received packets but continues actively participating in the network. In this strategy, the adversary may selectively drop packets, modify selected packets, transmit most of the data in its encoded form, and alter selected packets. It resembles a Byzantine general problem. To ensure that all obedient lieutenants obey the same order in this scenario, the commanding general must rely on his (n-1) lieutenant generals to provide commands. If the commanding general is trustworthy, the obedient lieutenant will follow his orders [59].

3.2.8. SIPDAS attack

Since it creates and transmits a legitimate SIP INVITE message to the destination component SIP, it is also related to the DoS attack. It may generate spoofed IP addresses in three ways: manually, randomly, or by picking the faked IP address from the subnet. IP addresses may be explicitly defined or created randomly [60].

3.2.9. Eavesdropping attacks

When a hacker intercepts, deletes, or alters data being transferred between two devices, this is referred to as an eavesdropping attack. Attackers can employ a variety of techniques to initiate eavesdropping attacks, which frequently entail the deployment of different eavesdropping devices to listen in on conversations and examine network activities [61].

Table 4
Summary of existing approaches in 5G smart healthcare security.

Security approaches	Privacy	Target components
SIPDAS attack simulator	×	Physical cloud
ENDER	✓	Centralized servers
Machine learning based algorithms	✓	Physical layer authentication
SDN-5G	✓	Centralized servers
Deep learning framework	×	Wireless android based devices
NFV method	✓	Edge/Fog computing
SDN-SC	×	Core network
APG-BFT algorithms	✓	Centralized servers
Elliptic-	✓	Secret key based authentication
Deep Q-network learning	✓	Edge server

3.2.10. *Smart attacks*

An intelligent attacker may use smart radio equipment to monitor the health of the network and select the appropriate attack method, such as jamming and spoofing, depending on the network's range from the edge node they are attempting to attack. This can be done by deploying smart radio equipment to monitor the network [62].

3.2.11. *Tampering attacks*

Without the user's knowledge or consent, an attacker may cause delays or make unauthorized changes to the data sent over the network connection. The attacker may interrupt or degrade edge or cloud computing's productivity and effectiveness. These attacks, which are difficult to detect, might cause data packets to be delayed or fail to transmit due to the wireless network and user mobility (UMs).

3.2.12. *MITM attack*

An attacker will carry out a man-in-the-middle attack, also known as a MITM attack when they establish a momentary condition that permits the interception of data transmission between UEs over the network to change the content of the data transfer [63].

3.2.13. *Hijacking attacks*

It serves the purpose of squandering the controller's resources (i.e., data-to-control plane saturation). By leveraging the resources the controllers provide, the attacker's goal is to either slow down or perhaps completely disable some areas of the network.

3.2.14. *Privacy leak*

In the worst-case scenario, the data stored on edge devices might be leaked by owners who are unauthorized or suspicious, or the devices themselves could be sold to a third party.

3.3. *Existing security approaches*

This section discusses available solutions for the attacks mentioned above in 5G smart healthcare networks.

3.3.1. *SIPDAS attack simulator*

It is a Cyber-Physical System (CPS) strategy tool for simulating SIP-based denial-of-service attacks and mitigating them from the edge/cloud. This strategy consists of four key elements: a message sender, a SIP message generator, an IP address generator, and a scenario player. It requires the output of SIP-ENUM (Network Enumerator) and SIP-NES (Network Scanner), as well as other preconfigured files [64]. SIP-ENUM determines whether SIP users are legitimate based on network replies by delivering registered messages to each client's IP address during SIP-NES production. This method creates completely random INVITE messages that do not include any patterns. Every single INVITE message generated abides by the SIP RFCs and is interoperable with every SIP component.

3.3.2. *ENDER*

ENDER is an abbreviation for a pre-dEcisioN, advaNce Decision, and lEaRning system. Two decision theory approaches are used in the CPS strategy to identify attack traffic on the cloud for mitigating HX-DoS and SIPDAS traffic attacks. This is followed by a process like that of a standard intrusion detection system. It, therefore, has the capability of identifying and marking an attack message [65]. When a SIPDAS or HX-DoS attack message is detected, the message is marked with a single bit. The Reconstruct and Drop RAD algorithms delete these messages from the system.

3.3.3. *Machine learning based algorithm*

Implementing a machine learning-based authentication system may reduce spoofing threats in 5G networks. In [66], the authors developed an authentication system at the physical layer to increase the authentication rate. The authentication model is reinforced by adopting a two-dimensional characteristic for the one-dimensional approach since the two-dimensional method is more effective at identifying attackers. The presented classifier is capable of rapid authentication because it is trained offline.

3.3.4. *SDN-5G*

To make the network even more secure, the SDN-5G security architecture was developed [67]. A synchronized secret key is the foundation of this method. An encryption technique generates this key, which is subsequently saved in back-end systems and 5G devices. This secret key is required for the attacker to detect the communication prior to the communication phase. The network will be able to tell if an attack came from an IP spoofing attack since the secret key changes over time; the same is true of a man-in-the-middle (MITM) attack, in which an attacker takes over a device's connection during the process of authentication. Besides that, the attack will be discovered and prevented since the back-end system cannot update the secret key stored on the device. Regarding the replay attack, the possibility of this happening in a 5G network following this design is close to 0 percent since the secret key will change with each transmission, rendering the replayed message with an out-of-date key [68].

3.3.5. *Deep learning framework*

By using AI-based deep learning algorithms, jamming attacks are mitigated. In [69], the authors presented a system based on deep learning to be used in smart cities and to enhance jamming attacks. The proposed deep learning method utilizes a network of interconnected heterogeneous wireless devices to collect the necessary data. Discovering previously unseen network threats requires extensive use of unsupervised learning.

