Mobile Networks and Applications
https://doi.org/10.1007/s11036-021-01841-2

Security Standards and Measures for Massive IoT in the 5G Era

Qin Qiu[1] · Ding Wang[2,3] · Xuetao Du[4] · Shengquan Yu[5] · Shenglan Liu[4] · Bei Zhao[4]

Accepted: 6 February 2021

Abstract
With the development of 5G technology, Internet of Things (IoT) is proliferating and deeply integrated with our daily lives and industry productions. IoT applications in the 5G era generate massive connections, and this would bring about many security issues. In this paper, we first analyze security risks for massive IoT in the 5G era, then summarize related security policies and standards. Furthermore, we propose security requirements and measures for various layers, including sensor control equipment and IoT card, IoT network and transmission exchange, IoT business application and service, and IoT security management and operation. Next, we introduce the case of the cyber security monitoring platform, explain the security technology based on edge computing, and point out the related standards. Finally, we put forward suggestions on IoT security technology and standardization work, so as to promote the secure development of IoT in the 5G era.

Keywords 5G · IoT · Security · Privacy · Standardization · Edge computing

1 Introduction

5G communication technology supports high-speed information transmission and massive terminal connections, which accelerates the development of IoT. In the 5G era, while IoT makes people 's life more convenient and intelligent, it also faces many security risks.

1.1 5G Accelerates the Development of IoT

In recent years, new technologies such as 5G, big data, cloud computing and artificial intelligence have brought innovation vitality to IoT, making the intelligent connection of things a reality. Main application scenarios of IoT are smart city, public security, transport, financial and so on, as shown in Fig. 1. Therefore, basic requirements of machine communication for 5G network are concentrated on massive terminal access, ultra-low delay, efficient connectivity, low cost, low power consumption, high reliability and wide cover range [1]. The development trend of the IoT in the 5G era is mainly manifested in following aspects [2]:

1.1.1 From Narrowband to Broadband

With the development of UHD, VR, AR and other technologies, the IoT industry has a higher demand for the network bandwidth.

1.1.2 From Mixed Use to Exclusive Use

The traditional public network is difficult to meet the needs of industry applications. Customized and differentiated

