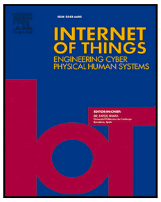
Internet of Things 20 (2022) 100610

Contents lists available at ScienceDirect

Internet of Things

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



Review article

Intelligent authentication of 5G healthcare devices: A survey

Ali Hassan Sodhro [a,b], Ali Ismail Awad [c,d,e,f,*], Jaap van de Beek [d], George Nikolakopoulos [d]

[a] Department of Computer Science, Kristianstad University, SE-29188 Kristianstad, Sweden
[b] Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, 518000 Shenzhen, China
[c] College of Information Technology, United Arab Emirates University, Al Ain P.O. Box 17551, United Arab Emirates
[d] Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 97187 Luleå, Sweden
[e] Faculty of Engineering, Al-Azhar University, Qena P.O. Box 83513, Egypt
[f] Centre for Security, Communications and Network Research, University of Plymouth, Plymouth PL4 8AA, UK

ARTICLE INFO

Keywords:
Internet of Things (IoT)
Internet of Things security
Device authentication
Artificial intelligence
Healthcare security
5G networks

ABSTRACT

The dynamic nature of wireless links and the mobility of devices connected to the Internet of Things (IoT) over fifth-generation (5G) networks (IoT-5G), on the one hand, empowers pervasive healthcare applications. On the other hand, it allows eavesdroppers and other illegitimate actors to access secret information. Due to the poor time efficiency and high computational complexity of conventional cryptographic methods and the heterogeneous technologies used, it is easy to compromise the authentication of lightweight wearable and healthcare devices. Therefore, intelligent authentication, which relies on artificial intelligence (AI), and sufficient network resources are extremely important for securing healthcare devices connected to IoT-5G. This survey considers intelligent authentication and includes a comprehensive overview of intelligent authentication mechanisms for securing IoT-5G devices deployed in the healthcare domain. First, it presents a detailed, thoughtful, and state-of-the-art review of IoT-5G, healthcare technologies, tools, applications, research trends, challenges, opportunities, and solutions. We selected 20 technical articles from those surveyed based on their strong overlaps with IoT, 5G, healthcare, device authentication, and AI. Second, IoT-5G device authentication, radio-frequency fingerprinting, and mutual authentication are reviewed, characterized, clustered, and classified. Third, the review envisions that AI can be used to integrate the attributes of the physical layer and 5G networks to empower intelligent healthcare devices. Moreover, methods for developing intelligent authentication models using AI are presented. Finally, the future outlook and recommendations are introduced for IoT-5G healthcare applications, and recommendations for further research are presented as well. The remarkable contributions and relevance of this survey may assist the research community in understanding the research gaps and the research opportunities relating to the intelligent authentication of IoT-5G healthcare devices.

1. Introduction

The Internet of Things (IoT) is a dynamic, adaptive, computationally complex, and ad hoc framework for connecting and integrating anything, anyone, and any service at anytime and anywhere [1,2]. The use of the IoT in healthcare is growing. For example, there was a huge investment of about 117 billion US dollars in 2020 [3]. The IoT is a major evolutionary change, as

---

* Corresponding author at: College of Information Technology, United Arab Emirates University, Al Ain P.O. Box 17551, United Arab Emirates.
E-mail address: ali.awad@uaeu.ac.ae (A.I. Awad).

https://doi.org/10.1016/j.iot.2022.100610
Received 30 June 2022; Received in revised form 31 August 2022; Accepted 31 August 2022

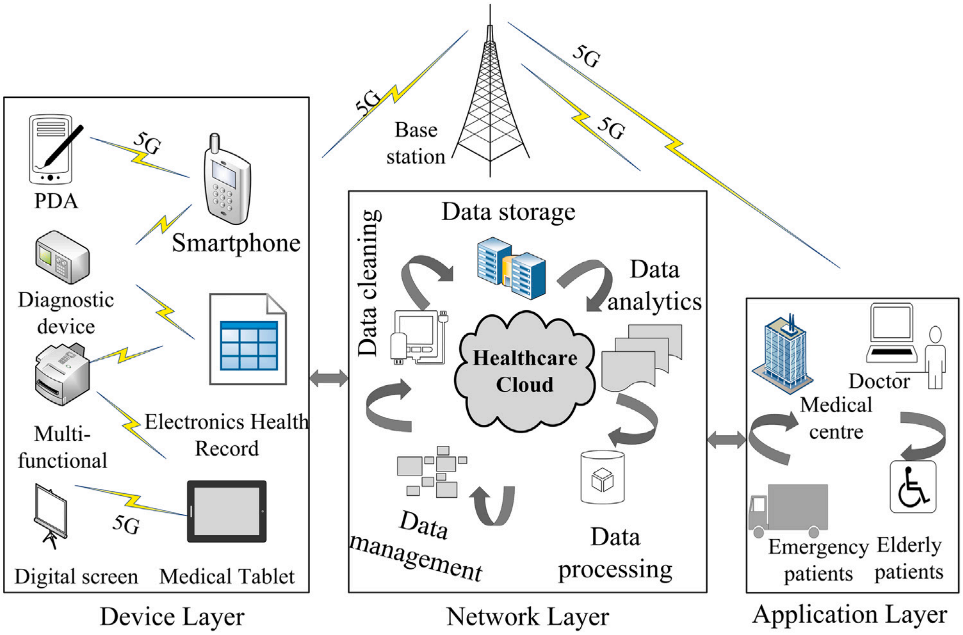


Fig. 1. Proposed IoT-5G framework for healthcare: It is based on the device layer, network layer and application layer, there is a strong interlink between three layer for efficient and sustainable connectivity.

it accommodates the needs of current medical trends and practices. A large number of healthcare applications, such as remote eldercare and assisted living, are being remarkably fueled by IoT-enabled wearable devices due to their enormous potential and integration possibilities [4–6].

IoT-enabled wearable devices, for instance, smart watches, smart glasses, smart belts, and smart rings, have entirely reshaped traditional healthcare practices, making them ubiquitous and pervasive. Furthermore, the adoption of both short- and long-range networks, such as body sensor networks, Bluetooth, ZigBee, Wi-Fi, wireless local area networks, and extensive area networks, will fundamentally revolutionize medical care by providing the required communication framework. Most wearable devices intelligently gather health-related information from sensors, actuators, and biomedical systems, which can be used for diagnosing, treating, and preventing disease [7,8]. For example, the authors in [9,10] address several healthcare applications from assisted living, telecare, and remote consultations to the monitoring of elderly and emergency patients through IoT-enabled wearable devices.

The newly deployed fifth-generation (5G) networks are key for integrating heterogeneous platforms together and fulfilling the needs of future IoT-enabled services and applications. Besides, 5G radio technologies are continually being developed and have a huge potential for building strong ties to the IoT, which has a central role due to the strong and rapid progress in lightweight wearable devices [11]. These technological trends are fostering and empowering the integration and synthesis of heterogeneous systems through device-to-device (D2D) communications via the IoT [12]. The strong ties between the IoT and 5G are powering and promoting the scope and vitality of future healthcare applications.

Despite the numerous benefits, there are some critical challenges for IoT in healthcare applications, for example, realizing better and insightful content extraction from the large and voluminous amounts of data from devices and maintaining high security, particularly authentication, for resource-constrained devices during the exchange of private and sensitive information between intended agents (i.e., patients, physicians, and healthcare facilities) [13].

IoT-enabled 5G (IoT-5G) devices can cooperate and communicate with high efficiency and with less interference without the involvement of base stations (BSs) or access points due to their unique and intelligent features and compatibility [14,15], as shown in Fig. 1. Authentication is one of the critical challenges for IoT-5G devices for healthcare applications. The large number of IoT devices led to ultra-densification by 2020 (i.e., there were about 106 connections per km^2). Due to the resource limitations, high mobility, and dynamic wireless links in IoT-5G, connected devices are the main cause of weaker authentication and identity management (IdM), and hence, there is a higher risk of eavesdropping attacks [16]. Therefore, security designers must consider both the access technologies and network deployment scenarios when designing intelligent authentication models, frameworks, and methods for IoT-5G healthcare devices.

Authentication mechanisms relying on artificial intelligence (AI) will become of paramount importance in IoT-5G healthcare devices because they can more effectively use resources, such as energy and battery power, of resource-constrained wearable devices. Furthermore, 5G integrates and supports millions of devices with inadequate built-in security plus various new devices. The high computing power of these devices makes them an easy target for attackers and hackers. Thus, device authentication in IoT-5G has recently received increasing interest for healthcare applications.

Joint IoT-5G platforms have become more popular in various fields. For instance, smart healthcare facilities, smart cities, and smart homes are remotely operating and accessing network devices. Offering consultations and monitoring elderly patients to collect data about their daily routines in rural areas is one example. Thus, it is important to develop an intelligent authentication mechanism that can block illegitimate or unauthorized users. Authentication via biometrics is appropriate in smart medical homes and hospitals in remote locations [17,18].

Authentication based on elliptic curve cryptography (ECC) uses short keys, making it appropriate for IoT devices, unlike Rivest–Shamir–Adleman (RSA) [19]. Small resource-constrained IoT devices cannot handle the computational complexity of some cryptosystems, thus increasing the vulnerability of interconnected entities. The highly scalable nature of joint IoT and 5G platforms, on the one hand, enables diverse vertical applications by connecting heterogeneous devices. On the other hand, the risk of various spoofing attacks is increased. The traditional authentication methods in the physical layer (PHY) are not able to provide good enough authentication because the networks are computationally complex and heterogeneous. Thus, due to the significant security overhead, low reliability, lack of efficient and precise authentication models, and limited availability of information in time-varying techniques, it is necessary to find more efficient and intelligent authentication methods [20,21].

The key aim of this survey is to provide detailed insights into cutting-edge technologies like AI, IoT, 5G, and D2D communications for the devices that are the building blocks of authenticated healthcare applications. Another goal is to describe the authentication mechanisms in IoT-5G healthcare devices. Densely deployed IoT devices, including low-cost sensors, actuators, and smart objects, should exchange data securely and intelligently with minimal human intervention. Given the importance of IoT device security, particularly authentication, in healthcare, robust authentication is essential before allowing any IoT device to connect. From the security perspective, this review presents comprehensive details on the core and enabling technologies used to build device authentication systems for IoT-5G healthcare applications. Additionally, this paper provides details of related standards of core IoT-5G technologies published by different standardization bodies as well as a brief overview of intelligent authentication of devices by healthcare applications.

1.1. Research motivations

Healthcare is being dramatically transformed from a conventional fixed physician-focused method to a dynamic and distributed patient-oriented strategy. The proliferation of several emerging technologies, for instance, IoT and 5G, is driving this rapid revolution of healthcare verticals by providing personalized and remote medical services efficiently and accurately [14]. Most traditional medical platforms are connected to a 4G network. However, the communication processes are static, computationally complex, and less secure. To cope with the emerging healthcare trends, conventional networks will face stricter requirements in terms of data rate, speed, and latency [15,16].

As the healthcare market matures, the connectivity requirements for numerous IoT devices in hospitals will promote the deployment of massive machine type communication (mMTC). Besides, other critical applications, for instance, remote surgery, will need ultra-reliable low-latency communications (URLLC) or critical machine type communication, which are possible through 5G [18,22]. Wearable IoT-5G devices require lightweight security while high-speed and critical applications and services need strong security and proper authentication. The traditional network-enabled hop-by-hop security method is inappropriate for protecting different devices in healthcare applications [19].

The adoption of portable devices is a prominent and radical shift for the healthcare sector, requiring huge future investments and implementation plans. However, it is difficult for these tiny resource-hungry devices to run the conventional cryptographic protocols while accessing the end user's confidential information. Several researchers have suggested that to improve authentication in healthcare, it is imperative to minimize the authentication overhead for small IoT devices. As noted above, ECC has short keys, making it suitable for some IoT devices, unlike RSA [20]. However, ECC is computationally complex for joint IoT-5G devices. Small resource-constrained IoT devices that cannot handle the computational complexity of ECC will have security vulnerabilities.

Security is one of the major challenges in healthcare due to threats and their high ramification during the exchange of confidential and sensitive information among intended entities. For instance, all the private content is transferred to all the layers in the healthcare stack by the integration of core, scalable, and heterogeneous technologies with 5G [23]. Malicious IoT-5G wearable devices not only can impact security but can also thwart the entire provision of healthcare services. Both the risks and the number of attacks have been increasing everywhere over the last few years, so that the detection or prevention of impairment is a big challenge for healthcare applications [24,25].

This survey article aims to provide an overview of the cutting-edge technologies (e.g., IoT, D2D communication, AI, smart healthcare, authentication at the device layer, and so on) that are the main building blocks of 5G-enabled healthcare applications. Another aim is to understand the security, especially authentication, from the viewpoint of the device layer in IoT and D2D communications, etc. Thus, we focus mainly on the contributions from both academia and industry on security, i.e., authentication in the device layer for 5G-enabled healthcare applications [26].

1.2. Our contributions

Due to the criticality of IoT and 5G security deployed in different applications, several review articles have been published. For example, the authors in [23,24] both reviewed PHY security for 5G and D2D communications, but IoT and healthcare were not covered. The authors in [18] surveyed end-to-end simulations of 5G mmWave networks, but the application domains were not considered. The authors of Ref. [29] considered IoT authentication schemes but neither 5G nor healthcare applications. Recently, in

Table 1
Existing related survey and tutorial articles with the main focuses highlighted.

Year	Reference	Focus	Covered network layers			Other technologies			
			Network	Application	Physical	5G	Healthcare	IoT	Security
2018	[14,15]	PHY layer security for 5G and D2D communication	✓		✓	✓			✓
2018	[17]	Intrusion detection systems for IoT-based environments	✓		✓			✓	✓
2018	[18]	5G mmWave device authentication	✓		✓	✓		✓	✓
2019	[19]	Low latency communication in 5G	✓		✓	✓			
2019	[20,21]	DL for intelligent networks, 5G channel models	✓		✓		✓		
2019	[27,28]	Authentication and mMTC for IoT networks						✓	✓
2019	[29]	Internet of Things authentication schemes	✓		✓			✓	✓
2020	[30,31]	Survey on 5G traffic models, ML for IoT security	✓	✓	✓				✓
2020	[32,33]	5G for E2E networks, SDN for IoT services							✓
2020	[34,35]	DL for IoT, Blockchain for cloud computing						✓	
2020	[36,37]	PHY security, FL for edge networks	✓		✓			✓	✓
2020	[38]	Challenges of wearable devices in 5G networks	✓	✓		✓	✓		
2020	[39]	Overview on security and privacy for 5G in IoT era	✓		✓	✓		✓	
2021	[40]	Authentication and Identity Management of IoHT Devices					✓	✓	✓
2021	[41]	Federated learning for Internet of Things					✓	✓	✓
Our survey		Intelligent authentication of 5G healthcare devices	✓	✓	✓	✓	✓	✓	✓

2021, a review [40] focused on authentication for an Internet of healthcare things (IoHT). However, IoT applications, the network layer, and 5G technology were not covered. Table 1 compares the scope of this survey to previously published surveys.

Although other survey articles have been published on IoT, 5G, and security, none of the articles fully covered the four pillars of this paper: technologies (e.g., IoT-5G), tools (e.g., AI), applications (e.g., healthcare), and challenges (e.g., authentication). This review is unique because it discusses these four pillars and the three IoT layers. Furthermore, this comprehensive survey identifies 20 technical articles, as listed in Table 2. These 20 articles are golden research on the triad of IoT, 5G, and healthcare and IoT device authentication.

Our main contribution is an extensive review on intelligent authentication for IoT-5G healthcare devices. We believe that this is a new, emerging, interesting, and demanding research direction. The main aspects of this review are as follows:

- We present a taxonomy for IoT-5G healthcare, covering communications technologies, requirements, objectives, and performance measures. This taxonomy is mentioned throughout the paper and summarized in Section 3.
- We review authentication mechanisms for devices, sensors, and the physical-layer, as well as radio-frequency (RF) fingerprinting. Mutual-authentication techniques are presented, characterized, clustered, and classified. In addition, we provide comprehensive details on the core and enabling technologies for building an IoT-5G device authentication model for healthcare applications. These points are covered in Sections 4 and 2.2.
- We envision that AI can be used to integrate the features of the physical layer with IoT-5G healthcare devices for the authentication model. In short, the intelligent authentication of IoT-5G healthcare devices is the initial step in connecting pervasive and heterogeneous technologies. These topics are distributed over Sections Section 2, 3, and 4.