3.3.6. *NFV method*

Distributed virtualization significantly improves the security of the network; it also increases network flexibility and reliability and resolves many attack issues at multiple tiers of the 5G-based networks, including tapering, eavesdropping, and so on [70–72]. In [73], the author advocated using third-party monitoring programmes (PMAs) to identify network slice anomalies. Encrypted data transmission prevents tampering attacks during transmission.

3.3.7. *SDN-guard*

SDN is a ground-breaking architecture for centralized network management that divides the network. This enables the advancements in networking programmability to accommodate an increasing variety of applications [74]. SDN-guard is proposed as a method for resolving security-related issues and providing answers for protecting tactile internet applications utilizing fog systems against MITM and DoS attacks [72].

3.3.8. SDN-SC

It is an architecture for software-defined networks (SDN) that provides security for 5G networks. Which is applied to handle security challenges in 5G core networks; as a consequence, SDN's logically centralized intelligence, abstraction, and programmability provide major benefits for tackling mobile network security issues. Due to the programmability of this suggested architecture, it can meet many user's security requirements and deploy the service as quickly as feasible. Additionally, the design demonstrates its independence by allowing the security controller and network management to operate concurrently without interfering with one another or with the regular operation of the mobile network [67].

3.3.9. APG-BFT algorithm

It is a secure authentication technique that is utilized in 5G UDN, and it is based on blockchain technology. This method is mostly used to protect networks against Byzantine general attacks [75]. This technique allows for the creation of trustworthy chain access point groups using APs and the transmission of authentication results inside the APG using Blockchain message propagation. It can decrease authentication frequency and increase access efficiency.

3.3.10. Elliptic-ElGamal authentication scheme

Cryptography-based strategies may be used to protect against RBS-based attacks. In [71], the authors presented a lightweight authentication technique based on elliptic-ElGamal. Elliptic curve cryptography is used to choose a key pair, and the ElGamal method is the technique that makes it possible for the station and the user to exchange the secret key. The primary key with less number of messages decreases the risk of guess-based attacks. For devices with limited computational capabilities, the suggested solution is effective.

3.3.11. Deep Q-network learning

Artificial intelligence has the potential to introduce new security protocols to the network. The most notable is Reinforcement Learning, in which an (i.e., MEC edge node) monitors the security complexity of a network and then learns from that monitoring by employing a Deep Q-network learning algorithm [76,77].

4. Security solutions for 5G-based smart healthcare network

This section will cover numerous innovative technologies employed in 5G for smart healthcare. These technologies have been categorized into several groups. As a result, we will present a discussion on several subcategories of technical issues and emerging technologies associated with 5G security for smart healthcare.

4.1. Blockchain

The word "blockchain" refers to innovative and transformative technologies for 5G security in smart healthcare that enables decentralized, secure authentication, validation, recording, and management of information and identity among diverse parties [78]. It is considered a turning point for 5G-based smart healthcare networks. As a peer-to-peer, distributed storage platform for maintaining chains of linked blocks of transaction data, block-chain has several qualities that contribute to the security of the 5G-based smart healthcare network, including decentralization, distribution, and others [79]. Because it is a decentralized and dispersing technology, it can be utilized for various applications, including smart finance, intelligent transportation, supply chain management, and autonomous vehicles [80]. The economic value of data sharing might be greatly increased by combining 5G with blockchain technology. The strength of 5G coverage enabled by blockchain technology has lowered latency, increased speed, and capacity, allowing widespread adoption of IoT devices for smart healthcare [81]. Simultaneously, these devices may use security, decentralization, integrity, and consensus arbitration of blockchain technologies as a support layer. While blockchain technology may offer security and confidentiality, the bulk of IoT activities and agreements occur at the network layer, with the possibility of resolving the issues on the chain. The implementation of 5G will almost benefit block-chain technology since it will boost the involvement of nodes and decentralization, enable quicker block times, advance on-chain scalability, and enable the Internet of Things for smart healthcare [82]. The blockchain enables many parties to securely exchange, transmit, and data access. A distributed ledger in blockchain technology contains the necessary data disseminated to all participants. As a result, blockchain technology enhances the security of 5G-based networks. Blockchain offers a secure data access solution for a transportation application that enables the various systems relevant to bus transportation stakeholders to access a passenger's record data (e.g., patients in an ambulance). Centralization and scalability are also critical issues in 5G-based smart healthcare and IoT applications. In this situation, blockchain-based technologies provide a decentralized framework for securing privacy for numerous applications of IoT in 5G, such as smart healthcare. Blockchain technology enables a rapid security authentication technique for addressing APG trusted generation and security, as well as efficient access to the user equipment in a 5G UDN context [83]. Several UDN systems build a collaborative blockchain using blockchain technology and provide user equipment access to the APG, a collection of numerous APs. The clusters of APs are managed by the local service centre (LSC). UE utilizes Blockchain technology to provide safe and dependable access in a 5G context.