✉ Ding Wang
wangding@nankai.edu.cn

Qin Qiu
qiuqin@chinamobile.com

Xuetao Du
duxuetao@cmdi.chinamobile.com

Shengquan Yu
yusq@bnu.edu.cn

Shenglan Liu
liushenglan@cmdi.chinamobile.com

Bei Zhao
zhaobei@cmdi.chinamobile.com

1 China Mobile Communications Group Co., Ltd, Beijing 100053, China

2 College of Cyber Science, Nankai University, Tianjin 300350, China

3 Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin 300350, China

4 China Mobile Group Design Institute Co., Ltd, Beijing 100080, China

5 Beijing Normal University, Beijing 100875, China

Published online: 10 November 2021

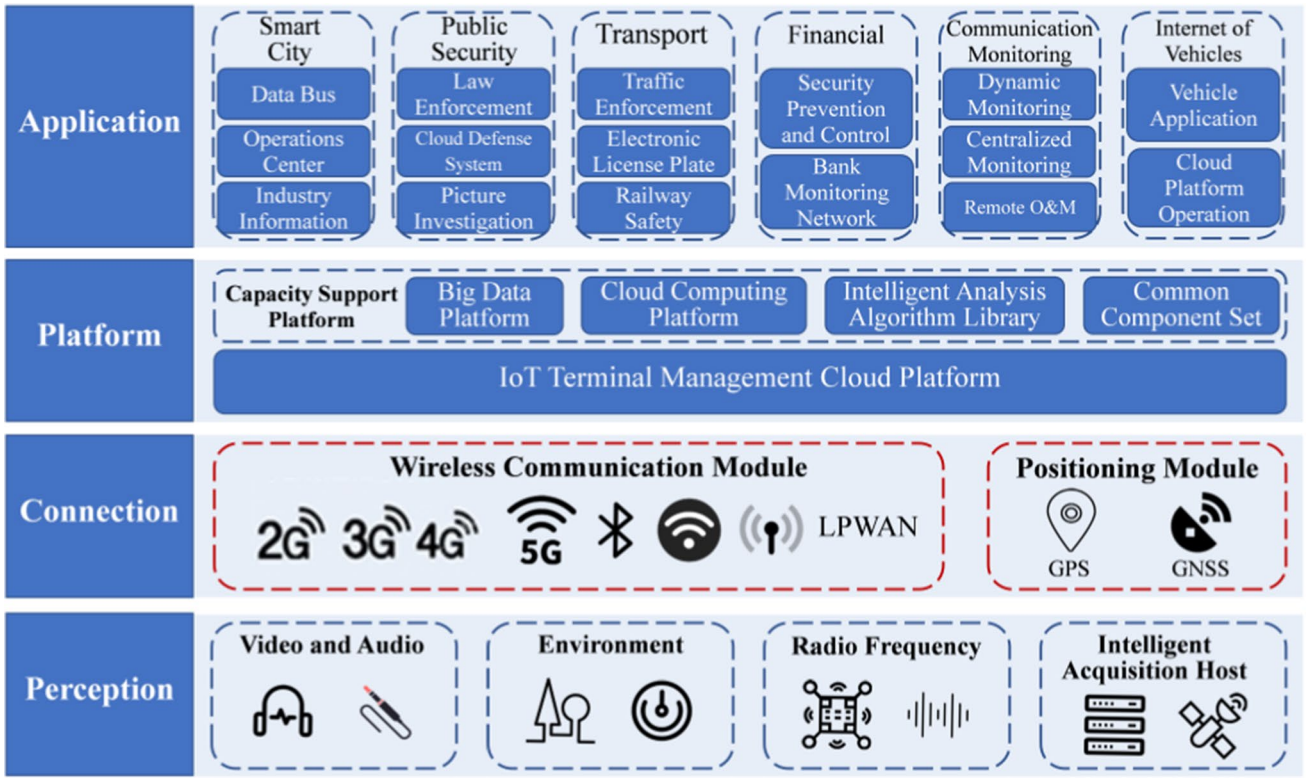

Fig. 1 Applications of the IoT

exclusive network services can meet the needs of vertical industry.

1.1.3 From Flat Coverage to Three-Dimensional Coverage

5G provides all-round breadth and height coverage. By network connection configuration and low altitude coverage optimization, it can meet the coverage of ATG, UAV and other scenes.

1.1.4 Improvement of Performance

The performance including time delay, reliability, security, positioning accuracy has been improved in the 5G era. For instance, remote control services need high reliability and low time delay, and UAV services need positioning accuracy.

With the development of IoT in the 5G era, there are also corresponding industry application scenarios, mainly including three aspects: (1) 5G enabled industry private network. The integrated network slice service platform provides high reliability and strong performance, making it easy to deploy private network services for the vertical industry and better meet customized needs of industry users. (2) New intelligent network management. According to requirements of industry customers for the stability and reliability of 5G communication network, the intelligent network management of the IoT is built to realize the predictable failure, simple operation of the system, docking and expansion of the network management platform with other business platforms. (3) Diversified and customized terminals. In view of the diverse use scenarios and complex environment of industrial terminals, the 5G communication module is integrated on the industrial terminals to achieve the diversification and customization of industrial terminals.

1.2 Security Risks for IoT in the 5G Era

5G introduces a new network structure, using Software Defined Network (SDN), network function virtualization), MEC (multi-access edge computing (NFV) and other technical means to meet the connection requirements of a large number of devices [3, 4]. 5G has penetrated into various industries, and various IoT devices have accessed to the communication network. At the same time, the network has become more vulnerable, bringing new risks and challenges [2].

1.2.1 Threats in Various Industries

5G network further strengthen the high-speed connection between not only people and things, but also things and

things, penetrating into medical treatment, transportation, education and many other industries. It promotes the development of the IoT, and brings about applications such as Smart Healthcare, Internet of Vehicles, Intelligent Wear, etc. However, it also increases the risk of network equipment being invaded, leading to further increase the threat to personal safety, industrial production, etc.

1.2.2 Risks Towards 5G Core Network

Mobile edge computing technology is closely related to the development of IoT. While the mobile edge computing technology is implemented as the enterprise network and 5G network are integrated, the 5G core network capability sinks to the network edge node, and there is an attack path from the edge equipment to the core network, which would increase risks in enterprise networks into the core network.

1.2.3 Threats to IoT Devices Based on the SIM Card

Many IoT devices use the SIM card within 5G network, such as intelligent factory devices, automatic driving vehicle, intelligent robot, etc. According to security standards of the SIM cards, it is possible to modify the content and function of the SIM card remotely by an invisible short message service (SMS) sent through OTA technology, which may be abused by attackers [5–7]. In the 5G era, the transmission capacity of these messages is enhanced, which will substantial increase the probability of abuse and threaten a large number of IoT devices based on the SIM card.

1.2.4 Complexity of Security Protection

With the rapid development of the 5G technology, a large number of IoT devices have been connected, and the types of IoT devices are also growing continuously. As a result, the network for IoT is becoming more and more complex. Massive equipment connection, emerging new services and application scenarios would change the current network structure, and increase the difficulty of IoT security protection.