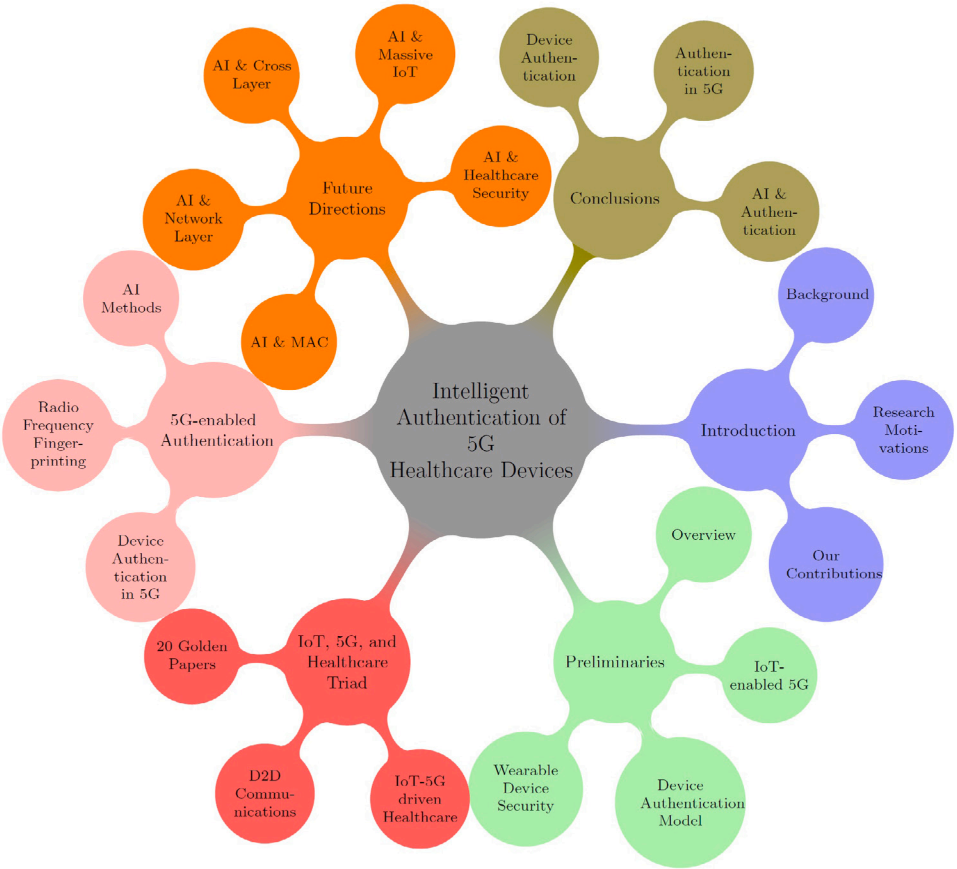


Fig. 2. Mind map demonstrating the structure, the key sections, and the concepts covered in this survey.

- We selected 20 golden relevant technical articles from all those surveyed based on their strong overlaps with IoT-5G, healthcare, authentication, and AI. We categorized and clustered based on applications and needs, the field of research, contributions, and limitations. They are represented by a Venn diagram. Finally, this subject is covered in Section 3.2.

The rest of the article is structured as follows. Section 2 presents preliminary information about the scope of the survey with a focus on the taxonomy of IoT-5G healthcare and the device authentication model. Section 3 reviews in detail the IoT, 5G, and healthcare triad. The section targets the four pillars of technologies, tools, applications, and challenges. Some broad and useful insights into the role of AI in device authentication are given in Section 4. Section 5 discusses in detail future research directions for the application of AI across the different IoT layers. Finally, the paper is concluded in Section 6. A mind map illustrates the structure of the paper, its key sections, and the main concepts covered (Fig. 2).

2. Preliminaries

This section presents necessary background information about the research scope with a focus on the taxonomy of IoT-5G healthcare and device authentication models.

2.1. Overview and scope

According to several research surveys, healthcare has a remarkable effect in boosting the economy. For instance, an analysis of the European Union found that aggregate savings from the implementation of smart healthcare were about 10% of its gross domestic product. The savings were 99 billion euros in 2020 [42]. Wearable IoT devices and wireless mobile networks are the key enablers of smart healthcare, as has been highlighted by many researchers. There is an increasing trend to adopt joint 5G and IoT-enabled portable devices. Smartphones and personal digital assistants can be used to diagnose and monitor chronic diseases. For example, severely ill diabetic patients can easily be examined and monitored 24/7 at an affordable cost through portable smartphones connected to a joint 5G and IoT platform [43].

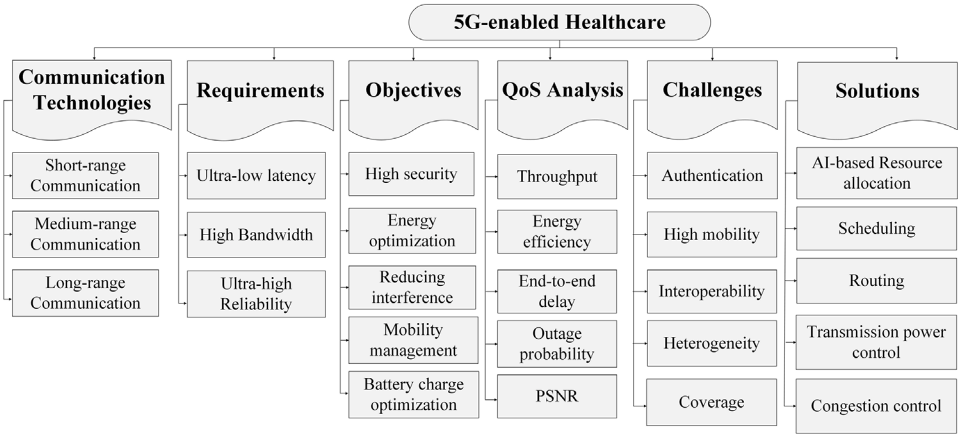


Fig. 3. Taxonomy of IoT-5G driven Healthcare: key indicators such as communication technologies, requirements, objectives, QoS analysis, challenges, and solutions are discussed in detail. In addition, from top to bottom, objectives and challenges columns are classified with respective solutions in the solutions column.

The use of 5G and IoT by the healthcare sector is an evolutionary step in delivering smart, ubiquitous, and cost-effective services anywhere at anytime. The reliable and better interconnections between IoT devices and 5G makes the provision of healthcare easier, more cost-effective, and more comfortable. Besides, combining various heterogeneous technologies, i.e., mobile networks, wearable devices, and intelligent resource allocation, is reshaping medical treatment, because better services can be delivered securely to remote locations.

Ensuring the security of IoT-enabled wearable devices while transmitting sensitive, confidential, and private content over 5G networks is important for healthcare applications. Because of their heterogeneous technologies, their innovative workflows, their dynamic wireless channels, and their mobility, sensor-based portable devices are easy targets for eavesdroppers and unauthorized entities, who may gain access to critical health information. Unauthorized modification of the data may lead to misinterpretation [44,45]. Thus, it is vital to develop novel AI-based intelligent and adaptive authentication strategies to identify and authorize legitimate users. AI-enabled security methods can wisely guide users by providing access to devices without human intervention. The combination of IoT, 5G, and AI is a remarkable and sustainable trend that could achieve intelligent authentication for 5G healthcare devices.

Fig. 3 presents a complete taxonomy of IoT-5G healthcare. Communication technologies include short-range, medium-range, and long-range communications. The necessary and basic requirements for IoT-5G healthcare applications are ultra-low latency, high bandwidth, and ultra-high reliability. The key objectives for emerging IoT-5G healthcare are high security, energy optimization, reduced interference, mobility management, and battery charge optimization. Quality of service (QoS) depends on throughput, energy efficiency, end-to-end delays, outage probabilities, and peak signal-to-noise ratio (PSNR). There are challenges with authentication, high mobility, interoperability, heterogeneity, and coverage. Possible solutions are AI-based resource allocation, scheduling, routing, transmission power control, and congestion control.

Recent trends in information and communication technology (ICT) have reshaped the entire medical world by making it easier and more effective to collect data, make diagnoses, and offer treatments [24,46]. However, it is necessary to manage and enhance the patient's experience of healthcare applications, for instance, during home health monitoring or accessing personal health records [23,47]. IoT-enabled portable and wearable devices, such as smart watches, smart rings, smart necklaces, and Fitbits, can collect health data. Other devices can operate inside the human body [48]. Service providers can use the data collected to provide an accurate, convenient, cost-effective, and timely diagnosis and subsequent treatment [49,50].

It is essential for a healthcare system to make accurate and error-free critical information available to its intended users (such as physicians and patients). Due to the mobility of IoT devices and the pervasive features of 5G, these technologies have been adopted for different healthcare applications, as they allow wide coverage and sustainable connectivity [24,29]. Authentication is important for security, especially when IoT-enabled portable devices are exchanging data. IdM based on the universal subscriber identity module (USIM) has been adopted by conventional cellular networks [44]. However, this approach is unsuitable for IoT-5G devices because information can leak out during authentication. One of the limitations of IdM based on USIM cards is that most wearable devices are not compatible with USIM cards, and hence, the method fails to secure multiple devices when they are synchronously accessing services on a cloud server.

The weak security of traditional methods affects the privacy of patients accessing healthcare. Even IdM cannot fulfill the security and privacy-preserving requirements of patients effectively [51,52]. A user who accesses multiple services may need to manage numerous identities, if these services are in the cloud. Federated and centralized versions of IdM have been designed to enhance the security of IoT-5G healthcare devices [53]. A security analysis found that orthodox IdM and all its versions were inadequate due to their limited control and weak authentication [44]. Unified data management (UDM) has been adopted for managing user data and profiles in both fixed and mobile access 5G networks [54]. The need for AI in IoT devices for different applications is discussed in Ref. [55] based on Kipling's method.

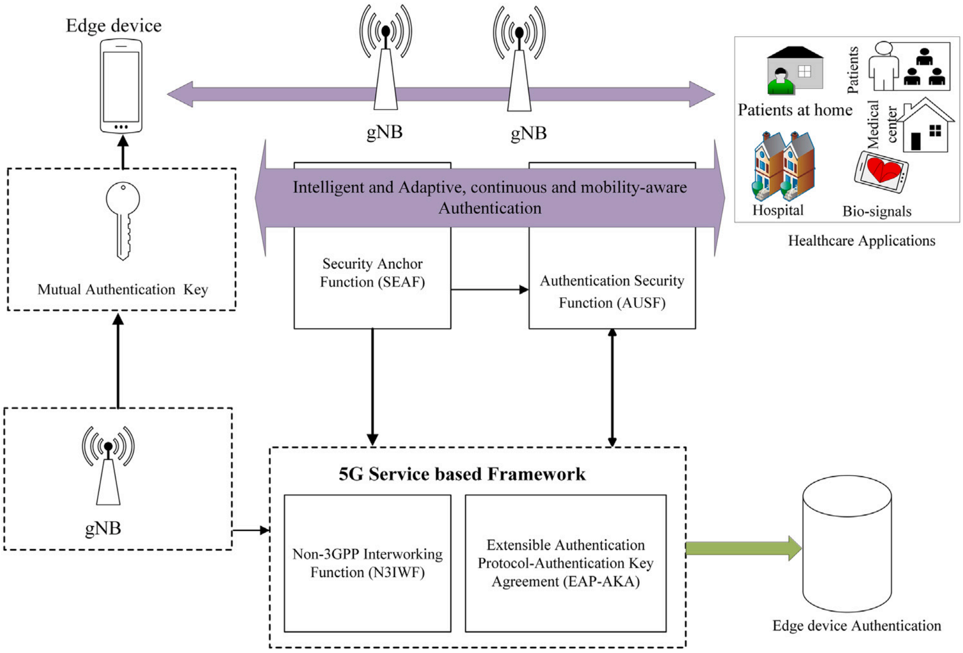

Edge device
gNB
gNB
Intelligent and Adaptive, continuous and mobility-aware Authentication
Patients at home
Patients
Medical center
Hospital
Bio-signals
Healthcare Applications
Mutual Authentication Key
Security Anchor Function (SEAF)
Authentication Security Function (AUSF)
gNB
5G Service based Framework
Non-3GPP Interworking Function (N3IWF)
Extensible Authentication Protocol-Authentication Key Agreement (EAP-AKA)
Edge device Authentication

Fig. 4. Authentication model for IoT-based 5G devices in smart healthcare: While exchanging the critical and sensitive patient's data over 5G links there are more chances of eavesdropping and attack. Therefore, an AI-enabled intelligent authentication model is necessary for authenticating legitimate users.

2.2. Device authentication in 5G

The authentication model illustrated in Fig. 4 is for a 5G network. A next-generation node B (gNB, i.e., a BS) provides one-time authentication by sending a token to a device. Mutual authentication keys can protect edge devices effectively. The security anchor function and the authentication security function are directly interconnected to the gNB and UDM through an interlink to the non-3GPP interworking function and the authentication key agreement in the extensible authentication protocol. These interconnected elements provide a high level of authentication to IoT-5G healthcare applications.

Wearable IoT-5G devices, such as smartphones, smart rings, and smart watches, are important devices as they can access the entire healthcare platform. Such lightweight devices are easily compromised, leaking secret and sensitive information [56]. Such attacks could give illegitimate entities access to the main network. Hence, an intelligent authentication method is direly needed. Such a system would repeatedly authenticate users in the background to detect illegitimate access [57]. IoT-5G devices can be a rich source of data while allowing authenticated users access to the regular system without interruption [58,59]. Many researchers have highlighted the use of mobile apps as a revolutionary step forward in digitization. However, some approaches are too simple because they do not consider network traffic patterns, which are necessary for accurate and effective device authentication. Hence, an intelligent authentication model needs to be developed to permit access only to legitimate users [60]. Our research focuses on using network traffic to and from a user device for authentication [61]. In our authentication model, patients and healthcare providers interact through their smartphones over a 5G wireless link. For example, this could be used to monitor the health status of emergency and elderly patients at home or in hospital [62,63].

Hospitals can be assumed to be trusted authorities. They could monitor contact between home devices, smartphones at emergency locations, other hospitals, and pharmacies, for example [15]. They could gather all the information related to when applications are utilized, which could be used to train an AI model. Such an intelligent device authentication model would classify network traffic patterns as legitimate to allow access. Every single network event would be classified, such as the traffic from a wearable device to a hospital. Unauthorized access would be detected with an accuracy threshold set during the training phase [49,64]. Thus, the trained AI model would authenticate users and allow access to resources. Its decisions could be input into an expert system. Such a system has a knowledge base (with facts) and an inference engine (with expertise) [65]. This whole process could be iterated to build an intelligent authentication system for identifying legitimate users and attackers in a healthcare network.

Generally, biometrics applications are categorized as verification or identification. The former is defined as the process of confirming whether a claimed identity is correct after comparing it to a threshold level. Verification is used interchangeably with authentication. Identification, in contrast, determines the identity of an individual [61,66].

An authentication model for healthcare applications should be evaluated with key performance indicators, for instance, false acceptance rate, false rejection rate, and human biometrics, such as data from an electrocardiogram [52,66].

3. Triad of IoT, 5G, and healthcare: A survey

This section presents an extensive survey that we completed of authentication, particularly device authentication, AI, and the triad comprising IoT, 5G, and healthcare. As a result, 20 technical articles were identified for the two main streams: the triad of IoT, 5G, and healthcare and authentication.

The main use cases for 5G technologies and their impact on healthcare are addressed in [7]. Healthcare is necessary for the aging world due to the immense power of the current technological trends. Instead of the expected proliferation in 5G networks and smart and lightweight portable devices, there have been various shortcomings that need to be rectified. The authors of that paper designed a two-layer cellular framework that comprises a micro-cell (for BS-to-device communication) and a device layer (for D2D communication). To improve transmission, the authors of that paper consider a device terminal to be a relay station. Device relaying is one of the key ways to reduce network resource costs [8]. D2D communication is an empowering and integral part of 5G technologies in providing improved services in terms of high data rate, low latency, and better reliability.

Cellular networks offer device-centric communication. Traffic offloading from conventional network components to a D2D network can reduce the computational complexity and enhance the capacity of the BS. Furthermore, the critical challenges in D2D communication have been highlighted [3]. That paper also provides a detailed survey of interference management, network security, and provisioning for proximity services plus future research directions. Our research focuses on IoT-5G devices and their authentication for smart healthcare applications that aim to help patients in a healthcare facility, at home, or in other remote locations. Optical cameras directly linked to a 5G access point can be used to monitor patients and healthcare units.