4.2. Artificial intelligence for 5G security

AI is a critical technology for 5G-based network security because that enables the management of a system capable of identifying abnormalities and predicting future situations. Algorithms based on machine learning and deep learning enable 5G networks to be proactive and predictive to deliver trustworthy, efficient services [84]. Algorithms based on artificial intelligence assist in realizing the different needs of 5G technology by working effectively to deliver high-quality of experience (QoE). Numerous fraudulent operations, including radio jamming attacks, MITM attacks, and other harmful actions, can be detected and discovered by studying current and previous patterns to avoid such attacks with the help of artificial intelligence in the future. Authentication is a critical component in securing 5G-enabled devices. In wireless communication, interception and spoofing methods are possible. Historically, authentication techniques depended on cryptographic processes, which resulted in significant delay and processing costs [85]. Additionally, these encryption techniques are not ideal for devices with little processing capability. Intelligent authentication powered by artificial intelligence offers the benefit of being situation-aware, extremely dependable, and cost-effective. In [86], suggested employing machine learning to authenticate physical-layer channels in 5G wireless communication. The authentication approach distinguished a legal user and a counterfeiter using double or single-dimensional joint characteristics. that the proposed machine learning-based solution detects spoofing attempts more frequently than physical layer-based authentication techniques. The authentication process is substantially quicker with data since the classifier is trained offline. In [87], authors compared an intelligent authentication strategy to a static authentication technique while investigating machine learning methods for 5G network authentication. The static authentication technique needed more processing resources and had a greater delay. In contrast, the AI-based authentication scheme had a lower rate of false positives and better authentication accuracy. By adopting access control, which restricts data access to authorized users and prevents access to unauthorized users, ensures data confidentiality. In [88], authors suggested using machine learning to secure secret communications delivered to users through the directional modulation transmitter. In [89], the authors suggested a unique approach for merging using a clone-resistant device identity with the user's biometric identification. Using keystroke dynamics and an accelerometer, a user's biometric identification is developed via machine learning. The cloning-immune identity is unaffected by the mobile service provider or the device maker. Combining the two identities results in a safe authentication system that protects the user's private connections from interception by the controlling trusted authority.

4.3. CPS for 5G security

Cyber-physical system (CPS) is an essential smart system for protecting 5G-based networks. Because of its ability to interact with both the network's physical and computational nodes. CPS technology is a security technique that aims to secure the whole cyber–physical environment uniformly. Sensors and actuators are often powered by batteries and have limited resources, making it impossible to apply computationally costly security methods [90]. It is a procedure that interacts with the physical world and conveys information across remote pieces in an edge/cloud environment through 5G [91]. It accomplishes network slice virtualization via the use of cyber–physical clouds. This cloud is equipped with a variety of sensors and actuators. 5G cloud services are provided by these virtual network components. Existing research in 5G-based networks faces several obstacles, including communication latency, enhanced resource requirements, and reliability. To address these issues, we can use the open-source solution Management and Orchestration (MANO), numerous industrial groups are already using it to improve the flexibility of 5G-based networks for CPS. It use of a hypervisor in combination with container-based virtualization techniques results in reduced resource needs, quick response times, and scalability over 5G networks. It meets 5G security and industrial characteristics, such as lightweight and secure processing, to achieve secure CPS activities (authentication, encryption, integrity). Sensitive CPS devices in a flexible network architecture need to gather log data relevant to security visibility in 5G-based networks. In 5G, CPS security must assure privacy, security, and scalability, the authenticity of sensor observations, and the maintenance of a plausible system state at all times. XML denial-of-service (HX-DoS) and HTTP attacks are associated with cloud-based CPS. The attacker in this technique forwards XML DoS and HTTP signals to the cloud through the 5G environment [92]. In [64], authors presented ENDER approaches in a cloud-enabled CPS context to counter this threat. It employs two decision theory approaches to identify cloud-based attack traffic and a strategy similar to that of a standard intrusion detection system. After then, it is capable of identifying and marking an attack message. When SIPDAS attacks or HX-DoS messages are detected, the message is added with the 1-bit mark. Such messages are removed from the system using the Reconstruct and Drop RAD algorithms.

4.4. Quantum cryptography for 5G security

Quantum computers are exponentially quicker than conventional computers in solving complicated mathematical problems [93]. Quantum computers and quantum-related information technologies are rapidly developing today, posing a challenge to the traditional public-key cryptography required to protect communication in 5G-based networks. For this purpose, before switching to the next network generation, the network must be protected from any potential quantum attacks. To protect the 5G-based networks against quantum attacks, it is necessary to use post-quantum cyphers. One of the conceivable and practical methods is lattice-based cryptography. In [94], the authors introduced the first use of Lattice systems in cryptography, in which they employed a random lattice chosen based on a specified distribution as a random key. Numerous applications use lattice-based encryption because it has been theoretically proven robust to quantum attacks. The lattice-based cryptosystem method, Nth degree truncated polynomial ring units (NTRU), is widely used for signature generation and encryption [95]. Quantum key distribution (QKD) is another viable approach resistant to quantum attacks. It is built on users exchanging cryptographic data [96]. Since 2016, QKD techniques have been used to protect over 350,000 customers of SK Telecom's LTE backhaul network, which connects Daejeon and Sejong in South Korea. The first quantum cryptography technology for 5G networks was unveiled by SK Telecom in 2018. Since there is no way to exclude the risk of a quantum attack in the future, post-quantum cyphers are an absolute necessity for 5G networks and beyond.

5. Open issues and future research directions

This article discussed vulnerabilities and security methods that may be used to avoid and overcome difficulties in 5G-based smart healthcare networks. AI and Blockchain are used to defend radio access and virtualization technologies such as SDN and NFV. Nonetheless, several security vulnerabilities remain in 5G-based networks. The following security flaws are following:

5.0.1. Authentication

Sensors come in several configurations, each needing its hardware and software, making it difficult to ensure that the system receives and transmits data to an authenticated sensor due to the absence of universal communication or design standards for the sensor. As a result, decreasing authentication restrictions may put patients in danger.