2 IoT Security Policies and Standards in the 5G Era

With the arrival of the 5G era, the applications of IoT are gradually popularized. In order to create a favorable environment for industrial development, it is required to carry out security policies and standards for 5G and IoT. Many countries in the world are formulating 5G and IoT security policies and standards in varying degrees, so as to promote the comprehensively development of IoT in the 5G era.

2.1 Security Policies

The advancement of 5G technologies has accelerated the speed of information transmission and data processing in our society. As a result, the connection between humans and devices has gradually increased, and the IoT has shown an explosive development trend. Focusing on enhancing the security of the IoT in the 5G era, countries all over the world attach great importance to 5G security since its significant influence on the IoT, and have formulated strategies and policies to reduce security risks of the IoT [8].

The United States promoted the construction of the IoT security mainly from aspects of strategic formulation and policy implementation [8], and issued strategic documents and laws, such as “Strategic Principles for Securing the Internet of Things” in 2016, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” in 2018, “IoT Cybersecurity Improvement Act” in 2019, etc. The European Union focuses on the security baseline setting of IoT and user data protection [9]. It issued the IoT security baseline guide for critical information infrastructure in 2017, and “General Data Protection Regulation” set new regulatory requirements for data protection of enterprises, which was effective from 2018. Besides, the United Kingdom also formulated policies related to the IoT security, and they concentrate on the security construction and innovation of the IoT ecosystem. Moreover, other countries such as Japan and South Korea also developed a series of work in the promotion of IoT security policies.

As early as 2013, the Chinese government incorporated the work for IoT security into its policy planning and successively issued the guidance of the State Council on promoting the orderly and healthy development of IoT. In 2019, the Ministry of Industry and Information Technology of China issued the implementation opinions on promoting the quality of manufacturing products and services, which clearly defined 5G and IoT related industries [10]. Besides, the Chinese government also issued laws and supported normative documents including “Cybersecurity Law of the People's Republic of China”, “the National Network Security Emergency Plan”, etc., which provided the supervision of IoT security [2].

2.2 Security Standards

It is a global common goal to accelerate the development of standards for IoT security in the 5G era, and IoT security standards are constantly evolving and developing. At present, many standardization organizations all around the world have carried out research in the field of IoT security [2]. The main research directions of the major standardization organizations are shown in Table 1.

With the rapid development of IoT, problems emerged such as fragmentation, scattered application scenarios, numerous standards, etc. 3GPP overcame various technical challenges and fulfilled the core standards of Narrow Band Internet of Things (NB-IoT) in 2016 [11], which enabled eligible IoT terminals to access the 5G core network securely. The 5G working group of the ITU-R divided 5G application scenarios into three types including Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low Latency Communications (uRLLC) and Massive Machine Type Communication (mMTC) [12]. Especially, mMTC is aim to connect millions or even billions of devices, which has a close relationship with the IoT and supports massive IoT terminal connections [13]. 3GPP carried out a lot of research work related to mMTC, such as the NB-IoT and Enhanced Machine Type Communication (eMTC) [14]. In addition, 3GPP also studied the business requirements related to IoT security and the management of remote contract information of devices, including the trusted mode of remote contract, security requirements and corresponding solutions.

In general, security standards for IoT tend to concentrate on the fields of application security and privacy protection. As for ISO/IEC, security standards for IoT are mainly in regard to the architecture and security technology, and it issued "Information Technology—Security Techniques—Lightweight Cryptography" in 2012 [15], "Information Technology—Internet of Things Reference Architecture" in 2018 [16], etc. ITU-T planned a series of security standards for IoT [17], and actively carried out the security standardization of the Internet of Vehicles. Moreover, ETSI released the first consumer security standard for the IoT [18], which promoted the development of the future certification scheme for the IoT. IETF mainly studies IP network protocol the standard also proposes protocol optimization for the characteristics of IoT terminals [19]. Besides, industry alliances including 5GAA, IIC, GSMA [8] also carried out a series of work in the security standards for IoT.

China attaches great importance to the IoT security supervision and has carried out work in security reference model, perception and wireless security technology, key industry applications, etc. TC260 issued a series of standards related to the IoT. For instance, "Information Security Technology—Security Reference Model and Generic Requirements for Internet of Things" in 2018 [20] clarified the reference framework for the IoT security, and "Baseline for Classified Protection of Cybersecurity" in 2019 [21] specified requirements for the IoT security. CCSA focuses on communication networks and systems, and completed the industry standards for IoT such as "General Framework and Technical Requirements of IoT" in 2012 [22] and "General Requirements for Cellular Narrowband Radio Access for Internet of Things (NB-IoT)" in 2018 [23], providing a reference for the IoT security construction.