Patient data are being collected by portable devices, such as cameras and sensor nodes. Such data can be used for diagnosing and monitoring diseases in rural areas, for example [4]. Ref. [5] presents insights into AI-enabled BSs for 5G networks. These BSs can help portable devices to establish dynamic clusters based on learned features rather than on previously stored and fixed components, which can improve network efficiency, as delays will be lower and reliability higher. The key issues faced by 5G technologies are highlighted in our future recommendations.

The authors in [6] comprehensively investigated the role of multi-access edge computing (MEC) in 5G and IoT for enriching different applications by providing supporting technologies, i.e., cloud computing, software-defined networks (SDNs), network function virtualization, smart devices, network slicing, and virtual machines. Additionally, research challenges related to MEC when integrating 5G and IoT are discussed. These researchers claimed that the rapid progress of IoT and e-health means that 5G is a game changer for the smart medical world and services. A content-centric network running on a 5G platform was proposed to support smart and cost-effective medical care. The authors noted that two key problems – packet loss and security – can be resolved by this type of network [1].

Ref. [2] examined the importance of the effective dissemination of electronic health records over an unreliable network with mobile nodes and cloud-enabled health information. Their proposed approach offers faster dissemination, better service composition, and reliable synchronization of healthcare content. The authors in [9] designed a 5G framework that ensured efficient mobility management and successful packet delivery for a healthcare system. Moreover, they noted that the proposed method can interconnect various links with a fair allocation of resources. 5G-enabled intelligent and cooperative technologies are promising options for multimedia platforms, i.e., video streaming. Multimedia data not only give detailed information but offer clear and highly visible insights for a critical scene analysis. For example, remote surgery needs high speeds, short delays, and better visualization at both the expert's and the patient's side [67]. An overview of the role of slice networks in transforming critical healthcare applications on a 5G platform has been presented [67]. Also discussed are media-centric healthcare use cases, which are key components for enhancing QoS.

The authors in [10] proposed non-orthogonal multiple access (NOMA) to allocate Internet resources, such as enhanced mobile broadband, mMTC, and URLLC, at application-specific nodes to the BS fairly and efficiently. Furthermore, they highlighted the emerging revolutionary technologies for obtaining reliable, delay-tolerant, and secure applications. A detailed and rigorous review of smart healthcare from 2011 to 2017 was presented. Moreover, the role of machine-learning (ML) strategies, such as artificial neural networks, support vector machines, and deep learning (DL), in supporting the operation of medical care units was examined. The main diseases that can be diagnosed include Alzheimer's, bacterial sepsis, and cataracts [12]. Machine-to-machine communication in association with the 3GPP and LTE-A has caught the attention of researchers in various fields, so a rigorous review of key features, network metrics, applications, and architectures has been conducted. Moreover, challenges in transmission and QoS optimization in machine-to-machine communications need to be considered [13].

The advantages, prototypes, classification, and applications of D2D communications for a cellular network have been presented as well as potential benchmarks. 5G is being extended with many new technologies, which can be used to build secure, reliable, cost-effective, and energy-aware platforms. D2D is one of these technologies, as it can efficiently allocate resources among devices without the involvement of any external entity [68,69]. D2D can play a key role in boosting the performance of 5G use cases by efficiently utilizing the throughput and spectrum for time-critical applications, such as healthcare [11].

The rapid progress in small, low-cost, wearable devices has transformed various fields, such as monitoring soldiers on a battlefield. 5G-enabled portable devices are the key enablers for defense automation and monitoring [38]. A detailed classification of 5G-enabled wearable technologies and their role in defense systems along with future communications and security challenges was presented. An architecture for smart watches that allows proper monitoring of healthcare applications over 5G has also been proposed [38].

The proliferation of 5G wireless technologies, IoT, big data analytics, wearable devices, and intelligent resource allocation techniques, such as those based on AI, has reshaped the entire medical world. For example, these changes have enhanced the

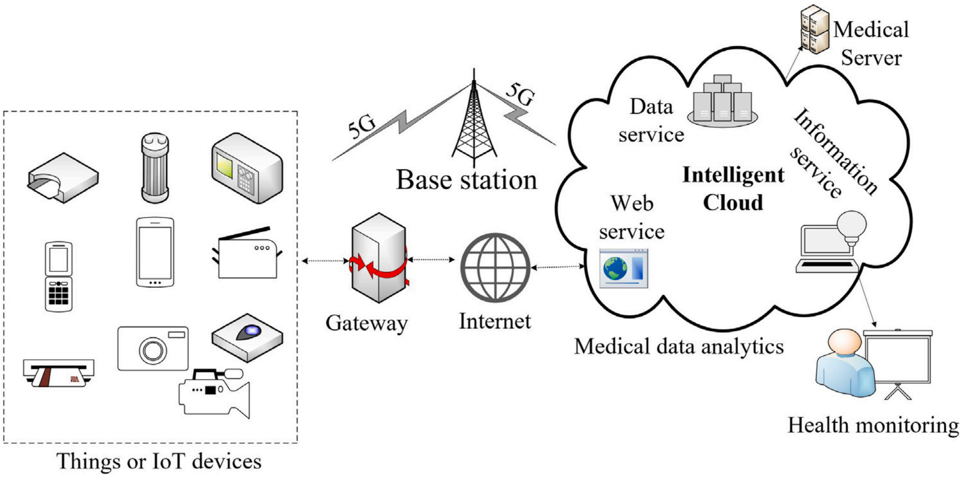


Fig. 5. IoT-based 5G healthcare: Patient's physiological signals are collected through wearable devices and transferred over the 5G wireless links to and from hospitals and patients.

examination, consultation, and diagnosis of diabetic patients. As it is essential to explore novel and effective methods, a detailed survey was completed [30]. In addition, a state-of-the-art 5G-enabled smart diabetic monitoring system built with heterogeneous technologies, such as, IoT-enabled wearables, big data, compressed sensing, and informatics, has been developed to allow better and more cost-effective personalized care [43].

The utilization of 5G for healthcare is growing, so it is necessary to develop and test relevant software for each new hardware setup to ensure compatibility and synchronization. Newly designed hardware must be able to communicate in high-frequency bands to allow proper integration with a 5G network. Thus, 60-GHz universal software radio peripherals have been adopted as a test bed during the emulation of the real world by software as a virtual world [70].

The latest and fast-growing trends in advanced technologies, namely, IoT, D2D, and sensor-enabled wearables, have remarkably revolutionized and promoted 5G-enabled, smart, secure, cost-effective, energy-efficient, and battery-aware systems [48]. The role of the physical and medium access control (MAC) layers in 5G in delivering healthcare services to remote locations, i.e., telemedicine, has been presented [48]. Low-cost wearable devices with small antennas are the major performance boosters for 5G healthcare applications [71]. A sequential arrangement of small antennas operating in the 4.8-GHz frequency band using the finite-difference time-domain technique has been adopted for a 5G healthcare use case [71].

Fig. 5 shows an IoT-5G enabled healthcare framework. It has things, a gateway, the internet, medical data analytics systems (web services, data services, and information services, which are all monitored and managed by an intelligent cloud) with an interconnection to a medical server for health monitoring. A BS has a key role in transmitting information over 5G links to the IoT-enabled things.

ICT is important for cost-effective and error-free pervasive healthcare provided via the IoT. Due to the remarkable reduction in the size of wearable devices, patients can wear harmless and low-cost devices that provide effective diagnosis and disease monitoring without the need of a physician [23]. However, a limitation of such portable and lightweight wearables is that they are power hungry so can have a limited lifetime and little capability to transfer their critical contents when used at a remote location. To remedy these challenges, 5G-enabled intelligent mobile gateways for smart healthcare wearables have been proposed. Such gateways can act as an intermediary by transferring data from wearable devices to edge nodes [23].

IoT-enabled sensor devices, mobile gateways, and relay-assisted wearables can monitor, diagnose, and detect a patient's health status efficiently and accurately. Furthermore, 5G mobile technology facilitates healthcare due to its high throughput, ultra-low latency, ultra-high reliability, and cost-effectiveness. When transferring critical information, 5G establishes a strong connection between a patient and a healthcare center, anywhere at anytime. The main problems with traditional wearable devices are the lack of capacity for the voluminous data and effective resource allocation. Thus, 5G-enabled network slicing and AI need to be investigated for heterogeneous and resource-constrained applications [72].

Self-driving vehicles are an emerging use case for 5G. They have caught the attention of smart industrialists and business executives. The concept of smart ambulances is entirely new in the healthcare world. Such ambulances will use the IoT, the Internet of vehicles (IoV), connectors, and indicators all connected over an intelligent and resource-efficient 5G network. Various wearable devices can easily collect physiological signals (such as blood pressure, temperature, and heart rate) from an onboard patient, then diagnose their health status. Such smart ambulances need further investigation [53].

5G is a revolutionary and promising technology due to its high capacity, high carrier frequencies, large antenna array, high device density, and large number of BSs [73]. Three hot and emerging 5G use cases – healthcare, vehicular networks, and drones – need to be explored further and standards need to be established [73].

5G divides the load by assigning tasks to edge nodes such as BSs. Different healthcare applications have different priorities and importance levels for data transfer and computational resources. It is essential to determine the priority and authenticity when allocating resources to healthcare applications, as it is hard to justify and fairly allocate resources without knowing the priority of the service (i.e., emergency or routine). Moreover, end-to-end delay management in 5G healthcare is important [74]. The healthcare market is evolving with emerging 5G trends, but there are both opportunities (high bandwidth, ultra-high reliability, ultra-low latency, and longer connectivity) and challenges (heterogeneity, poor compatibility with traditional infrastructures, and lack of interoperability). It is necessary for modern medical facilities to fully integrate with 5G to realize digital and pervasive healthcare [42].

Conventional medical facilities need to be redesigned and equipped with state-of-the-art digital technologies, such as 5G. Smart, efficient systems rely on modern innovative technologies, such as 5G, edge computing, IoT, big data analytics, and D2D communications. There has been a rapid development of imaginative technological applications but emotionally aware care and services for elderly patients, for example, have often been overlooked. Ref. [75] describes an emotion-based connected healthcare platform for an aging society. The platform uses heterogeneous technologies. For example, IoT-enabled wearables capture the speech and image signals of elderly patients in hospitals and smart homes. The utilization of the effective and adaptive role of 5G, D2D, and IoT in healthcare is still in its infancy and still growing. There is a dire need to think about improving healthcare services and applications. The digital world can offer ease and comfort when 5G is properly integrated with medical services [55].

Healthcare applications, such as telesurgery and telerobotics, are extensively supported by 5G due to its ultra-high reliability and ultra-low latency when delivering multimedia content, such as video, audio, text, and haptics [46]. Telerobotics can be used by medical professionals and the relatives of elderly patients to provide cost-effective services in rural areas. Some of the challenges faced by 5G-enabled teleservices are the high mobility of sensor nodes and the dynamic nature of wireless links. As a result, information can be lost due to fading, signal scattering, or shadowing [46].

Due to the rapid proliferation of 5G mobile networks, emerging and critical healthcare services, such as telemedicine and telesurgery, and remote medical care have significant potential. At present, most remote healthcare services are fulfilled by 5G mobile technology due to its sustainability, range, and delay-tolerant features [76,77]. Pervasive and sustainable healthcare has been made possible by 5G technology, which allows various caregivers, including physicians, hospitals, and other medical care providers, to offer good cost-effective services. 5G is a promising platform for helping patients to rejoin the workforce as they can receive precautionary guidelines and consultations. Further, 5G enables data to be gathered by wearable devices and cloud-enabled entities, which can be used to provide accurate diagnoses [24,78].

The intelligent and adaptive features of 5G, such as ultra-high bandwidth, ultra-high reliability, and ultra-low latency, support various use cases, including smart healthcare, smart cities, and smart transportation [79]. Integrity and high compatibility allow 5G networks to accommodate diverse technologies, such as federated learning, network slicing, and virtual reality. However, visualization, high device density, and heterogeneity are key security concerns and the subject of debate. Additionally, 5G can enrich our world due to its high density and longer connectivity, compared to 4G, which offers pale and fewer vibrant scenarios [79,80].

3.1. D2D communications in IoT-5G

D2D communications offer a direct link between devices with or without the involvement of conventional network infrastructure, such as a 3GPP network. Consequently, the intelligence and adaptability of a connected D2D platform used for data offloading can directly support the sharing of resources with nearby devices [81,82]. Thus, congestion and scarcity of spectrum can be efficiently addressed, leading to increased network coverage and throughput and reduced power drain and delay. Most communications in 5G and IoT are performed by lightweight and resource-constrained portable devices. Thus, D2D communication has significant promise and may be a key enabler in reshaping the entire world [83]. The considerable increase in the data transferred by 5G needs a powerful workforce to effectively manage, monitor, and demand the high level of network services [84].

Conceptually, D2D communications are a promising and adaptive technology that enable portable devices, such as smartphones, sensors, and personal data assistants, to communicate effectively without using a BS, access point, or core network [85,86]. The closeness between devices in D2D communications provides better insights for optimizing the throughput, delay, energy dissipation, and traffic load [87]. Hence, more peer-to-peer and location-based services and applications are accommodated through D2D communications and next-generation networks.

The dynamic and scalable features of a 5G network mean that is a heterogeneous platform, allowing healthcare applications to monitor patients better. However, the high mobility of sensor-based IoT devices and dynamic wireless links causes two major challenges, namely, security and energy drain. Integrating massive IoT (mIoT) technology into healthcare through 5G D2D communications is promising due to the highly secure, effective, and fair management of radio resources [88]. Besides, D2D communications have been widely adopted as an emerging method of short-range data delivery for IoT-5G healthcare applications due to the high security, minimum power drain, high energy efficiency, and ultra-high reliability [89].

A conventional macro-cell BS supplies a small amount of power to a BS. However, D2D transmissions between end users are performed without passing through a BS and serve as a cell tier in the IoT-5G [90]. Besides, D2D is a potential candidate for smart healthcare, because 5G offers fast data transfers, reliable connections, and good coverage. Moreover, IoT-5G is a key enabler for healthcare, as it supports the recording and delivery of human physiological signals, such as blood pressure, temperature, and electrocardiograms, which are used to diagnose a patient [45,91].

Due to the lightweight and small size of IoT devices, it is inappropriate to deploy conventional cryptographic methods over 5G-enabled healthcare platforms, because of their high computational complexity and communication overhead. Conventional

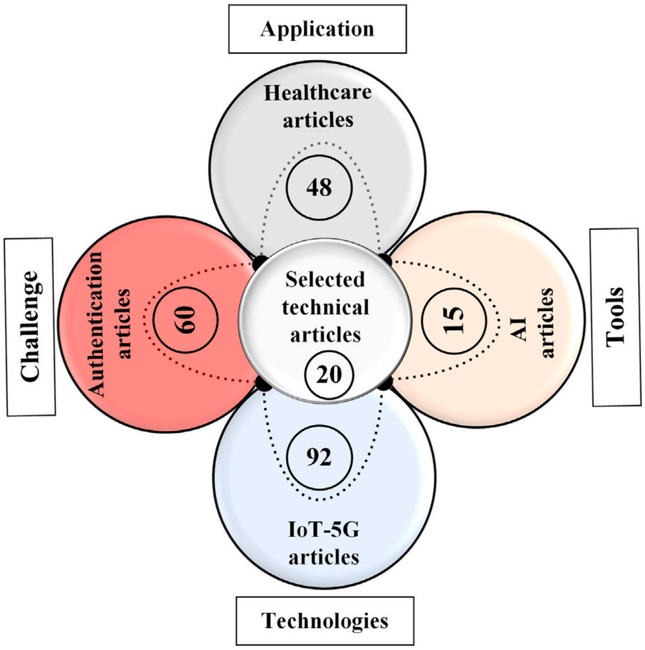


Fig. 6. Venn diagram for categorization of research papers in different domains: Technologies (IoT-5G), applications (healthcare), tools (AI), and challenges (Authentication). Besides, the circle in front of each entity shows the number of relevant articles accordingly.

cryptosystems consume too much power and thus, shorten battery lifetimes. As a result, authentication can be problematic for a resource-poor IoT-5G device [92,93]. Thus, better authentication methods must be developed for devices that transmit sensitive medical information. Despite several advantages of D2D communications, challenges include security, mobility of nodes, and performance degradation [94].