5.0.2. Confidentiality

Maintaining the confidentiality of health information remains challenging due to the weak points in wireless networks and the specialized technology used by sensors [97]. There is no uniform solution that works for all sorts of sensors, and even comprehensive systems, such as those featured in 5G networks, have drawbacks. Ensuring the privacy of healthcare providers and patients is critical, and when that confidentiality is violated, their safety may be affected.

5.0.3. Availability

Patients and examiners should always have access to previous and current data. Additionally, servers and sensors must never fail, and data must always be in the right format. These operational standards are likely unachievable with present technology and scientific knowledge. However, advancements in other domains, such as quantum computers or superconductors, can change the nature of this challenge.

5.0.4. Energy limitation

While some computing power is required for sensors, there are circumstances when using less energy is advantageous, such as embedded in the body sensor. Additionally, implanted sensors must have sufficient power to function for an extended period, ideally, the usual diagnostic length, since changing them is uncomfortable and costly. It is difficult to balance the energy required to run the sensor with the energy that a patient can tolerate, and this presumably varies by sensor type.

5.0.5. Computational and memory limitations

Because smart healthcare sensors are often tiny, their memory size and processing capability are likewise limited. Security algorithms for these sensors must operate with minimal memory while not interfering with the sensor's operation. Novel computational strategies are necessary since most security algorithms today are too complicated to perform consistently with limited resources.

5.0.6. Fault tolerance

Smart healthcare components should be capable of operating if a system component is down or fail. Backup sensors are one option, but they are not always feasible, and building fault tolerance into life-critical systems may save lives. Although this challenge is more concerned with how sensors work outside than within, a robust internal structure is still crucial.

5.0.7. Data freshness

Smart healthcare sensors must continually provide current data to healthcare practitioners. It is critical to verify the condition of system nodes frequently and to collect data from sensors. Calculating how far apart these intervals should provide difficulty since sending frequent requests for fresh information might make the network overburdened. On the other hand, failure to make frequent calls may endanger patients if sensors fail to convey a problematic state.

5.0.8. Authorization

An essential ongoing security risk is to take precautions to ensure that only authorized persons have access to the data related to a patient. There is a connection to the concept of information confidentiality, but it should be understood as a separate concept in its own right because confidentiality can be compromised even when only authorized personnel have access to information.

5.0.9. Non repudiation

It should not be difficult for two entities that have been properly authorized and have contracts to get data or validate their identities. While digital signatures are the modern technique for assuring data integrity, some sensor types lack the processing power or knowledge necessary to compute signatures.

5.0.10. Self-healing

Smart healthcare sensors should eventually be able to detect outages, connection failures, and hardware issues. Additionally, they should be capable of diagnosing and resolving such issues automatically. This is an open topic due to the large diversity of sensor technology and requirements. Because it calls for the development of new software and hardware technologies, it is one of the most challenging research topics in the field of smart healthcare.

5.0.11. Resiliency

Sensors and servers must fast recover from faults to reduce the time patients are not monitored. While testing sensors and servers are feasible, certain gear cannot incorporate backups due to their architecture, while others are unstable. It is a challenge to design durable sensors and servers independent of their physical shape.

5.0.12. Scalability

Smart healthcare networks must be able to expand or contract in response to patient requirements. New sensors should be able to easily integrate into an existing system without creating any complications, and modifications should not be performed that affect the integrity of the current system. Again, variations in sensor technology might make this challenging, and network traffic restrictions could make things even more difficult.

5.0.13. Mobility

Since many sensors in smart healthcare networks are designed to be connected to the body in some way, they are frequently quite mobile. This implies that the sensors may frequently enter and exit wireless networks, passing through places where transmissions may be interfered with, and have difficulty sending data if moved in a specific manner or separated from a patient. All of these options must be considered while developing sensor hardware or software.

5.0.14. Algorithms

Developing security algorithms for servers and sensors that are light and robust enough to function on very minimal computational resources is unquestionably the most significant open challenge [98]. Certain security techniques demand a considerable amount of memory, and the addition of encryption to the algorithm, which is necessary for smart healthcare, enhances the amount of memory required even more. Algorithms need new security principles since they are the most often attacked sector.

5.1. Future research directions

The analysis of the examined articles revealed many promising paths for future 5G-based smart healthcare research. While these recommendations benefit smart healthcare privacy and security, they may also benefit other growing applications.

5.1.1. Machine learning

Sensor data in a 5G-based smart healthcare network is frequently noisy, overlapping, and unstructured. Sensors also gather an enormous amount of data quickly, making it critical to separate the signal from the noise before decoding the data. Machine learning algorithms may be trained to understand sensor data and differentiate between vital information and noise that is delivered by the sensor. They may also reduce both the number of sensors required for data collection as well as the amount of data that medical professionals need to manually sort. However, since healthcare data is sensitive, it must be handled appropriately. In order to make ML models secure and privacy-preserving, one viable option is the merging of federated learning and edge computing. This might entail the creation of ML-based security solutions that can retain patient data privacy while learning from data gathered from various edge devices. Additionally, using explainable AI techniques could result in a more open and reliable security decision method.

5.1.2. Blockchain

The capacity of blockchain technology to connect records using cryptography can potentially change privacy and security in 5G-based smart healthcare allowing for safe and transparent data sharing between patients and healthcare professionals. To automate and streamline healthcare operations may entail creating blockchain-based identity and access management systems and integrating smart contracts and decentralized applications. However, integrating blockchain in 5G-based smart healthcare requires more computational energy, which may be challenging for resource-constrained devices. Therefore, the implementation of new consensus methods based on blockchain technology may accommodate constrained devices and offer a secure and decentralized method of network management and governance is required. Additionally, standardization initiatives and stakeholder engagements will be required to guarantee the scalability and interoperability of blockchain-based solutions in 5G networks for smart healthcare.