Security-related problems have been extensively reviewed by various researchers [95]. Healthcare applications are used to monitor and manage a person's health. Thus, security is of paramount importance in 5G devices because portable and lightweight devices can directly affect user safety [96]. 5G accommodates and supports millions of existing devices that do not have adequate built-in security, as well as new devices whose extreme computing power will make them attractive targets for hackers. 5G-enabled D2D communications may experience various types of attack, such as eavesdropping, jamming, primary user impersonation, and code injection. Multi-path routing is a potential solution for mitigating most attacks and security problems [85].

When most sensors communicate with an energy-rich node, that node will authenticate the sensors. However, security is weaker during end-to-end communications [86]. Portable devices need lightweight security solutions that are feasible and cost-effective. Hence, innovative, efficient, and intelligent security solutions suitable for the higher and lower layers of a network need to be developed [91,93].

3.2. Twenty golden studies

The 20 golden studies were selected based on their potential relevance, correlation, and overlap between IoT, 5G, healthcare, authentication, and AI. The papers covered:

- 5G ∪ healthcare,
- AI ∪ healthcare,
- AI ∪ IoT,
- IoT ∪ authentication,
- IoT ∪ healthcare,
- IoT-5G ∪ authentication,
- IoT-5G ∪ healthcare,
- AI ∪ 5G ∪ authentication,
- AI ∪ authentication ∪ healthcare,
- AI ∪ IoT ∪ authentication,
- AI ∪ IoT ∪ healthcare, and
- IoT-5G ∪ authentication ∪ healthcare.

Table 2
Selected twenty Technical papers: 10 from IoT-5G-Healthcare and 10 from Authentication sections. The explanations of the selected articles are distributed over Section 3.

References	Applications and needs	Field of research	Contribution	Limitations	Our value addition
[74]	Mobile edge computing for high-speed data transmission in 5G	MEC,5G, healthcare	An algorithm for E2E delay optimization in wireless network	higher delay and less reliability in traditional methods	AI with MEC and 5G for secure Authentication
[10]	AI and 5G	Dynamic adaptive clusters	NOMA-based communication architecture	Poor spectrum efficiency of 4G	AI-driven authentication devices are necessary
[58]	On-body IoT devices	IoT devices, authentication	General authentication solution with PHY signatures for upper-layers	weak security of IoT devices	AI for authentication of IoT-5G
[1]	Secure, reliable and efficient E-health	Content-centric, IoT, 5G,	Content-centric framework for 5G-based e-healthcare	high packet loss and weak security	Intelligent and reliable authentication model for IoT-based 5G healthcare
[23]	Less error-prone and cost-effective healthcare	Healthcare, AI, 5G, IoT, ICT	Intelligent and energy-efficient 5G-based smart gateway	Limited resources of IoT-based smart devices	Intelligent, efficient and authenticated IoT-5G devices for healthcare
[74]	MEC-based delay-tolerant healthcare	MEC, IoT, 5G, Blockchain	End-to-end delay optimization for wireless users	less secure and high-delay oriented networks	5G-based intelligent, secure and delay-tolerant healthcare
[46,75]	5G-based healthcare for everyone	mobile healthcare, ambulance, IoT	5G-driven telemedicine, and wireless tele-surgery frameworks	connectivity and compatibility of heterogeneous platforms	IoT and 5G enabled intelligent and secure remote healthcare prototypes
[24,79]	5G for connected wellness and smart healthcare	5G, IoT, healthcare, smart cities	IoT-5G driven wellbeing framework	security, reliability and compatibility	Secure, and intelligent techniques are dire need for pervasive and cost-effective healthcare
[97]	5G and beyond wireless networks	5G, ML, heterogeneous devices and machines	Novel authentication techniques with the help of PHY attributes	high-security overhead, low reliability, and lack of precise authentication model	Intelligent, cost-effective, reliable, and dynamic authentication model
[26]	Secure 5G heterogeneous networks	5G, Cross-authentication, Heterogeneous	SDN-driven fast cross-authentication method	High latency and weak security	5G-driven intelligent, authenticated models for IoT-devices are dire need
[98]	Channel-based PHY-layer enhanced authentication for 5G	Channel, PHY-layer, Authentication	Novel authentication technique for spoofing attack detection	less detection rate of PHY-layer authentication	Joint intelligent and authenticated methods for IoT-5G devices
[99]	Connectivity monitoring and authentication for massive IoT devices	Authentication and access control in IoT devices	Slice-driven authentication and access control method for IoT devices	High signaling load and weak security	To boost flexibility, modularity, authentication, and intelligent level of IoT-5G devices
[100]	Key authentication in NB-IoT and 5G devices	Authentication, bootstrapping, 5G	Bootstrapping protocol with 5G features and authentication extensible protocol for NB-IoT devices	Weak authentication and key establishment mechanism of IoT devices	Intelligent and authenticated methods for IoT devices
[101]	Access authentication for the user equipment and MTC devices	5G, authentication and key agreement	5G-based authentication and key agreement protocol	Weak session and authentication keys	Adaptive and intelligent access and authentication methods for 5G-based lightweight IoT devices
[91,102]	Efficient and quick authentication for IoT devices in healthcare	IoT devices,three-way authentication	survey on authentication	Unauthorized, weak and computational complexity	Intelligent and authenticated methods for IoT-5G devices for healthcare
[16,103]	IoT device authentication for end to end services and applications	IoT device authentication	Enhanced IoT device authentication	complexity of cryptographic methods	AI for IoT devices authentication

Moreover, these 20 papers were chosen due to their strong connections between the four main pillars, namely, technologies (IoT-5G), tools (AI), applications (healthcare), and challenges (authentication). The Venn diagram in Fig. 6 shows the four pillars and the distribution of the articles, while Table 2 lists the selected papers. The selected articles are described in Section 3. Furthermore, Table 2 lists the limitations we identified and possible improvements to suggested approaches.

4. AI-based methods for device authentication

Device authentication is necessary for IoT-5G healthcare devices and applications [90,104]. Traditionally, eavesdropping and illegitimate use of sensitive data occur due to computationally complex and weaker forms of authentication. The data collected by modern wearable healthcare devices must be transferred according to the standards of the IoT-5G platform, such as proper authentication and user authorization [52,105].

Joint authentication based on AI is an interesting approach for IoT-5G healthcare applications [106,107]. Rapid progress in wearable IoT-5G devices has placed huge demands on authentication and intelligent resource allocation, which need to consider features of the entire system [108]. The adaptability and intelligence of AI make it useful for authenticating users, as it can provide efficient ways of detecting illegitimate entities in IoT-5G healthcare applications [109]. The role of AI has been extended in other fields, leading to effective and mature authentication resources [110]. Intelligent firewalls can detect and block unauthorized users in sensitive IoT-5G devices used for healthcare [29,111]. Table 3 provides a detailed overview of AI-based methods for authenticating IoT-5G healthcare devices.

4.1. Radio-frequency fingerprinting

Radio-frequency (RF) emissions play a major role in identifying and authenticating portable devices. Minor differences in the materials and structure of an electronic circuit (made by different manufacturers or production chains) result in small changes in the RF signal over air [120]. Detecting these differences is known as RF fingerprinting. It can be used to achieve secure and reliable communications through portable electronic devices [47,121]. RF fingerprinting supports multi-factor authentication, in which physical-layer authentication functions autonomously, and traditional cryptographic authentication.

Identifying the unique physical features of the RF circuits in an electronic device can prevent any fake, illegitimate, or unauthorized entity from accessing the system. Multi-authentication is a common use of RF fingerprinting, as it can differentiate between two examples of the same model of an electronic device that have unique serial numbers [122]. It is essential that authentication is based on IdM for IoT devices. In a new secure authentication mechanism based on identity provisioning and management of IoT devices, an identity association is obtained between a cellular network and an IoT platform, which allows devices to execute tasks in a secure and trustworthy fashion [123].

RF fingerprints for several users (i.e., user 1 to user n) can be input into a feature extraction module. A classifier is then trained on the data and the results are stored in a database. The outputs from the training stage and database are the inputs to a classifier, which makes the final decision regarding the identity of a user (Fig. 7).

4.2. IoT device authentication

For critical healthcare applications, IoT devices need a high level of security, especially authentication and proper access control, when transferring sensitive information. Because of the dynamic nature of the wireless link and open signal propagation of wireless technologies, it is easy for attackers or eavesdroppers to intercept messages or impersonate a user [124,125]. An in-depth review of traditional authentication methods found numerous IoT security challenges. These include inadequate security measures, inefficient or insecure interoperability, computational complexity, and issues with the deployment of cryptosystems over IoT devices [126]. The static and inflexible nature of authentication methods makes it difficult for them to adapt to the growing number of mIoT devices [127,128].

According to Ref. [129], there are four major steps in a D2D authentication model:

1. A D2D token is generated. This is done once only for each piece of user equipment (UE).
2. Devices are discovered.
3. The data link is set up.
4. The authenticated data are transmitted.

This process authenticates IoT-5G devices, ensures their integrity, and preserves the confidentiality of the data.

Authentication with conventional cryptographic techniques does not seem to be feasible due to several major challenges, such as high computational complexity, high communication overheads, high latency, and weak security of resource-constrained mobile IoT devices for healthcare applications [124,130]. Key management is suitable only for traditional cryptosystems. The static features of traditional cryptographic methods do not allow the detection of the reuse of compromised keys by unauthorized entities [131,132]. Rapid progress in the development of IoT devices for heterogeneous platforms has been enabled by 5G and beyond networks. The low cost and small size of such devices make them suitable for diverse applications [123,133].

ML authentication techniques implemented on the physical layer have caught the attention of academia and industry. This approach provides security intelligently and efficiently to 5G-enabled portable devices [91,134]. ML-enabled techniques, for instance, supervised and unsupervised learning and DL, are useful for authenticating entities. Because ML approaches consider unique multi-dimensional attributes, they can achieve more secure, better authorized, fairly accessible, highly reliable, dynamic, and self-driven device verification for an unspecified network status [91,135]. Poor security and long delays can affect the performance of critical applications such as healthcare. Such issues can be resolved with a fast cross-authentication approach, which uses SDN-aware joint cryptographic and non-cryptographic attributes [26]. Initially, unpredictable secret keys are provoked with the support of the vector of received signal strengths as the source of an RF fingerprint of a mobile terminal.

Table 3
AI methods for 5G-enabled authenticated healthcare.

References	Application domain	AI techniques or methods	Key features	Remarks
[112]	UE authentication for 5G networks	Fault-tolerant driven authentication for 5G	5G end-device authentication through fault-tolerant method	Resource-poor nature of UE authentication and fault diagnosis are vital
[113]	Cognition-based D2D authentication	Lightweight key exchange method for authentication	Cost-effective and secure D2D communication	Direct communication weakens security with less reliability
[37]	Mobile edge computing for edge intelligence in medical applications	FL for training the ML data models	Collaborative training of ML driven mobile edge networks	Communication cost, and security in FL deployment
[31]	ML methods for IoT security	Requirements and secure solutions for IoT	Overview, problems and secure ML methods for IoT	Less secure and complex cryptography techniques
[114]	Mobility in D2D communication	Intelligent D2D communication in 5G	Real-time applications of D2D networks	Resource-efficient, reliable and direct D2D communication
[29]	Authentication for wearable and e-health devices	An overview of IoT authentication	Classification and evaluation of authentication	Due to the resource-constrained nature of IoT devices, authentication is demanding
[73]	5G for healthcare	5G-based high career frequencies and bandwidth	5G as a game-changer with more BSs and high device density	5G communication for healthcare and vehicular platform
[115]	IoT features, components and protocols	Adaptive and self-organ zing IoT frameworks	Comprehensive survey on IoT	Compatibility of IoT with other technologies
[5]	Intelligent and self-decisive base stations	Detailed survey on the AI methods for 5G	AI-driven techniques for 5G technologies	An overview of challenges, and future research in 5G and AI
[6]	Mobile data traffic of IoT-based healthcare	Multi-access edge computing for IoT-5G	Role of MEC in IoT-5G based cloud computing, SDN	Challenges of MEC in IoT-5G and related use cases
[97]	ML for effective and reliable authentication in 5G	ML-based intelligent authentication method for 5G	Intelligence to 5G authentication	Security overhead and low-reliability overhead issues in cryptography methods.
[116]	Intelligent 5G networks	Trade-off between AI and 5G networks	To manage and allocate the resources in 5G networks	Joint AI and 5G networks for radio resource and mobility management
[117]	Secure and remote health monitoring	IoT-enabled security solution in Telemedicine	Remote patient monitoring and authentication to IoT devices	Dynamic and heterogeneous nature of wearable healthcare devices
[118]	IoT-5G driven smart healthcare and homes	Adaptive Kalman filter based private data streaming technique	Security provisioning to the sensitive and critical sensor-data	Testbed setup and analysis of results by adopting real-time datasets
[110]	Mutual authentication and key establishment for WBANs	Adaptive secure authentication approach for wearable devices	Secure and mutual authentication for IoT-devices	Comparative analysis with existing state-of-the-art methods is performed
[111]	Massive MIMO, mmWave, and ultradense networks	AI-driven flexible and cross-layer framework for 5G and beyond networks	Intelligent agent-based technique that integrates sensing, learning, and optimization of emerging technologies	Joint AI approach for 5G use-cases by adopting massive MIMO antenna system, and ultradense networks
[91]	Security and resources allocation in IoT devices	AI-based approach for trust management and adaptive access control	a lightweight intelligent authentication mechanism for identifying access time slots or frequencies of IoT devices	Authentication and authorization are important for large-scale IoT devices due to their diverse and heterogeneous nature
[45]	Digital healthcare system	Supervised deep belief architectures	To improve the QoS level	Intelligent and smart healthcare with the help of AI, IoT, and 5G
[85]	High-speed Internet networks	AI techniques for massive IoT data management and flow	AI-driven remedy for data mining, manage and control of congestion in IoT	AI, fuzzy logic and intelligent methods for IoT, data mining, and data traffic monitoring applications

(*continued on next page*)

Good authentication and access control of IoT devices can enhance the security of these portable entities and hence, the overall 5G platform. For most IoT-enabled technologies, such as 5G release 16 (R16) and cellular networks, the authentication and access control of IoT devices are performed in the same way as they are performed for mobile broadband and UE [99]. The rapid progress

Table 3 (*continued*).

References	Application domain	AI techniques or methods	Key features	Remarks
[23]	IoT-5G enabled Smart healthcare	Intelligent and Energy-efficient mobile gateway	Integration of ICT and IoT for smart healthcare	To minimize the medical errors and healthcare cost, intelligent 5G-driven mobile gateway are vital
[104]	Cyber-assurance of IoT	AI for better connectivity	AI and IoT for interconnection	Interactive connection between the physical world and computer field for improving efficiency, accuracy, and economy
[119]	Data traffic and connectivity of massive IoT devices	AI-driven semantic-IoT for smart city	AI-based semantic IoT for user-centric smart city	Main focus is the AI-driven semantic IoT for hybrid services and architectures

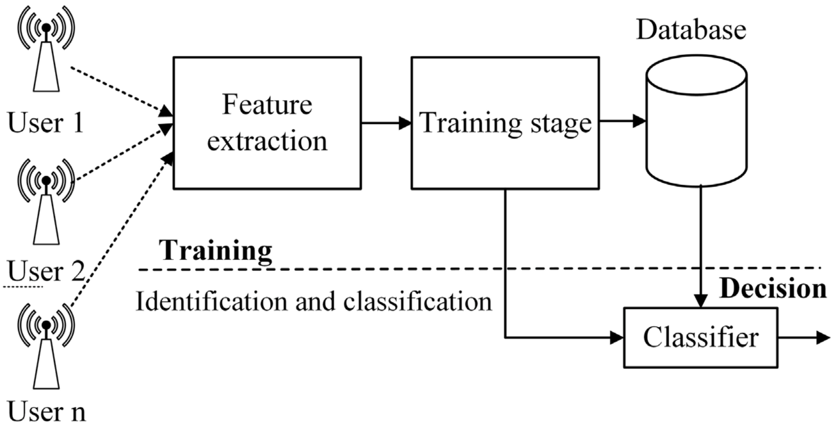


Fig. 7. RF fingerprinting mechanism: Several base stations can send their signal beams to the feature extraction, training stage, and then to the database. Outputs of the training stage and database are the inputs to the classifier.

in the development of mIoT devices could put a heavy load on the core network and cause major failures of network connections. A flexible and virtual approach to slice-specific authentication and access control is promising for the efficient authentication and access control of a large number of IoT devices [136].

Researchers from academia and industry have made remarkable progress in investigating secure and trustworthy communications among IoT-enabled applications, including healthcare. However, a simple and cost-effective security mechanism with a single sign-on authentication approach is important for providing ubiquitous medical care [137]. Radio channel information can play a significant role in countering spoofing attacks. Thus, channel-aware PHY-layer authentication is important and a potential candidate for securing lightweight IoT-5G healthcare devices. One of the downsides of PHY-layer authentication is its low attack detection rate, and hence, an innovative authentication approach is needed to identify an attack without using a test threshold. Trained models can efficiently determine whether a user is legitimate [100,137].

Efficient and adaptive authentication techniques are necessary for lightweight sensor-driven healthcare devices [138]. Researchers have proposed an efficient and strong authentication protocol. Its main steps are two-factor authentication, mutual authentication, symmetric encryption and decryption to ensure the confidentiality of content, secret session formation after authentication, and finally, changing the passwords of medical experts and patients. However, the authors did not focus specifically on authenticating IoT-5G devices for healthcare applications [138]. Due to its flexibility and easy deployment, bilateral PHY-layer handover authentication may be useful for 5G heterogeneous SDNs [139]. The features of the physical layer of a wireless link communicating with a BS play a major role in verifying, testing, and validating the identity of both UE and access points [139].

Assessing the integrity of IoT devices to prevent access by illegitimate entities can be done effectively by physical-layer authentication. The authors in [140] devised Gaussian-tag embedded physical-layer authentication based on a weighted fractional Fourier transform. Due to the low-power consumption and efficient features of the Gaussian tag, there is an easy mapping with a message signal. Thus, legitimate and authorized receivers can attest to the legitimacy of the received signal without being exposed to an antagonist [102,140]. Besides, the mutual authentication level is higher, the session-key formation is better, and the forward and backward secrecy is more accurate [101].

The authors in [113] proposed the lightweight incognito key exchange protocol for authenticating LTE-A devices. The main purpose of their research was to provide trusted D2D communications, which may allow 5G devices to offer secure, cost-effective, and pervasive services for advanced and critical applications. Secure and power-aware methods are key enablers for long-range wide area networks, as they can reduce energy consumption by end devices during encryption with the Advanced Encryption Standard

(AES). Properly monitoring the power allocated to traditional AES will help IoT devices to get the resources required according to the requirements of applications [141]. Mutual authentication has received special attention for IoT-enabled portable devices. The authors of the work above designed a framework utilizing secondary authentication between UE and a data network. The two core parts of the proposed framework are the secondary authentication and the authentication data management. It ensures authentication is adequate and cost-effective for legitimate devices [142].

Combining a wireless body sensor network with a cloud computing platform is a promising and effective strategy for offloading workload, increasing the bandwidth, and reducing delays for healthcare applications. The authors of Ref. [143] highlighted the key merits and related challenges of hybrid methods and their integration with 5G technologies. Moreover, they discussed issues relating to authentication for body sensor networks, cloud computing, and 5G, such as possible risks, attacks, and solutions. IoT is a key pillar of various applications, including smart healthcare, smart cities, and smart transportation, and also of various services. Further, IoT-enabled wearable devices have reshaped many aspects of academia and industry, especially healthcare. However, since patient information is critical and sensitive, it is essential to authenticate user devices with proper verification and authorization [29].

Healthcare professionals are important caregivers in urban and rural areas. With the rapid boom in IoT-enabled wearables, IdM and security, i.e., authentication, have become more important. However, traditional cryptographic techniques are inappropriate for lightweight, power-hungry IoT devices due to their limited battery lifetime. Hence, there is a need for new secure and efficient resource allocation methods for IoT-5G [144,145]. IoT-enabled wearable devices are a paradigm shift and key ingredients for transforming conventional care into entirely digitized and smart healthcare, which fulfills the needs of medical professionals and patients to a large extent. However, the transfer of critical patient data is at high risk of eavesdropping, impersonation, or illegitimate access [146]. Thus, to provide access to authenticated and authorized entities in healthcare, it is vital to develop novel and efficient security techniques [147].

Entropy is a measure of the amount of information transferred. The authors in [148] proposed using entropy-driven authentication of IoT devices based on RF fingerprinting. They also compared current and conventional authentication techniques [148]. If there are good interconnections between a 5G network and mIoT devices, then vehicular networks are envisioned as being particularly useful. The higher and longer connectivity between IoT devices offered by ultra-high-speed 5G platforms raises concerns about security due to the wide heterogeneity of vehicular environments [149]. Efficient software security is essential for ensuring privacy while a vehicle is exchanging information over a 5G network. Message authentication among vehicles is achieved through elliptic-curve public-key cryptography but without a certificate cancellation list [149]. Tolerating and rectifying faults in 5G devices are important for strengthening security in general and authentication in particular.

Virtualization is one of the core services of 5G. If any virtual machine fails, then the service function will take over its tasks for end devices to ensure the security and QoS of the entire network [112]. Biometric authentication has become more popular for healthcare wearables, as security based on identifying and validating users is important for healthcare applications [150]. Furthermore, the authors of that work compared the security of the proposed method with other verification and adversary-detection tools. IoT can easily be adjusted to new technological trends. It has significant potential in various domains, for instance, smart healthcare, smart homes, and smart industry. The role of IoT in healthcare is less certain for remote elderly patients, particularly those with chronic disease or who need continuous assisted living. There have been high-security alerts and challenges, thus precautionary measures and recommendations are needed. The small size and resource-constrained nature of IoT devices coupled with the inefficiency of traditional cryptographic techniques means it is essential to develop novel key generation, agreement, and authentication methods to protect against eavesdropping and denial of service attacks [151].

AI-based authentication for resource-constrained IoT devices is a game changer, as it cost-effectively allows access only to legitimate users with effective resource allocation. Gateway nodes equipped with high intelligence can fairly manage energy consumption and battery lifetimes to ensure high security levels. The low weight and portable nature of IoT devices encourages rapid authentication and continuous authorization of emergency applications [10,91]. An extensive review of authentication and privacy protection for 4G, 5G, and associated technologies has been conducted [152]. Attack modes and the corresponding countermeasures have been categorized and clustered [153]. There is also a detailed overview of existing surveys of 4G and 5G cellular networks [61]. Besides, there is an in-depth review of several other related authentication and privacy frameworks, methods, and platforms, such as handovers, mutual authentication, RFID, anonymity, and three-factor authentication [152].

Wireless body area networks (WBANs) connect well with an IoT to allow efficient monitoring of human vital signs by wearable devices. However, due to the dynamic and mobile behavior of the sensors and wireless link, security is a major concern and a subject of debate. Further, the small size and resource-restricted nature of IoT nodes limit their wider application. Thus, novel adaptive authentication and key management techniques with high compatibility with modern smart healthcare applications are direly needed [154]. The increased capacity and faster computational speeds of smart mobile phones allow them to gather and monitor voluminous amounts of data and to act as a mediator for managing the services in a next-generation 5G network [155]. One of the merits of a WBAN is that it enables lightweight and efficient biometric authentication for IoT-5G platforms based on intelligent key management.

Most end-to-end services and applications are enriched by IoT devices, as they provide seamless and pervasive connectivity. Thus, security, particularly authentication with limited computational resources on a dynamic platform, is the primary requirement. Traditional complex cryptosystems are inappropriate for low-cost IoT devices because the risk of attacks and eavesdropping by unauthorized entities is too high [156].

One of the downsides of conventional security methods is that credentials compromised by malicious users may be considered to be legitimate and authorized. Since the upper layers may, thus, be accessed illegitimately, it is too hard to deploy PHY-layer authentication from such layers to end IoT devices. However, strong and efficient end-device security can be achieved if there is coordination between PHY-layer authentication and asymmetric cryptosystems [156]. Over the last decade, the number of mIoT devices has increased fivefold, which not only has revolutionized the whole world but also raised several security questions.

The authors in [157] proposed a blockchain-based security architecture for IoT devices to augment the authentication of relevant applications. Named data networking (NDN) is an emerging technology that discovers and delivers data gathered from mIoT devices, intelligently and effectively, for various applications. However, security, specifically authentication, is a major challenge for NDN-IoT platforms. To remedy these critical issues, a cross-combination of an NDN-packet-based signature and a PHY-layer identity has been built to validate and provide strong authentication of resource-poor end IoT devices [156].

Due to the dynamic trends and massive amounts of data generated by IoT devices, it is very easy for an attacker to replicate or change a device or manipulate the data. Because of the high mobility of the wireless link in IoT, it is necessary to cross-correlate message authentication as well as device attestation and testing [158]. Thus, a hybrid device- and data-dependent PHY-layer approach for authentication based on a dynamic device-specific key generation mechanism has been developed. The remarkable progress in both 5G and IoT technologies has enriched the role of D2D communications in mobile networks. D2D communications play a pivotal role by supporting a direct and resource-efficient environment for 5G applications [159,160]. However, despite the many benefits and the remarkable future of D2D technology, because of the dynamic behavior of wireless links and the heterogeneous platform, security, in particular, is a critical challenge. By carefully analyzing the features of portable devices, a secure certificate-less authentication approach may become significant [106].

Innovative tools are key enablers for achieving high storage and good data management with significant performance at low cost in healthcare applications. E-health clouds are promising for ensuring the continuous availability and accessibility of medical data, such as for monitoring remote patients [102]. The storage of large amounts of data poses a high risk from adversaries, so authenticating devices is a key concern for healthcare applications. Several IdM and authentication methods, for instance, smart cards, passwords, and biometrics have been adopted to provide strong security [102]. The fast-growing trends and flexible features of IoT mean that it has good potential for various applications, including smart healthcare, smart cities, and smart agriculture.

The authors of Ref. [161] proposed a lightweight intrusion detection mechanism using a WiFi Pineapple and Raspberry Pis. Through extensive testing on software and hardware platforms, they found that their proposed system outperformed conventional strategies with a higher throughput, shorter delay, and stronger security [161]. A cellular network with a fog-computing mechanism was proposed for securing sensors and IoT-enabled cyber–physical systems. The same authors noted that security was vital for edge nodes and core networks [153].

Due to the diversity of services and devices in next-generation networks, autonomous decision-making for security, especially policy verification, converting a policy to a configuration, and subsequent deployment, can be achieved with AI [123,162,163]. A stringent requirement of IoT-5G healthcare applications is latency. Authentication and access control need to be proactively carried out within the time constraints to meet the main service requirements, such as when migrating a service from one edge node to another. AI can play a critical role in the timely identification of terminal actions and requirements to avoid service interruptions [164].

The most prominent use of AI for IoT-5G healthcare devices is authenticating legitimate users and recognizing malicious traffic. Thus, AI has a key role in identifying intruders in healthcare applications [113,165,166]. AI can detect malware during D2D and device-to-server communications. Therefore, strong authentication is provided to healthcare applications through IoT-5G devices [118]. Besides, AI is a cornerstone in limiting access by illegitimate actors to the sensitive information collected by IoT-5G devices [139]. The effective and well-known fuzzy and artificial neural networks are important for identifying malicious devices and authenticating legitimate entities [5,142,163].

AI has attracted significant attention from researchers in different fields, especially healthcare when diagnosing patients [24,29,99]. For example, AI-enabled agents can identify illegitimate entities effectively and accurately [97,167]. Besides, TensorFlow has various AI libraries and open-source tools for identifying malicious users [23].

5. Discussion and future research directions

AI is an impressive and adaptive way to provide strong and better authentication of IoT-5G devices. Conventional authentication is static and computationally complex, as it does not utilize AI. Thus, there is a huge demand for adaptive and intelligent authentication strategies. Besides, strong authentication is urgently needed for IoT-5G wearable devices used for healthcare applications [14]. Details of AI methods and their importance from different aspects are presented in Table 3.

Much previous research has considered using AI only for resource optimization, such as reducing delays and increasing reliability, or for enhancing general security. In contrast, authentication for IoT-5G wearable devices for healthcare has not been addressed [116,168]. Due to wearable devices' dynamic and portable features and their advanced and effective data collection abilities, good authentication is necessary [29,119]. Fig. 8 demonstrates the components of the discussion and the future research directions.

5.1. AI for MAC

Basing authentication for IoT-5G devices on MAC is essential for identifying illegitimate entities in healthcare applications. Duty-cycle optimization with a central device, such as at a hospital, increases the vulnerability of sensitive patient information. Thus, intelligent authentication is necessary [169,170]. It is difficult to manage and monitor a large number of devices in the MAC layer. Besides, authentication and resource allocation need more time [31,114].

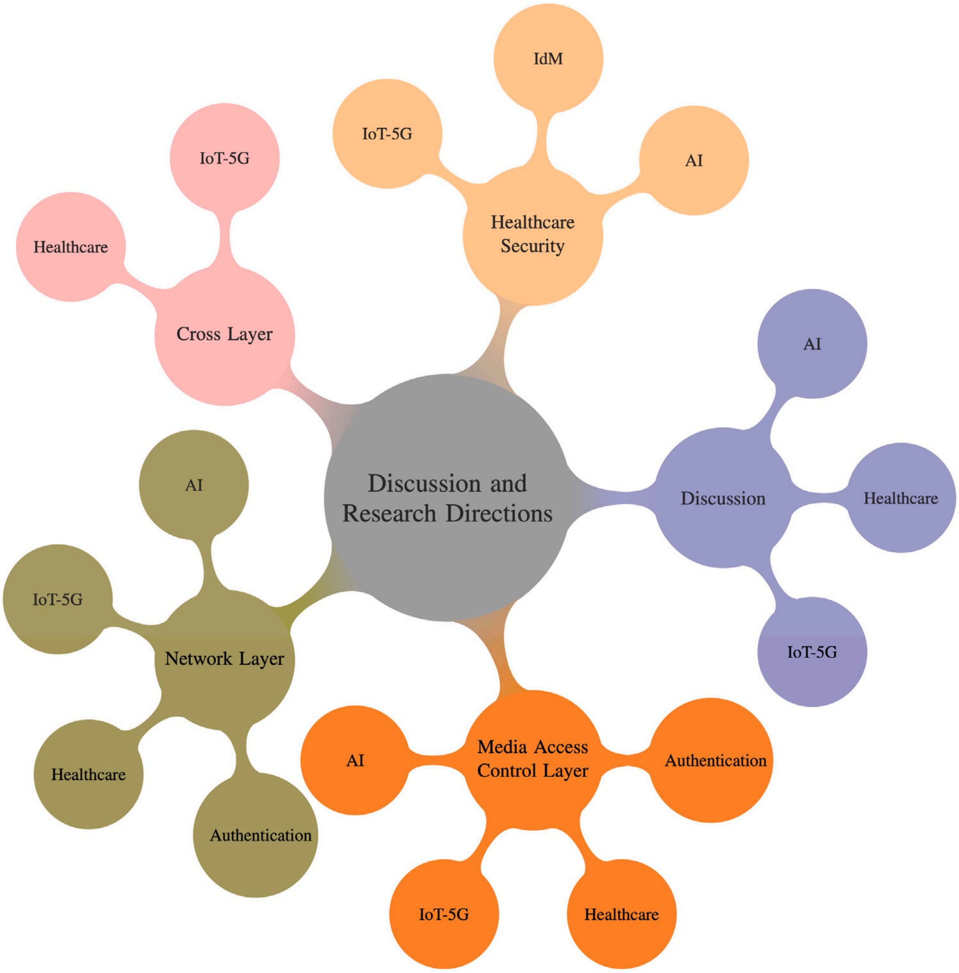


Fig. 8. Mind map illustrating the discussion elements and the future research directions.

Intelligent authentication and effective resource allocation are necessary for IoT-5G devices in healthcare applications because sensitive data need a higher degree of protection from intruders [49]. The high mobility of IoT-5G devices not only weakens security but also compromises reliability. Thus, AI could be used to detect unwanted and highly alarming conditions in healthcare applications [32,147]. Moreover, AI can enhance the authentication of IoT-5G devices used for healthcare applications [171].