5.1.3. Trust management

Even though nodes in the network should trust one another, this is not always prudent since attackers might impersonate trustworthy nodes to get access to data. The ability of one node to trust another is referred to as “trust management”. Because the network’s nodes depend on one another to successfully process and transfer data, nodes must understand how to identify and respond appropriately if one or more are compromised. This may involve the development of AI-based algorithms for risk assessment and decision-making, as well as the use of ML techniques to detect and respond to security threats in real time.

5.1.4. Edge/Fog computing

For 5G- based smart healthcare, cloud computing is beneficial because it enables decentralized networks. However, edge/fog computing may be more suited to smart healthcare requirements. Edge/Fog computing solutions offer better control over data privacy and are less expensive than traditional cloud computing. Additionally, they are more robust to errors and reduced latency. In order to safeguard sensitive data and processes at the edge may entail integrating hardware-based security features like Trusted Execution Environments (TEEs). Additionally, by treating all devices and connections as untrusted until confirmed, the adoption of Zero Trust architectures may offer a more safe and more scalable solution to edge security.

5.1.5. Energy optimization

Because sensors have a limited amount of processing power, there is also a temporal limit placed on how long they can remain powerful to process and compute. Consumption of energy and production in smart healthcare is far from optimized. Therefore, developing algorithms and hardware that are both lightweight and efficient is a very essential and challenging task.

5.1.6. Protocol standardization

Communication is crucial in smart healthcare networks; it is necessary to balance content and speed. This is compounded by the fact that there are several protocols available for the various kinds of sensors. It will be possible for several distinct sensors to work together on the same network by standardizing the protocols necessary for communication among the various types of sensors. Additionally, Conventional protocols may also be modified to effectively carry data without overloading the network with unnecessary requests.

5.1.7. Smart gateways

Smart gateways provide a secure data entry point, hence improving verification and authorization. These gateways are resistant to routing attacks as well as other kinds of cyberattacks, such as denial-of-service attacks, that rely on data being supplied by users which is not allowed. Smart gateways may be able to aggregate data from several devices while also managing different elements of network routing and enhancing security [99].

6. Conclusion

Significant security threats and concerns faced by 5G-enabled smart healthcare systems. It is necessary to reduce these issues and threats to understand the security needs of such systems. Because smart healthcare devices have limited scalability, resource constraints, single-point-of-failure, high cost, and standard security techniques are unable to meet all of the security requirements of 5G-enabled smart healthcare. Many technologies such as Blockchain and Artificial intelligence have recently brought a new healthcare security and privacy era. This paper presents 5G smart healthcare architecture and key enabling technologies. This study looked at various technological features and services related to 5G smart healthcare security, including authentication, confidentiality availability, non-repudiation and integrity. We also discussed many security threats in 5G smart healthcare connectivity poses and available solutions. Finally, open issues and future research directions are presented for young researchers.

Declaration of competing interest

There are no conflicts of interest.

Data availability

No data was used for the research described in the article

Acknowledgments

This work is funded by FCT/MEC through national funds and, when applicable, co-funded by the FEDER-PT2020 partnership agreement under the project UIDB/50008/2020.

References

[1] Smit M, Brinkman K, Geerlings S, Smit C, Thyagarajan K, van Sighem A, de Wolf F, Hallett TB, et al. Future challenges for clinical care of an ageing population infected with HIV: a modelling study. Lancet Infect Dis 2015;15(7):810–8.

[2] Sen-Crowe B, Sutherland M, McKenney M, Elkbuli A. A closer look into global hospital beds capacity and resource shortages during the COVID-19 pandemic. J Surg Res 2021;260:56–63.

[3] Qadri YA, Nauman A, Zikria YB, Vasilakos AV, Kim SW. The future of healthcare internet of things: a survey of emerging technologies. IEEE Commun Surv Tutor 2020;22(2):1121–67.

[4] Harimoorthy K, Thangavelu M. Cloud-assisted Parkinson disease identification system for remote patient monitoring and diagnosis in the smart healthcare applications. Concurr Comput: Pract Exper 2021;e6419.

[5] Chen M, Yang J, Zhou J, Hao Y, Zhang J, Youn C-H. 5G-smart diabetes: Toward personalized diabetes diagnosis with healthcare big data clouds. IEEE Commun Mag 2018;56(4):16–23.

[6] Bartur G, Joubran K, Peleg-Shani S, Vatine J-J, Shahaf G. A pilot study on the electrophysiological monitoring of patient's engagement in post-stroke physical rehabilitation. Disabil Rehabil: Assist Technol 2020;15(4):471–9.

[7] Chen M, Li W, Hao Y, Qian Y, Humar I. Edge cognitive computing based smart healthcare system. Future Gener Comput Syst 2018;86:403–11.

[8] Hussain A, Wenbi R, da Silva AL, Nadher M, Mudhish M. Health and emergency-care platform for the elderly and disabled people in the Smart City. J Syst Softw 2015;110:253–63.

[9] Ahad A, Al Faisal S, Ali F, Jan B, Ullah N, et al. Design and performance analysis of DSS (dual sink based scheme) protocol for WBASNs. Adv Remote Sens 2017;6(04):245.

[10] Joyia GJ, Liaqat RM, Farooq A, Rehman S. Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. J Commun 2017;12(4):240–7.

[11] Banka S, Madan I, Saranya S. Smart healthcare monitoring using IoT. Int J Appl Eng Res 2018;13(15):11984–9.