5.2. AI for the network layer

An IoT-5G network relies on an impressive and compatible trade-off in the use of AI for strong authentication for healthcare applications. There are various problems in authenticating legitimate users, but two important ones are addressed here [33,172]. First, the control plane must be monitored and authenticated because it is the core part of the entire network. Second, there has to be a close relation between the network control panel and the distributed network control framework [3,173]. Most network features have manually set parameters and weak authentication. Thus, it is vital to adopt AI methods to strengthen authentication in IoT-5G healthcare applications. There are clear and insightful consequences for not doing so. For example, it is challenging to modify network rules based on network status when authenticating IoT-5G devices. Second, a traditional network is complex, so that authentication is inaccurate and weak. Third, emerging AI techniques provide better authentication and resource allocation of IoT-5G wearable devices for healthcare applications [34,43,73,174]. To mitigate the aforementioned issues, it is vital to adopt intelligent authentication for healthcare [7,14,29]. The most recent application, which is still a high research focus, is based on IoT-5G massive multiple-input and multiple-output (MIMO), mMTC, and URLLC. Their practical deployment is known as OpenFlow [167].

AI is not only a key part of centralized and decentralized networks but also plays a major role in routing protocols and their decision-making, such as for mobile ad hoc networks. Due to the random and mobile behavior of IoT devices, it is easier for an intruder to leak sensitive information [35,175]. Hence, AI is important for detecting illegitimate actors and properly authenticating IoT-5G devices due to its better decision-making ability. Furthermore, devices join or leave a 5G network, which creates opportunities for illegitimate actors to access private information without permission. Thus, AI authentication is essential [176–178].

5.3. AI for the cross layer

The vertical integration of network systems from the physical layer to the application layer has been a major focus of research, which considers the connections among network entities in the various layers [37,179]. One approach has been to use a cross layer due to several challenges with the isolated layers [36,166]. Different protocols often make different assumptions about each layer, which may not result in a global optimum or work well with the assumptions for other layers, resulting in what is called the best-effort service [43,180]. Some advances in new wireless access technologies and dynamic networks require cooperation among all the layers for many reasons, such as scheduling, congestion control, and routing [73]. Therefore, there are many cross-layer approaches and design proposals, as described in [39]. However, the current approaches exacerbate the complexity of the overall system and increase the network overhead, especially for dynamic networks.

There have been several proposals for enabling cognition in IoT-5G healthcare devices, which would introduce intelligence and cooperative decision-making among all the layers [23]. Cognitive networks perceive the current state of the network, learn, and act according to end-to-end goals [181]. However, there are many challenges in realizing cognition throughout a network. For example, cognitive networks need perceptive radios that can actively and continuously sense the environment so that they can learn and adapt to the environment (e.g., by switching to a specific frequency band). The main challenges with such systems are that adjusting the MAC and network layer parameters, for example, for scheduling and routing, still requires cross-layer approaches [26].

Recently, new architectures that disintegrate the vertical layering of OSI by separating the control and data planes have been proposed [157]. The most common implementation of IoT-5G (i.e., network slicing and OpenFlow) mitigates the need for cross-layer interactions and facilitates innovation in each layer independently. The split architecture allows the functions of a radio access network to be performed in the cloud (e.g., CloudRAN). Thus, radio resource scheduling and carrier sensing can be performed together, which is an example of efficient cooperation among the layers. Using AI for such purposes still needs further investigation, but there has been no major research work on this topic. Similarly, using AI and authentication of IoT-5G devices for healthcare to increase cooperation among various functions in the network needs additional research.

5.4. AI for 5G-enabled healthcare security

As already noted, IdM based on USIM has been adopted by conventional cellular networks [44]. However, this approach is unsuitable for IoT-5G devices because information can leak out during authentication. One of the limitations of basing IdM on USIM cards is that most wearable devices are not compatible with USIM cards. Moreover, this method fails to provide security to multiple devices when they are simultaneously accessing a cloud server [31]. The weak security provided by traditional methods affects the privacy of patients using healthcare applications. IdM does not effectively fulfill the security and privacy-preserving requirements of patients [17,99].

Federated and centralized versions of IdM have been designed to enhance the security of IoT-enabled portable devices [182]. A security analysis found that orthodox IdM and all its versions were inadequate due to their limited control and weak authentication [142]. UDM has been adopted by 5G networks for managing user data and profiles in both fixed and mobile access networks [54]. The dynamic behavior of UDM is superior to that of IdM, making it suitable for healthcare applications. To achieve the above requirements, AI could make effective decisions using the massive amount of data generated by a large number of IoT devices. AI can analyze data to extract patterns to give a better understanding of the network and improve the performance of end devices. The need for AI in future applications of IoT-5G healthcare has been discussed by following Kipling's method [55].

5.5. AI for mIoT

The intelligent authentication of IoT-5G wearable devices in healthcare is a paradigm shift. An mIoT has a large number of lightweight portable devices communicating D2D. The mIoT is structured independently, and the mutual coordination of devices is a basic form of integrating or establishing a connection between devices for simple tasks, such as monitoring elderly or emergency patients in distant locations [183,184].

When designing AI-based solutions for mIoT, special emphasis must be put on collaborative learning and on the adaptive optimization of computing and caching resources when handling huge amounts of raw data [28,47]. Moreover, the main future research directions on using AI for mIoT include latency-sensitive and lightweight learning mechanisms, as well as giving IoT devices intelligent sensing and decision-making capabilities [24,185]. For end-to-end communications, mIoT will require cross-layer collaboration. Therefore, it would be interesting to investigate whether AI can improve cross-layer communications for an mIoT [186,187]. Due to power constraints, mIoT devices simply transmit data without performing any heavy computation, such as encryption or compression. Thus, the upper layers must cooperate to adaptively encrypt or compress the data, which means they have to understand the need for such actions. Similarly, a method for selecting a topology based on node mobility by extracting mobility information from physical layer parameters is still needed [24]. Accordingly, AI methods are needed to synchronize the operation of all layers, not only to minimize the challenges faced by mIoT but to facilitate the end-to-end communication between mIoT devices [58,188].

Two important roles of AI in mIoT and 5G are to authenticate lightweight devices and to fairly allocate resources to healthcare applications. The main task of AI in IoT-5G is to ensure a high level of authentication when devices are performing tasks such as sensing and processing or transmitting data [27,189]. There may be critical problems when transmitting data through large devices or machines. Moreover, due to the heterogeneous nature of devices and the huge data volumes, it can be challenging to enforce synchronization between devices when they are performing such tasks [190,191]. Besides, AI has promise as a synchronization platform and for enhancing connectivity for resource-constrained devices (with relatively higher power consumption but shorter battery lifetimes) [192,193].

Another critical issue is the large overhead during synchronization between devices, as rapid convergence is required among devices [28,194]. Also, it is necessary to deal with the short battery lifetimes and higher power consumption of devices when transmitting data [15,62,195,196]. In addition, selecting the right technologies impacts the coverage, battery lifetime, and costs, unlike orthodox LTE networks [18,22].

Choosing the right combination of technologies depends upon the network plans set out by the operators, the coverage pattern, and the unique use cases [19,197]. Cat-M is complementary to other technologies, as it has additional capabilities. It is designed to support the efficient coexistence of mobile broadband and IoT traffic. Using an mIoT radio access network in combination with the core IoT network enables the separation of resources for mobile broadband and IoT as well as the flexibility and scalability needed for the predicted growth of IoT [20,21]. AI-based mIoT has better capabilities for managing, monitoring, configuring, allocating, diagnosing, and optimizing the operation and outcomes of a network adaptively and intelligently [65,198].

6. Conclusions

The compatibility of 5G and IoT strengthens the scope and vitality of healthcare applications. IoT-enabled devices can cooperate and communicate with high efficiency and less interference without the involvement of BSs and access points due to the unique and intelligent features of 5G. Authenticating 5G healthcare devices is still a critical challenge, especially with the rapid advances. Besides, the resource limitations of small and lightweight IoT devices, the weaker authentication and IdM, and their high mobility significantly increase the risk of eavesdropping and illegitimate access. IoT-5G devices require more power for processing, sensing, communicating, and monitoring when exchanging data. However, the transmission of data between devices over a wireless link can lead to security threats, such as information leakage. Transmitting data consumes more energy and shortens battery lifetimes of critical healthcare applications.

For various IoT-5G applications, such as healthcare, massive amounts of data can be gathered from devices anywhere at anytime. The dynamic nature of wireless connections and the high mobility of devices put the entire network at the risk of a spoofing attack, especially if IoT-enabled wearable devices are used in a medical or home environment. IoT devices require strong IdM and intelligent authentication. Thus, identifying the right authentication model for 5G-IoT healthcare devices remains a challenging problem.

Authentication is of paramount importance for IoT-5G devices because they directly impact personalized healthcare services and medical appliances. 5G integrates and supports millions of devices that have an inadequate built-in security plus various new devices. The high computing power of these devices makes them an easy target for attackers and hackers. The authentication of 5G healthcare devices has recently attracted increased interest. More research is expected on blockchain-based security and frameworks for telemedicine and telehealthcare. A combination of AI with a blockchain can be built for distributed security management in 5G and beyond networks, which could provide intelligent and autonomous healthcare services.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Co-author, Ali Ismail Awad, is an Editorial Board Member (EBM) or the Internet of Things; Engineering Cyber Physical Human Systems Journal.

Acknowledgment

This work has been partially funded by Kempe Stiftelsern.

References

[1] K.N. Lal, A. Kumar, E-health application over 5G using Content-Centric networking (CCN), in: 2017 International Conference on IoT and Application, ICIOT, IEEE, 2017, pp. 1–5.

[2] R.K. Lomotey, R. Deters, Middleware-enabled mobile framework in m-Health, in: 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing, IEEE, 2013, pp. 1–8.

[3] R.I. Ansari, C. Chrysostomou, S.A. Hassan, M. Guizani, S. Mumtaz, J. Rodriguez, J.J. Rodrigues, 5G D2D networks: Techniques, challenges, and future prospects, IEEE Syst. J. 12 (4) (2017) 3970–3984.

[4] M.Z. Chowdhury, M.T. Hossan, M. Shahjalal, M.K. Hasan, Y.M. Jang, A new 5G e-health architecture based on optical camera communication: An overview, prospects, and applications, IEEE Consum. Electron. Mag. (2020).

[5] M.E.M. Cayamcela, W. Lim, Artificial intelligence in 5G technology: A survey, in: 2018 International Conference on Information and Communication Technology Convergence, ICTC, IEEE, 2018, pp. 860–865.

[6] Y. Liu, M. Peng, G. Shou, Y. Chen, S. Chen, Towards edge intelligence: Multi-access edge computing for 5G and Internet of Things, IEEE Internet Things J. 7 (8) (2020) 6722–6747.

[7] D. Li, 5G and intelligence medicine—how the next generation of wireless technology will reconstruct healthcare? Precis. Clin. Med. 2 (4) (2019) 205–208.

[8] M.N. Tehrani, M. Uysal, H. Yanikomeroglu, Device-to-Device communication in 5G cellular networks: challenges, solutions, and future directions, IEEE Commun. Mag. 52 (5) (2014) 86–92.

[9] S. Din, A. Paul, A. Ahmad, S. Rho, Emerging mobile communication technologies for healthcare system in 5G network, in: 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), IEEE, 2016, pp. 47–54.

[10] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, J.J. Rodrigues, Tactile Internet for smart communities in 5G: An insight for NOMA-based solutions, IEEE Trans. Ind. Inf. 15 (5) (2019) 3104–3112.

[11] H.H. Hussein, H.A. Elsayed, S.M. Abd El-kader, Intensive benchmarking of D2D communication over 5G cellular networks: prototype, integrated features, challenges, and main applications, Wirel. Netw. (2019) 1–20.

[12] Z. Rayan, M. Alfonse, A.-B.M. Salem, Machine learning approaches in smart health, Procedia Comput. Sci. 154 (2019) 361–368.

[13] F. Ghavimi, H.-H. Chen, M2M communications in 3GPP LTE/LTE-A networks: Architectures, service requirements, challenges, and applications, IEEE Commun. Surv. Tutor. 17 (2) (2014) 525–549.

[14] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead, IEEE J. Sel. Areas Commun. 36 (4) (2018) 679–695.

[15] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, M.A. Javed, A survey of device-to-device communications: Research issues and challenges, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2133–2168.

[16] P. Hao, X. Wang, W. Shen, A collaborative PHY-aided technique for end-to-end IoT device authentication, IEEE Access 6 (2018) 42279–42293.

[17] M.F. Elrawy, A.I. Awad, H.F. Hamed, Intrusion detection systems for IoT-based smart environments: a survey, J. Cloud Comput. 7 (1) (2018) 21.

[18] M. Mezzavilla, M. Zhang, M. Polese, R. Ford, S. Dutta, S. Rangan, M. Zorzi, End-to-end simulation of 5G mmWave networks, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2237–2263.

[19] I. Parvez, A. Rahmati, I. Guvenc, A.I. Sarwat, H. Dai, A survey on low latency towards 5G: RAN, core network and caching solutions, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3098–3130.

[20] Q. Mao, F. Hu, Q. Hao, Deep learning for intelligent wireless networks: A comprehensive survey, IEEE Commun. Surv. Tutor. 20 (4) (2018) 2595–2621.

[21] C.-X. Wang, J. Bian, J. Sun, W. Zhang, M. Zhang, A survey of 5G channel measurements and models, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3142–3168.

[22] J. Hu, K. Yang, G. Wen, L. Hanzo, Integrated data and energy communication network: A comprehensive survey, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3169–3219.

[23] T. Sigwele, Y.F. Hu, M. Ali, J. Hou, M. Susanto, H. Fitriawan, Intelligent and energy efficient mobile smartphone gateway for healthcare smart devices based on 5G, in: 2018 IEEE Global Communications Conference, GLOBECOM, IEEE, 2018, pp. 1–7.

[24] A. Aldaej, U. Tariq, IoT in 5G Aeon: An inevitable fortuity of next generation healthcare, in: 2018 1st International Conference on Computer Applications & Information Security, ICCAIS, IEEE, 2018, pp. 1–4.

[25] A.I. Awad, S. Furnell, M. Paprzycki, S.K. Sharma, Security in Cyber-Physical Systems: Foundations and Applications, Springer, 2021.

[26] C.M. Moreira, G. Kaddoum, E. Bou-Harb, Cross-layer authentication protocol design for ultra-dense 5G HetNets, in: 2018 IEEE International Conference on Communications, IEEE, 2018, pp. 1–7.

[27] J.M. McGinthy, L.J. Wong, A.J. Michaels, Groundwork for neural network-based specific emitter identification authentication for IoT, IEEE Internet Things J. 6 (4) (2019) 6429–6440.

[28] S.K. Sharma, X. Wang, Toward massive machine type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions, IEEE Commun. Surv. Tutor. 22 (1) (2019) 426–471.

[29] M. El-hajj, A. Fadlallah, M. Chamoun, A. Serhrouchni, A survey of Internet of Things authentication schemes, Sensors 19 (5) (2019) 1141.

[30] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J.J. Ramos-Munoz, J.M. Lopez-Soler, A survey on 5G usage scenarios and traffic models, IEEE Commun. Surv. Tutor. 22 (2) (2020) 905–929.

[31] F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: current solutions and future challenges, IEEE Commun. Surv. Tutor. (2020).

[32] N. Slamnik-Kriještorac, H. Kremo, M. Ruffini, J.M. Marquez-Barja, Sharing distributed and heterogeneous resources toward end-to-end 5G networks: A comprehensive survey and a taxonomy, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1592–1628.

[33] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. ur Rasool, W. Dou, Complementing IoT services through software defined networking and edge computing: A comprehensive survey, IEEE Commun. Surv. Tutor. (2020).

[34] L. Lei, Y. Tan, K. Zheng, S. Liu, K. Zhang, X. Shen, Deep reinforcement learning for autonomous internet of things: Model, applications and challenges, IEEE Commun. Surv. Tutor. (2020).

[35] K. Gai, J. Guo, L. Zhu, Blockchain meets cloud computing: A survey, IEEE Commun. Surv. Tutor. (2020).

[36] M.A. Arfaoui, M.D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. Assi, H. Haas, Physical layer security for visible light communication systems: A survey, IEEE Commun. Surv. Tutor. (2020).

[37] W.Y.B. Lim, N.C. Luong, D.T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, C. Miao, Federated Learning in mobile edge networks: A comprehensive survey, IEEE Commun. Surv. Tutor. (2020).

[38] P.K. Sharma, J. Park, J.H. Park, K. Cho, Wearable computing for defence automation: Opportunities and challenges in 5G network, IEEE Access 8 (2020) 65993–66002.

[39] S. Sicari, A. Rizzardi, A. Coen-Porisini, 5G in the Internet of Things era: an overview on security and privacy challenges, Comput. Netw. (2020) 107345.

[40] M. Mamdouh, A.I. Awad, A.A. Khalaf, H.F. Hamed, Authentication and identity management of IoHT devices: Achievements, challenges, and future directions, Comput. Secur. 111 (2021) 102491, http://dx.doi.org/10.1016/j.cose.2021.102491.

[41] D.C. Nguyen, M. Ding, P.N. Pathirana, A. Seneviratne, J. Li, H. Vincent Poor, Federated learning for internet of things: A comprehensive survey, IEEE Commun. Surv. Tutor. 23 (3) (2021) 1622–1658, http://dx.doi.org/10.1109/COMST.2021.3075439.

[42] A. Pundziene, S. Heaton, D.J. Teece, 5G, dynamic capabilities and business models innovation in healthcare industry, in: 2019 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE), IEEE, 2019, pp. 1–8.

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

[44] D. Fang, F. Ye, Identity management framework for E-Health systems over 5G networks, in: 2018 IEEE International Conference on Communications, ICC, IEEE, 2018, pp. 1–6.

[45] B. Mohanta, P. Das, S. Patnaik, Healthcare 5.0: A paradigm shift in digital healthcare system using Artificial Intelligence, IoT and 5G communication, in: 2019 International Conference on Applied Machine Learning, ICAML, IEEE, 2019, pp. 191–196.

[46] D. Soldani, F. Fadini, H. Rasanen, J. Duran, T. Niemela, D. Chandramouli, T. Hoglund, K. Doppler, T. Himanen, J. Laiho, et al., 5G mobile systems for healthcare, in: 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), IEEE, 2017, pp. 1–5.

[47] D. Nouichi, M. Abdelsalam, Q. Nasir, S. Abbas, IoT devices security using RF fingerprinting, in: 2019 Advances in Science and Engineering Technology International Conferences, ASET, IEEE, 2019, pp. 1–7.

[48] A. Markhasin, Fundamentals of the extremely green, flexible, and profitable 5G M2M ubiquitous communications for remote e-healthcare and other social e-applications, in: 2017 International Multi-Conference on Engineering, Computer and Information Sciences, SIBIRCON, IEEE, 2017, pp. 292–297.

[49] M. Noura, R. Nordin, A survey on interference management for device-to-device (D2D) communication and its challenges in 5G networks, J. Netw. Comput. Appl. 71 (2016) 130–150.

[50] M.I. Mamun, A. Rahman, M.A. Khaleque, M.A. Hamid, M.F. Mridha, AutiLife: A healthcare monitoring system for autism center in 5G cellular network using machine learning approach, in: 2019 IEEE 17th International Conference on Industrial Informatics, INDIN, vol. 1, IEEE, 2019, pp. 1501–1506.

[51] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P.K. Nakarmi, M. Näslund, P. O'Hanlon, et al., A security architecture for 5G networks, IEEE Access 6 (2018) 22466–22479.

[52] A. Alzubaidi, J. Kalita, Authentication of smartphone users using behavioral biometrics, IEEE Commun. Surv. Tutor. 18 (3) (2016) 1998–2026.

[53] M.I. Mamun, A. Rahman, M.A. Khaleque, M.F. Mridha, M.A. Hamid, Healthcare monitoring system inside self-driving smart car in 5G cellular network, in: 2019 IEEE 17th International Conference on Industrial Informatics, INDIN, vol. 1, IEEE, 2019, pp. 1515–1520.

[54] R. Shekhar, A. Ghosh, S. Chandra, H.J. La Roche, I.M. Campbell, Methods and apparatus for use in reducing signal latency in a mobile network with use of localized unified data management (UDM) entities, 2020, US Patent 10, 555, 165.

[55] W.D. de Mattos, P.R. Gondim, M-health solutions using 5G networks and M2M communications, IT Prof. 18 (3) (2016) 24–29.

[56] M.A. Azad, S. Bag, C. Perera, M. Barhamgi, F. Hao, Authentic caller: Self-enforcing authentication in a next-generation network, IEEE Trans. Ind. Inf. 16 (5) (2019) 3606–3615.

[57] K. Madiha, Tahir, Cryptanalysis of radio frequency identification system mutual authentication protocol, in: 2019 2nd International Conference on Communication, Computing and Digital Systems (C-CODE), IEEE, 2019, pp. 258–263.

[58] Y. Huang, W. Wang, H. Wang, T. Jiang, Q. Zhang, Authenticating on-body IoT devices: An adversarial learning approach, IEEE Trans. Wireless Commun. (2020).

[59] M. Ghahramani, R. Javidan, M. Shojafar, RSS: An energy-efficient approach for securing IoT service protocols against the DoS attack, IEEE Internet Things J. (2020).

[60] S.A. Hamad, Q.Z. Sheng, W.E. Zhang, S. Nepal, Realizing an Internet of Secure Things: A survey on issues and enabling technologies, IEEE Commun. Surv. Tutor. 22 (2) (2020) 1372–1391.

[61] H. Huang, L. Hu, J. Chu, X. Cheng, An authentication scheme to defend against UDP DrDoS in 5G networks, IEEE Access 7 (2019) 175970–175979.

[62] P.V. Klaine, M.A. Imran, O. Onireti, R.D. Souza, A survey of machine learning techniques applied to self-organizing cellular networks, IEEE Commun. Surv. Tutor. 19 (4) (2017) 2392–2431.

[63] J. Tang, A. Xu, Y. Jiang, Y. Zhang, H. Wen, T. Zhang, MmWave, MIMO physical layer authentication by using channel sparsity, in: 2020 IEEE International Conference on Artificial Intelligence and Information Systems, ICAIIS, IEEE, 2020, pp. 221–224.

[64] J. Li, Z. Zhang, L. Hui, Z. Zhou, A novel message authentication scheme with absolute privacy for the IoT networks, IEEE Access 8 (2020) 39689–39699.

[65] I. Ahmed, H. Khammari, A. Shahid, A. Musa, K.S. Kim, E. De Poorter, I. Moerman, A survey on hybrid beamforming techniques in 5G: Architecture and system model perspectives, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3060–3097.

[66] E. Okoh, A.I. Awad, Biometrics applications in e-health security: A preliminary survey, in: International Conference on Health Information Science, Springer, 2015, pp. 92–103.

[67] Q. Wang, J. Alcaraz-Calero, R. Ricart-Sanchez, M.B. Weiss, A. Gavras, N. Nikaein, X. Vasilakos, B. Giacomo, G. Pietro, M. Roddy, et al., Enable advanced QoS-aware network slicing in 5G networks for slice-based media use cases, IEEE Trans. Broadcast. 65 (2) (2019) 444–453.

[68] Z. Haddad, M.M. Fouda, Blockchain-based authentication for 5G networks, in: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), IEEE, 2020, pp. 189–194.

[69] S. Gupta, B.L. Parne, Security vulnerabilities in handover authentication mechanism of 5G network, in: 2018 First International Conference on Secure Cyber Computing and Communication, ICSCCC, IEEE, 2018, pp. 369–374.

[70] S.A. Bruendl, H. Fang, Making the switch to 5G and 60 GHz in mHealth applications using USRP hardware, IEEE Internet Comput. 24 (2) (2019) 57–64.

[71] Y. Li, Y. Liu, X. Zhao, Study on wearable antenna arrangement for intelligent healthcare management, in: 2018 International Applied Computational Electromagnetics Society Symposium-China, ACES, IEEE, 2018, pp. 1–2.

[72] E. Kapassa, M. Touloupou, A. Mavrogiorgou, A. Kiourtis, D. Giannouli, K. Katsigianni, D. Kyriazis, An innovative e-Health system powered by 5G network slicing, in: 2019 Sixth International Conference on Internet of Things: Systems, Management and Security, IOTSMS, IEEE, 2019, pp. 7–12.

[73] H. Ullah, N.G. Nair, A. Moore, C. Nugent, P. Muschamp, M. Cuevas, 5G communication: an overview of vehicle-to-everything, drones, and healthcare use-cases, IEEE Access 7 (2019) 37251–37268.

[74] D. Lin, S. Hu, Y. Gao, Y. Tang, Optimizing MEC networks for healthcare applications in 5G communications with the authenticity of users' priorities, IEEE Access 7 (2019) 88592–88600.

[75] M.S. Hossain, G. Muhammad, Emotion-aware connected healthcare big data towards 5G, IEEE Internet Things J. 5 (4) (2017) 2399–2406.

[76] M.A. Usman, N.Y. Philip, C. Politis, 5G enabled mobile healthcare for ambulances, in: 2019 IEEE Globecom Workshops (GC Wkshps), IEEE, 2019, pp. 1–6.

[77] J. Xingzhong, X. Qingshui, M. Haifeng, C. Jiageng, Z. Haozhi, The research on identity authentication scheme of IoT equipment in 5G network environment, in: 2019 IEEE 19th International Conference on Communication Technology, ICCT, IEEE, 2019, pp. 312–316.

[78] S. Behrad, E. Bertin, S. Tuffin, N. Crespi, 5G-SSAAC: Slice-specific authentication and access control in 5G, in: 2019 IEEE Conference on Network Softwarization (NetSoft), IEEE, 2019, pp. 281–285.

[79] D. Loghin, S. Cai, G. Chen, T.T.A. Dinh, F. Fan, Q. Lin, J. Ng, B.C. Ooi, X. Sun, Q.-T. Ta, et al., The disruptions of 5G on data-driven technologies and applications, 2019, arXiv preprint arXiv:1909.08096.

[80] J. Wang, J. Liu, N. Kato, Networking and communications in autonomous driving: A survey, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1243–1274.

[81] M.I. Ayadi, F.Z. Saadaoui, A. Maizatc, M. Ouzzif, C. Mahmoudi, Deep learning for packet forwarding with an application for real time IoT, in: 2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), IEEE, 2018, pp. 142–148.

[82] E.M. Torroglosa-Garcia, J.M.A. Calero, J.B. Bernabe, A. Skarmeta, Enabling roaming across heterogeneous IoT Wireless Networks: LoRaWAN meets 5G, IEEE Access (2020).

[83] M.T. Khorshed, N.A. Sharma, K. Kumar, M. Prasad, A.S. Ali, Y. Xiang, Integrating Internet of Things with the power of cloud computing and the intelligence of Big Data analytics—A three layered approach, in: Computer Science and Engineering (APWC on CSE), 2015 2nd Asia-Pacific World Congress on, IEEE, 2015, pp. 1–8.

[84] A.H. Sodhro, S. Pirbhulal, A.K. Sangaiah, Convergence of IoT and product lifecycle management in medical health care, Future Gener. Comput. Syst. (2018).

[85] A.A. Osuwa, E.B. Ekhoragbon, L.T. Fat, Application of artificial intelligence in Internet of Things, in: 2017 9th International Conference on Computational Intelligence and Communication Networks, IEEE, 2017, pp. 169–173.

[86] Z. Song, K. Yao, The design and implementation of mobile intelligent terminal guide system based on the Internet of Things, in: Computational Intelligence and Design (ISCID), 2014 Seventh International Symposium on, Vol. 1, IEEE, 2014, pp. 133–137.

[87] M.S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, A.P. Sheth, Machine learning for Internet of Things data analysis: A survey, Digit. Commun. Netw. (2017).

[88] T. Park, N. Abuzainab, W. Saad, Learning how to communicate in the Internet of Things: Finite resources and heterogeneity, IEEE Access 4 (2016) 7063–7073.

[89] H. Green, The Internet of Things in the Cognitive Era: Realizing the Future and Full Potential of Connected Devices, Ed: IBM Watson IoT, 2015.

[90] J. Tang, D. Sun, S. Liu, J.-L. Gaudiot, Enabling deep learning on IoT devices, Computer 50 (10) (2017) 92–96.

[91] H. Fang, A. Qi, X. Wang, Fast authentication and progressive authorization in large-scale IoT: how to leverage Artificial Intelligence for security enhancement, IEEE Netw. 34 (3) (2020) 24–29.

[92] A. Aadhityan, A novel method for implementing Artificial Intelligence, cloud and Internet of Things in robots, in: Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on, IEEE, 2015, pp. 1–4.

[93] A. Poniszewska-Maranda, D. Kaczmarek, Selected methods of Artificial Intelligence for IoT conception, in: Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on, IEEE, 2015, pp. 1343–1348.

[94] S. Earley, Analytics, machine learning, and the Internet of Things, IT Prof. 17 (1) (2015) 10–13.

[95] B. Nathani, R. Vijayvergia, The Internet of Intelligent things: An overview, in: Intelligent Communication and Computational Techniques (ICCT), 2017 International Conference on, IEEE, 2017, pp. 119–122.

[96] A.H. Sodhro, S. Pirbhulal, A.K. Sangaiah, S. Lohano, G.H. Sodhro, Z. Luo, 5G-based Transmission Power Control mechanism in fog computing for IoT devices, Sustainability 10 (4) (2018) 1258.

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

[98] S. Chen, H. Wen, J. Wu, J. Chen, W. Liu, L. Hu, Y. Chen, Physical-layer channel authentication for 5G via Machine Learning algorithm, Wirel. Commun. Mob. Comput. 2018 (2018).

[99] S. Behrad, E. Bertin, Tuffin, C. Noel, A new scalable authentication and access control mechanism for 5G-based IoT, Future Gener. Comput. Syst. 108 (2020) 46–61.

[100] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, A.F. Skarmeta, Secure authentication and credential establishment in narrowband IoT and 5G, Sensors 20 (3) (2020) 882.

[101] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, H. Li, LSAA: A lightweight and secure access authentication scheme for both UEs and mMTC devices in 5G networks, IEEE Internet Things J. (2020).

[102] M.F. Ayub, K. Mahmood, S. Kumari, A.K. Sangaiah, et al., Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology, Digit. Commun. Netw. (2020).

[103] P. Zhang, J. Liu, Y. Shen, H. Li, X. Jiang, Lightweight tag-based PHY-Layer authentication for IoT devices in smart cities, IEEE Internet Things J. 7 (5) (2019) 3977–3990.

[104] U. Kose, An artificial Intelligence perspective on ensuring cyber-assurance for the Internet of Things, in: Cyber-Assurance for the Internet of Things, 2016, p. 249.

[105] M. Mohammadi, A. Al-Fuqaha, S. Sorour, M. Guizani, Deep learning for IoT Big Data and streaming analytics: A survey, IEEE Commun. Surv. Tutor. (2018).

[106] H. Tan, Y. Song, S. Xuan, S. Pan, I. Chung, Secure D2D group authentication employing smartphone sensor behavior analysis, Symmetry 11 (8) (2019) 969.

[107] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, G. Wang, Security and privacy in the medical internet of things: a review, Secur. Commun. Netw. 2018 (2018).

[108] X. Liu, M. Zhao, S. Li, F. Zhang, W. Trappe, A security framework for the internet of things in the future internet architecture, Future Internet 9 (3) (2017) 27.

[109] A. Dey, S. Nandi, M. Sarkar, Security measures in IoT-based 5G networks, in: 2018 3rd International Conference on Inventive Computation Technologies, ICICT, IEEE, 2018, pp. 561–566.

[110] M. Kim, J. Lee, S. Yu, K. Park, Y. Park, Y. Park, A secure authentication and key establishment scheme for wearable devices, in: 2019 28th International Conference on Computer Communication and Networks, ICCCN, IEEE, 2019, pp. 1–2.

[111] M. Yao, M. Sohul, V. Marojevic, J.H. Reed, Artificial intelligence defined 5G radio access networks, IEEE Commun. Mag. 57 (3) (2019) 14–20.

[112] F.-Y. Leu, K.-L. Tsai, H. Susanto, C.-Y. Gu, I. You, A fault tolerant mechanism for UE authentication in 5G networks, Mob. Netw. Appl. (2020) 1–18.

[113] S.B.M. Baskaran, G. Raja, A lightweight incognito key exchange mechanism for LTE-A assisted D2D communication, in: 2017 Ninth International Conference on Advanced Computing, IEEE, 2017, pp. 301–307.

[114] M. Waqas, Y. Niu, Y. Li, M. Ahmed, D. Jin, S. Chen, Z. Han, Mobility-aware device-to-device communications: Principles, practice and challenges, IEEE Commun. Surv. Tutor. (2019).

[115] H. Hejazi, H. Rajab, T. Cinkler, L. Lengyel, Survey of platforms for massive IoT, in: 2018 IEEE International Conference on Future IoT Technologies (Future IoT), IEEE, 2018, pp. 1–8.

[116] R. Li, Z. Zhao, X. Zhou, G. Ding, Y. Chen, Z. Wang, H. Zhang, Intelligent 5G: When cellular networks meet Artificial Intelligence, IEEE Wirel. Commun. 24 (5) (2017) 175–183.