[12] Baskar S, Shakeel PM, Kumar R, Burhanuddin M, Sampath R. A dynamic and interoperable communication framework for controlling the operations of wearable sensors in smart healthcare applications. Comput Commun 2020;149:17–26.

[13] Pashazadeh A, Navimipour NJ. Big data handling mechanisms in the healthcare applications: A comprehensive and systematic literature review. J Biomed Inform 2018;82:47–62.

[14] Li S, Da Xu L, Zhao S. 5G Internet of Things: A survey. J Ind Inf Integr 2018;10:1–9.

[15] Mateen A, Ahad A, Zia S, Shayea I, Ali S. Energy-efficient routing to prevent void holes in heterogeneous 5G wireless sensor network using game theory. In: 2023 international conference on smart computing and application. ICSCA, IEEE; 2023, p. 1–6.

[16] Gong H, Li R, Bai Y, An J, Li K. Message response time analysis for automotive cyber–physicalsystems with uncertain delay: An m/ph/1 queue approach. Perform Eval 2018;125:21–47.

[17] Khurpade JM, Rao D, Sanghavi PD. A survey on IOT and 5G network. In: 2018 international conference on smart city and emerging technology. ICSCET, IEEE; 2018, p. 1–3.

[18] Hu J, Liang W, Hosam O, Hsieh M-Y, Su X. 5GSS: a framework for 5G-secure-smart healthcare monitoring. Connect Sci 2021;1–23.

[19] Ahad A, Tahir M, Yau K-LA. 5G-based smart healthcare network: architecture, taxonomy, challenges and future research directions. IEEE Access 2019;7:100747–62.

[20] Dhanvijay MM, Patil SC. Internet of Things: A survey of enabling technologies in healthcare and its applications. Comput Netw 2019;153:113–31.

[21] Mahmoud MM, Rodrigues JJ, Ahmed SH, Shah SC, Al-Muhtadi JF, Korotaev VV, De Albuquerque VHC. Enabling technologies on cloud of things for smart healthcare. IEEE Access 2018;6:31950–67.

[22] Tariq N, Qamar A, Asim M, Khan FA. Blockchain and smart healthcare security: a survey. Procedia Comput Sci 2020;175:615–20.

[23] Qi J, Yang P, Min G, Amft O, Dong F, Xu L. Advanced internet of things for personalised healthcare systems: A survey. Pervasive Mob Comput 2017;41:132–49.

[24] Algarni A. A survey and classification of security and privacy research in smart healthcare systems. IEEE Access 2019;7:101879–94.

[25] Baker SB, Xiang W, Atkinson I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. IEEE Access 2017;5:26521–44.

[26] Ahad A, Tahir M, Aman Sheikh M, Ahmed KI, Mughees A, Numani A. Technologies trend towards 5G network for smart health-care using IoT: A review. Sensors 2020;20(14):4047.

[27] Zhang Q, Liu J, Zhao G. Towards 5G enabled tactile robotic telesurgery. 2018, arXiv preprint arXiv:1803.03586.

[28] Chochliouros IP, Kostopoulos A, Giannoulakis I, Spiliopoulou AS, Belesioti M, Sfakianakis E, Kourtis A, Kafetzakis E. Using small cells for enhancing 5G network facilities. In: 2017 IEEE conference on network function virtualization and software defined networks (NFV-SDN). IEEE; 2017, p. 264–9.

[29] Mughees A, Tahir M, Sheikh MA, Ahad A. Towards energy efficient 5g networks using machine learning: Taxonomy, research challenges, and future research directions. IEEE Access 2020;8:187498–522.

[30] Michalopoulos DS, Viering I, Du L. User-plane multi-connectivity aspects in 5G. In: 2016 23rd international conference on telecommunications. ICT, IEEE; 2016, p. 1–5.

[31] Mughees A, Tahir M, Sheikh MA, Ahad A. Energy-efficient ultra-dense 5G networks: Recent advances, taxonomy and future research directions. IEEE Access 2021.

[32] Shaikh FS, Wismüller R. Routing in multi-hop cellular device-to-device (D2D) networks: A survey. IEEE Commun Surv Tutor 2018;20(4):2622–57.

[33] Noura M, Nordin R. A survey on interference management for device-to-device (D2D) communication and its challenges in 5G networks. J Netw Comput Appl 2016;71:130–50.

[34] Alkurd R, Shubair RM, Abualhaol I. Survey on device-to-device communications: Challenges and design issues. In: 2014 IEEE 12th international new circuits and systems conference. NEWCAS, IEEE; 2014, p. 361–4.

[35] Kumar A, Albreem MA, Gupta M, Alsharif MH, Kim S. Future 5G network based smart hospitals: Hybrid detection technique for latency improvement. IEEE Access 2020;8:153240–9.

[36] Huang Y, Li Y, Ren H, Lu J, Zhang W. Multi-panel MIMO in 5G. IEEE Commun Mag 2018;56(3):56–61.

[37] Bannour F, Souihi S, Mellouk A. Distributed SDN control: Survey, taxonomy, and challenges. IEEE Commun Surv Tutor 2017;20(1):333–54.

[38] Benzekki K, El Fergougui A, Elbelrhiti Elalaoui A. Software-defined networking (SDN): a survey. Secur Commun Netw 2016;9(18):5803–33.

[39] Akbar A, Jangsher S, Bhatti FA. NOMA and 5G emerging technologies: A survey on issues and solution techniques. Comput Netw 2021;190:107950.

[40] Islam SR, Avazov N, Dobre OA, Kwak K-S. Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges. IEEE Commun Surv Tutor 2016;19(2):721–42.