[117] M. Talal, A. Zaidan, B. Zaidan, A. Albahri, A. Alamoodi, O. Albahri, M. Alsalem, C. Lim, K.L. Tan, W. Shir, et al., Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review, J. Med. Syst. 43 (3) (2019) 42.

[118] J. Wang, R. Zhu, S. Liu, A differentially private unscented Kalman filter for streaming data in IoT, IEEE Access 6 (2018) 6487–6495.

[119] K. Guo, Y. Lu, H. Gao, R. Cao, Artificial Intelligence-based semantic Internet of Things in a user-centric smart city, Sensors (Basel, Switzerland) 18 (5) (2018).

[120] N. Soltanieh, Y. Norouzi, Y. Yang, N.C. Karmakar, A review of radio frequency fingerprinting techniques, IEEE J. Radio Freq. Identif. (2020).

[121] Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: Challenges and opportunities, IEEE Commun. Surv. Tutor. 18 (1) (2015) 94–104.

[122] S.U. Rehman, K.W. Sowerby, S. Alam, I. Ardekani, Radio frequency fingerprinting and its challenges, in: 2014 IEEE Conference on Communications and Network Security, IEEE, 2014, pp. 496–497.

[123] B.d.M.P. dos Santos, B. Dzogovic, B. Feng, N. Jacot, T. Van Do, et al., Towards achieving a secure authentication mechanism for IoT devices in 5G networks, in: 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), IEEE, 2019, pp. 130–135.

[124] R. Melki, H.N. Noura, A. Chehab, Lightweight and secure D2D authentication & key management based on PLS, in: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), IEEE, 2019, pp. 1–7.

[125] P. Pawar, A. Trivedi, Device-to-device communication based IoT system: benefits and challenges, IETE Tech. Rev. 36 (4) (2019) 362–374.

[126] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, D. Zheng, Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks, IEEE Access 7 (2019) 114721–114730.

[127] N.N. Santhosh, Future black board using IoT with cognitive computing: Machine learning aspects, in: Communication and Electronics Systems (ICCES), International Conference on, IEEE, 2016, pp. 1–4.

[128] A.H. Sodhro, Z. Luo, A.K. Sangaiah, S.W. Baik, Mobile Edge Computing-based QoS optimization in medical healthcare applications, Int. J. Inf. Manage. 45 (2019) 308–318.

[129] B. Seok, J.C.S. Sicato, T. Erzhena, C. Xuan, Y. Pan, J.H. Park, Secure D2D communication for 5G IoT network based on lightweight cryptography, Appl. Sci. 10 (1) (2020) 217.

[130] P. Yu, J. Cao, M. Ma, H. Li, Quantum-resistance authentication and data transmission scheme for NB-IoT in 3GPP 5G networks, in: 2019 IEEE Wireless Communications and Networking Conference, WCNC, IEEE, 2019, pp. 1–7.

[131] S. Shin, T. Kwon, A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated IoT, IEEE Access 8 (2020) 67555–67571.

[132] J. Cao, P. Yu, X. Xiang, M. Ma, H. Li, Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system, IEEE Internet Things J. 6 (6) (2019) 9794–9805.

[133] B.D. Deebak, F. Al-Turjman, M. Aloqaily, O. Alfandi, An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT, IEEE Access 7 (2019) 135632–135649.

[134] O.A. Sianaki, A. Yousefi, A.R. Tabesh, M. Mahdavi, Internet of Everything and Machine Learning applications: Issues and challenges, in: 2018 32nd International Conference on Advanced Information Networking and Applications Workshops, WAINA, IEEE, 2018, pp. 704–708.

[135] A. Asadi, Q. Wang, V. Mancuso, A survey on Device-to-Device communication in cellular networks, IEEE Commun. Surv. Tutor. 16 (4) (2014) 1801–1819.

[136] M. Yazici, S. Basurra, M. Gaber, Edge Machine Learning: Enabling smart IoT applications, Big Data Cogn. Comput. 2 (3) (2018) 26.

[137] J.-L. Hou, K.-H. Yeh, Novel authentication schemes for IoT based healthcare systems, Int. J. Distrib. Sens. Netw. 11 (11) (2015) 183659.

[138] P. Kumar, S.-G. Lee, H.-J. Lee, E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks, Sensors 12 (2) (2012) 1625–1647.

[139] T. Ma, F. Hu, M. Ma, Securing 5G HetNets using mutual physical layer authentication, in: Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City, 2019, pp. 275–278.

[140] N. Zhang, X. Fang, Y. Wang, S. Wu, H. Wu, D. Kar, H. Zhang, Physical layer authentication for internet of things via WFRFT-based Gaussian tag embedding, IEEE Internet Things J. (2020).

[141] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, C.-H. Tsai, AES-128 based secure low power communication for LoRaWAN IoT environments, IEEE Access 6 (2018) 45325–45334.

[142] S. Gong, A. El Azzaoui, J. Cha, J.H. Park, Secure secondary authentication framework for efficient mutual authentication on a 5G data network, Appl. Sci. 10 (2) (2020) 727.

[143] A. Al Hayajneh, M.Z.A. Bhuiyan, I. McAndrew, et al., Security of broadcast authentication for cloud-enabled wireless medical sensor devices in 5G networks, Comput. Inf. Sci. 13 (2) (2020) 1–13.

[144] S. Rahimi Moosavi, T. Nguyen Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen, SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways, in: Procedia Computer Science, Vol. 52, Elsevier, 2015, pp. 452–459.

[145] M. Hassaballah, M.A. Hameed, A.I. Awad, K. Muhammad, A novel image steganography method for industrial internet of things security, IEEE Trans. Ind. Inf. 17 (11) (2021) 7743–7751, http://dx.doi.org/10.1109/TII.2021.3053595.

[146] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, Y. Lee, A three-factor anonymous user authentication scheme for Internet of Things environments, J. Inf. Secur. Appl. 52 (2020) 102494.

[147] K. Renuka, S. Kumari, X. Li, Design of a secure three-factor authentication scheme for smart healthcare, J. Med. Syst. 43 (5) (2019) 133.

[148] G. Baldini, R. Giuliani, G. Steri, R. Neisse, Physical layer authentication of Internet of Things wireless devices through permutation and dispersion entropy, in: 2017 Global Internet of Things Summit (GIoTS), IEEE, 2017, pp. 1–6.

[149] J. Huang, Y. Qian, R.Q. Hu, Secure and efficient privacy-preserving authentication scheme for 5G software defined vehicular networks, IEEE Trans. Veh. Technol. (2020).

[150] T. Kumar, A. Braeken, A.D. Jurcut, M. Liyanage, M. Ylianttila, AGE: authentication in gadget-free healthcare environments, Inf. Technol. Manag. (2019) 1–20.

[151] R.S.M. Joshitta, L. Arockiam, Device authentication mechanism for IoT-enabled healthcare system, in: 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, ICAMMAET, IEEE, 2017, pp. 1–6.

[152] M.A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, H. Janicke, Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes, J. Netw. Comput. Appl. 101 (2018) 55–82.

[153] F. Sharevski, S. Oteafy, Security for cyber-physical systems: Leveraging cellular networks and fog computing, 2018, arXiv preprint arXiv:1806.11053.

[154] J. Cañedo, A. Skjellum, Using Machine Learning to secure IoT systems, in: Privacy, Security and Trust (PST), 2016 14th Annual Conference on, IEEE, 2016, pp. 219–222.

[155] H. Tan, I. Chung, Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor, IEEE Access 7 (2019) 151459–151474.

[156] P. Hao, X. Wang, Integrating PHY security into NDN-IoT networks by exploiting MEC: Authentication efficiency, robustness, and accuracy enhancement, IEEE Trans. Signal Inf. Process. Netw. 5 (4) (2019) 792–806.

[157] K. Albalawi, M.M.A. Azim, Cloud-based IoT device authentication scheme using blockchain, in: 2019 IEEE Global Conference on Internet of Things (GCIoT), IEEE, 2019, pp. 1–7.

[158] Y. Zheng, S.S. Dhabu, C.-H. Chang, Securing IoT monitoring device using PUF and physical layer authentication, in: 2018 IEEE International Symposium on Circuits and Systems, ISCAS, IEEE, 2018, pp. 1–5.

[159] T.O. Olwal, K. Djouani, A.M. Kurien, A survey of resource management toward 5G radio access networks, IEEE Commun. Surv. Tutor. 18 (3) (2016) 1656–1686.

[160] D. Liu, L. Wang, Y. Chen, M. Elkashlan, K.-K. Wong, R. Schober, L. Hanzo, User association in 5G networks: A survey and an outlook, IEEE Commun. Surv. Tutor. 18 (2) (2016) 1018–1044.

[161] C. Nykvist, M. Larsson, A.H. Sodhro, A. Gurtov, A lightweight portable intrusion detection communication system for auditing applications, Int. J. Commun. Syst. 33 (7) (2020) e4327.

[162] L. Xing, Q. Ma, H. Wu, P. Xie, General multimedia trust authentication framework for 5G networks, Wirel. Commun. Mob. Comput. 2018 (2018).

[163] B. Dzogovic, B. Santos, N. Jacot, B. Feng, T. Van Do, et al., Secure healthcare: 5G-enabled network slicing for elderly care, in: 2020 5th International Conference on Computer and Communication Systems, IEEE, 2020, pp. 864–868.

[164] J. Liu, N. Kato, J. Ma, N. Kadowaki, Device-to-device communication in LTE-advanced networks: A survey, IEEE Commun. Surv. Tutor. 17 (4) (2014) 1923–1940.

[165] T. Bakhshi, S. Shahid, Securing Internet of Bio-Nano Things: ML-Enabled parameter profiling of bio-cyber interfaces, in: 2019 22nd International Multitopic Conference, INMIC, IEEE, 2019, pp. 1–8.

[166] S. Yu, X. Zhang, P. Huang, L. Guo, Secure authentication in cross-technology communication for heterogeneous IoT, in: 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), IEEE, 2019, pp. 1–2.

[167] A. Bartoli, M. Dohler, A. Kountouris, D. Barthel, Advanced security taxonomy for machine-to-machine communications in 5G capillary networks, in: Machine-to-Machine (M2M) Communications, Elsevier, 2015, pp. 207–226.

[168] K. Sultan, H. Ali, Z. Zhang, Big data perspective and challenges in next generation networks, Future Internet 10 (7) (2018) 56.

[169] M.A. Alvarez, U. Spagnolini, Collision vs non-collision distributed time synchronization for dense IoT deployments, in: Communications (ICC), 2017 IEEE International Conference on, IEEE, 2017, pp. 1–6.

[170] C. Sergiou, P. Antoniou, V. Vassiliou, A comprehensive survey of congestion control protocols in wireless sensor networks, IEEE Commun. Surv. Tutor. 16 (4) (2014) 1839–1859.

[171] U. Raza, P. Kulkarni, M. Sooriyabandara, Low power Wide Area Networks: An overview, IEEE Commun. Surv. Tutor. 19 (2) (2017) 855–873.

[172] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, L. Hanzo, Machine learning paradigms for next-generation wireless networks, IEEE Wirel. Commun. 24 (2) (2017) 98–105.

[173] D. Shin, K. Yun, J. Kim, P.V. Astillo, J.-N. Kim, I. You, A security protocol for route optimization in DMM-based smart home IoT networks, IEEE Access 7 (2019) 142531–142550.

[174] V. Sharma, I. You, F. Palmieri, D.N.K. Jayakody, J. Li, Secure and energy-efficient handover in fog networks using blockchain-based DMM, IEEE Commun. Mag. 56 (5) (2018) 22–31.

[175] M. Mohammadi, A. Al-Fuqaha, Enabling cognitive smart cities using Big Data and machine learning: Approaches and challenges, IEEE Commun. Mag. 56 (2) (2018) 94–101.

[176] J. Chin, V. Callaghan, I. Lam, Understanding and personalising smart city services using machine learning, the Internet of Things and Big Data, in: Industrial Electronics (ISIE), 2017 IEEE 26th International Symposium on, IEEE, 2017, pp. 2050–2055.

[177] J. Park, H. Park, Y.-J. Choi, Data compression and prediction using machine learning for Industrial IoT, in: Information Networking (ICOIN), 2018 International Conference on, IEEE, 2018, pp. 818–820.

[178] X.-W. Chen, X. Lin, Big data deep learning: challenges and perspectives, IEEE Access 2 (2014) 514–525.

[179] I. Al-Anbagi, M. Erol-Kantarci, H.T. Mouftah, A survey on cross-layer QoS approaches in WSNs or delay and reliability-aware applications, IEEE Commun. Surv. Tutor. 18 (1) (2014) 525–552.

[180] J. Zuo, C. Dong, S.X. Ng, L.-L. Yang, L. Hanzo, Cross-layer aided energy-efficient routing design for ad hoc networks, IEEE Commun. Surv. Tutor. 17 (3) (2015) 1214–1238.

[181] M. Ahmad, M. Hussain, B. Abbas, O. Aldabbas, U. Jamil, R. Ashraf, S. Asadi, End-to-end loss based TCP congestion control mechanism as a secured communication technology for smart healthcare enterprises, IEEE Access 6 (2018) 11641–11656.

[182] M.A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for Internet of Things security, IEEE Commun. Surv. Tutor. (2020).

[183] A.H. Sodhro, S. Pirbhulal, G.H. Sodhro, A. Gurtov, M. Muzammal, Z. Luo, A joint transmission power control and duty-cycle approach for smart healthcare system, IEEE Sens. J. 19 (19) (2018) 8479–8486.

[184] M. Luvisotto, F. Tramarin, L. Vangelista, S. Vitturi, On the use of LoRaWAN for indoor Industrial IoT applications, Wirel. Commun. Mob. Comput. 2018 (2018).

[185] J. Cao, P. Yu, M. Ma, W. Gao, Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network, IEEE Internet Things J. 6 (2) (2018) 1561–1575.

[186] M.A. Alsheikh, S. Lin, D. Niyato, H.-P. Tan, Machine Learning in wireless sensor networks: Algorithms, strategies, and applications, IEEE Commun. Surv. Tutor. 16 (4) (2014) 1996–2018.

[187] J. Ni, X. Lin, X.S. Shen, Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT, IEEE J. Sel. Areas Commun. 36 (3) (2018) 644–657.

[188] B. Chatterjee, D. Das, S. Maity, S. Sen, RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning, IEEE Internet Things J. 6 (1) (2018) 388–398.

[189] X. Yin, X. Fang, N. Zhang, P. Yang, X. Sha, J. Qiu, Online learning aided adaptive multiple attribute-based physical layer authentication in dynamic environments, IEEE Trans. Netw. Sci. Eng. (2020).

[190] G. Baldini, R. Giuliani, C. Gentile, An assessment of the impact of IQ imbalances on the physical layer authentication of IoT wireless devices, in: 2019 Global IoT Summit (GIoTS), IEEE, 2019, pp. 1–6.

[191] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, G. Fettweis, 5G-enabled tactile internet, IEEE J. Sel. Areas Commun. 34 (3) (2016) 460–473.

[192] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan, A. Seneviratne, A survey of wearable devices and challenges, IEEE Commun. Surv. Tutor. 19 (4) (2017) 2573–2620.

[193] B. Ali, A.I. Awad, Cyber and physical security vulnerability assessment for IoT-based smart homes, Sensors 18 (3) (2018) 817.

[194] F. Masmoudi, Z. Maamar, M. Sellami, A.I. Awad, V. Burégio, A guiding framework for vetting the internet of things, J. Inf. Secur. Appl. 55 (2020) 102644.

[195] M. Elsaadany, A. Ali, W. Hamouda, Cellular LTE-A technologies for the future Internet of Things: Physical layer features and challenges, IEEE Commun. Surv. Tutor. 19 (4) (2017) 2544–2572.

[196] A. Ijaz, L. Zhang, M. Grau, A. Mohamed, S. Vural, A.U. Quddus, M.A. Imran, C.H. Foh, R. Tafazolli, Enabling massive IoT in 5G and beyond systems: PHY radio frame design considerations, IEEE Access 4 (2016) 3322–3339.

[197] N. Xia, H.-H. Chen, C.-S. Yang, Radio resource management in machine-to-machine communications—A survey, IEEE Commun. Surv. Tutor. 20 (1) (2017) 791–828.

[198] F.S. Shaikh, R. Wismüller, Routing in multi-hop cellular device-to-device networks: A survey, IEEE Commun. Surv. Tutor. 20 (4) (2018) 2622–2657.