[41] Yousaf FZ, Bredel M, Schaller S, Schneider F. NFV and SDN—Key technology enablers for 5G networks. IEEE J Sel Areas Commun 2017;35(11):2468–78.

[42] Niu Y, Li Y, Jin D, Su L, Vasilakos AV. A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges. Wirel Netw 2015;21(8):2657–76.

[43] Niu Y, Gao C, Li Y, Su L, Jin D, Zhu Y, Wu DO. Energy-efficient scheduling for mmWave backhauling of small cells in heterogeneous cellular networks. IEEE Trans Veh Technol 2016;66(3):2674–87.

[44] Hassan N, Yau K-LA, Wu C. Edge computing in 5G: A review. IEEE Access 2019;7:127276–89.

[45] Kumari A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Rodrigues JJ. Fog computing for smart grid systems in the 5G environment: Challenges and solutions. IEEE Wirel Commun 2019;26(3):47–53.

[46] Sicato JCS, Singh SK, Rathore S, Park JH. A comprehensive analyses of intrusion detection system for IoT environment. J Inf Process Syst 2020;16(4):975–90.

[47] Ahad A, Tahir M, Sheikh MAS, Hassan N, Ahmed KI, Mughees A. A game theory based clustering scheme (GCS) for 5G-based smart healthcare. In: 2020 IEEE 5th international symposium on telecommunication technologies. ISTT, IEEE; 2020, p. 157–61.

[48] Peng F, Guo R-S, Li C-T, Long M. A semi-fragile watermarking algorithm for authenticating 2D CAD engineering graphics based on log-polar transformation. Comput Aided Des 2010;42(12):1207–16.

[49] Jiang R, Lai C, Luo J, Wang X, Wang H. EAP-based group authentication and key agreement protocol for machine-type communications. Int J Distrib Sens Netw 2013;9(11):304601.

[50] Huang C, Cao J. Almost sure exponential stability of stochastic cellular neural networks with unbounded distributed delays. Neurocomputing 2009;72(13–15):3352–6.

[51] Huang C, Cao J, Cao J. Stability analysis of switched cellular neural networks: A mode-dependent average dwell time approach. Neural Netw 2016;82:84–99.

[52] Istiaque Ahmed K, Tahir M, Hadi Habaebi M, Lun Lau S, Ahad A. Machine learning for authentication and authorization in IoT: Taxonomy, challenges and future research direction. Sensors 2021;21(15):5122.

[53] Park JH, Rathore S, Singh SK, Salim MM, Azzaoui AE, Kim TW, Pan Y, Park JH. A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions. Hum-Centric Comput Inf Sci 2021;11(3).

[54] Kumarl CR, Jayanthi V. A novel fuzzy rough sets theory based CF recommendation system. Comput Syst Sci Eng 2019;34(3):123–9.

[55] Xiong B, Yang K, Zhao J, Li K. Robust dynamic network traffic partitioning against malicious attacks. J Netw Comput Appl 2017;87:20–31.

[56] Chen H-C, Kuo S-S. Active detecting DDOS attack approach based on entropy measurement for the next generation instant messaging app on smartphones. Intell Autom Soft Comput 2019;25(1):217–28.

[57] Jamel AA, Akay B. A survey and systematic categorization of parallel K-means and Fuzzy-c-Means algorithms. Comput Syst Sci Eng 2019;34(5):259–81.

[58] Gu K, Wang Y, Wen S. Traceable threshold proxy signature. J Inf Sci Eng 2017;33(1).

[59] SIP-based DoS attack simulator: SIP-DAS. 2017, Available: https://malware.news/t/sip-based-dos-attack-simulator-sip-das/12413, Online.

[60] Ficco M, Rak M. Stealthy denial of service strategy in cloud computing. IEEE Trans Cloud Comput 2014;3(1):80–94.

[61] Akinyoade AJ, Eluwole OT. The internet of things: Definition, tactile-oriented vision, challenges and future research directions. In: Third international congress on information and communication technology. Springer; 2019, p. 639–53.

[62] Xiao L, Xie C, Chen T, Dai H, Poor HV. A mobile offloading game against smart attacks. IEEE Access 2016;4:2281–91.

[63] Mistry I, Tanwar S, Tyagi S, Kumar N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mech Syst Signal Process 2020;135:106382.

[64] Ahmad I, Shahabuddin S, Kumar T, Okwuibe J, Gurtov A, Ylianttila M. Security for 5G and beyond. IEEE Commun Surv Tutor 2019;21(4):3682–722.

[65] Konstantopoulos G. Understanding blockchain fundamentals, part 1: Byzantine fault tolerance. 2017.

[66] Chen S, Wen H, Wu J, Chen J, Liu W, Hu L, Chen Y. Physical-layer channel authentication for 5G via machine learning algorithm. Wirel Commun Mob Comput 2018;2018.

[67] Liang X, Qiu X. A software defined security architecture for SDN-based 5G network. In: 2016 IEEE international conference on network infrastructure and digital content (IC-NIDC). IEEE; 2016, p. 17–21.

[68] Yao J, Han Z, Sohail M, Wang L. A robust security architecture for SDN-based 5G networks. Future Internet 2019;11(4):85.

[69] Singh SK, Jeong Y-S, Park JH. A deep learning-based IoT-oriented infrastructure for secure smart city. Sustainable Cities Soc 2020;60:102252.

[70] Li C, Qin Z, Novak E, Li Q. Securing SDN infrastructure of IoT–fog networks from MitM attacks. IEEE Internet Things J 2017;4(5):1156–64.

[71] Abro A, Deng Z, Memon KA. A lightweight elliptic-Elgamal-based authentication scheme for secure device-to-device communication. Future Internet 2019;11(5):108.

[72] Dridi L, Zhani MF. SDN-guard: DoS attacks mitigation in SDN networks. In: 2016 5th IEEE international conference on cloud networking (Cloudnet). IEEE; 2016, p. 212–7.

[73] Porambage P, Miche Y, Kalliola A, Liyanage M, Ylianttila M. Secure keying scheme for network slicing in 5G architecture. In: 2019 IEEE conference on standards for communications and networking. CSCN, IEEE; 2019, p. 1–6.

[74] Duan X, Wang X. Authentication handover and privacy protection in 5G hetnets using software-defined networking. IEEE Commun Mag 2015;53(4):28–35.

[75] Kofahi NA, Al-Rabadi AR. Identifying the top threats in cloud computing and its suggested solutions: a survey. Adv Netw 2018;6(1):1–13.

[76] Ahad A, Tahir M, Sheikh MAS, Mughees A, Ahmed KI. Optimal route selection in 5G-based smart health-care network: A reinforcement learning approach. In: 2021 26th IEEE Asia-Pacific conference on communications. APCC, IEEE; 2021, p. 248–53.

[77] Xiao L, Wan X, Dai C, Du X, Chen X, Guizani M. Security in mobile edge caching with reinforcement learning. IEEE Wirel Commun 2018;25(3):116–22.

[78] Cha J, Singh SK, Pan Y, Park JH. Blockchain-based cyber threat intelligence system architecture for sustainable computing. Sustainability 2020;12(16):6401.

[79] Tahir M, Habaebi MH, Dabbagh M, Mughees A, Ahad A, Ahmed KI. A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities. IEEE Access 2020;8:115876–904.

[80] Mamun Q. Blockchain technology in the future of healthcare. Smart Health 2022;23:100223.

[81] Almalki J, Al Shehri W, Mehmood R, Alsaif K, Alshahrani SM, Jannah N, Khan NA. Enabling blockchain with IoMT devices for healthcare. Information 2022;13(10):448.

[82] Jain G, Jain A. Blockchain for 5G-enabled networks in healthcare service based on several aspects. In: Blockchain applications for healthcare informatics. Elsevier; 2022, p. 471–93.

[83] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5G and beyond networks: A state of the art survey. J Netw Comput Appl 2020;166:102693.

[84] Haider N, Baig MZ, Imran M. Artificial intelligence and machine learning in 5G network security: Opportunities, advantages, and future research trends. 2020, arXiv preprint arXiv:2007.04490.

[85] Shen M, Lu H, Wang F, Liu H, Zhu L. Secure and efficient blockchain-assisted authentication for edge-integrated internet-of-vehicles. IEEE Trans Veh Technol 2022.

[86] Enad EH, Younis S. Machine learning based decision stratigies for physical layer authentication in wireless systems. In: 2020 2nd annual international conference on information and sciences (AiCIS). IEEE; 2020, p. 114–8.

[87] Fang H, Wang X, Tomasin S. Machine learning for intelligent authentication in 5G and beyond wireless networks. IEEE Wirel Commun 2019;26(5):55–61.

[88] Shu F, Qin Y, Chen R, Xu L, Shen T, Wan S, Jin S, Wang J, You X. Directional modulation: A secure solution to 5G and beyond mobile networks. 2018, arXiv preprint arXiv:1803.09938.

[89] Mars A, Abadleh A, Adi W. Operator and manufacturer independent D2D private link for future 5g networks. In: IEEE INFOCOM 2019-IEEE conference on computer communications workshops (INFOCOM WKSHPS). IEEE; 2019, p. 1–6.

[90] Dai Y, Xu D, Maharjan S, Chen Z, He Q, Zhang Y. Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE Netw 2019;33(3):10–7.

[91] Kim J, Jo G, Jeong J. A novel cpps architecture integrated with centralized opc ua server for 5g-based smart manufacturing. Procedia Comput Sci 2019;155:113–20.

[92] Zhang S, Lin Y, Liu Q, Jiang J, Yin B, Choo K-KR. Secure hitch in location based social networks. Comput Commun 2017;100:65–77.

[93] Gill SS, Kumar A, Singh H, Singh M, Kaur K, Usman M, Buyya R. Quantum computing: A taxonomy, systematic review and future directions. Softw - Pract Exp 2022;52(1):66–114.

[94] Ajtai M. Representing hard lattices with O (n log n) bits. In: Proceedings of the thirty-seventh annual ACM symposium on theory of computing. 2005, p. 94–103.

[95] Clancy TC, McGwier RW, Chen L. Post-quantum cryptography and 5G security: tutorial. In: Proceedings of the 12th conference on security and privacy in wireless and mobile networks. 2019, p. 285.

[96] Azzaoui AE, Park JH. Post-quantum blockchain for a scalable smart city. J Internet Technol 2020;21(4):1171–8.

[97] Ahad A, Ullah Z, Amin B, Ahmad A. Comparison of energy efficient routing protocols in wireless sensor network. Am J Netw Commun 2017;6:67–73.

[98] Ahad A, Tahir M. Perspective—6G and IoT for intelligent healthcare: Challenges and future research directions. ECS Sensors Plus 2022.

[99] Ahad A, Tahir M, Sheikh MA, Ahmed KI, Mughees A. An intelligent clustering-based routing protocol (CRP-GR) for 5G-based smart healthcare using game theory and reinforcement learning. Appl Sci 2021;11(21):9993.