Remarkably, the edge computing technology is a key field that must be considered of IoT in the 5G era. For edge computing, ISO, ITU, and ESTI formulated relevant security standards [24]. The ISO/IEC proposed standards such as "Information technology—Cloud Computing—Edge Computing Landscape" and "Technical Report on Information Technology—IOT and Related Technologies—Edge Computing", which involve the security and other aspects in IoT applications. Besides, ESTI defined the technical requirements, framework and reference architecture for mobile edge computing. ITU-T formulated "Security Capabilities of Network Layer for 5G Edge Computing and Security Framework for 5G Edge Computing Services", which focuses on the network layer security of edge computing.

Table 1 Main research directions of standardization organizations

Standardization organizations	Main research directions
3GPP	Security architecture, NB-IoT, eMTC, business secuity requirements, etc. [11–14]
ISO/IEC	Architecture, security technology, including encryption, lightweight, authentication, privacy control, etc. [15, 15]
ITU	Smart city and community, privacy protection, trust and identification, Internet of Vehicles, etc. [17]
ETSI	Authentication authorization, quantum security threat assessment and analysis of the authentication security mechanism of the IoT group. [18]
IETF	Protocol of authorization, authentication and audit in IP network. [19]
5GAA	Security architecture of the Internet of Vehicles for all regions. [8]
IIC	Establish open interoperability standards and accelerate the implementation of industrial Internet. [8]
GSMA	Security Research of operators in the field of IoT. [8]
TC260	Grade protection, IoT security reference model, IoT security standardization white paper, etc. [20, 20]
CCSA	Communication network and system, security framework. [22, 22]

3 Security Requirements and Measures of IoT

According to the entity classification of ISO/IEC 30141:2018 [25] and the reference model of GB/T 37044–2018 [21], security requirements of IoT are mainly located in sensing devices and cards, network and transmission exchange, business applications and services, and security management and operation [8], as shown in Fig. 2 [2]. There are four areas that work together as an organic whole to guarantee the security of IoT systems. The sensing security area focus on security requirements of sensing devices and corresponding system. In the network security area, security requirements major in the network and transmission exchange. The application security area is mainly to meet service security requirements of the user, such as the identity authentication, access control and so on. As for the operation security area, it concentrates on security requirements of the operation and maintenance management, and it is an indispensable part to ensure the security operation of the above three areas.

Based on the Fig. 2, the existing security risks are considered, and the results are shown in Fig. 3 [2]. Combined with the risk points, security requirements and key technologies are analyzed, and security measures of IoT in the 5G era are summarized in Fig. 4 [2].

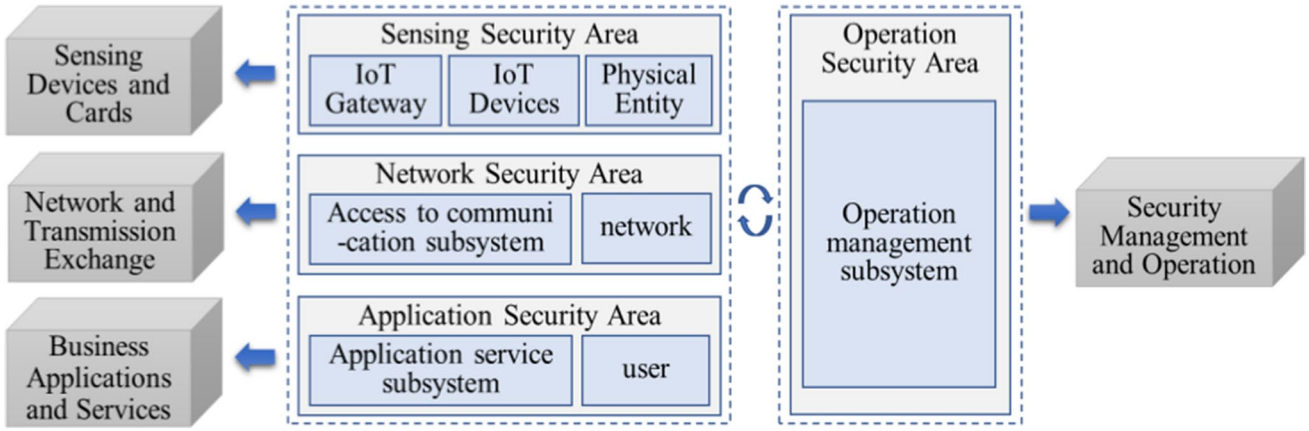

Fig. 2 Security requirements of IoT

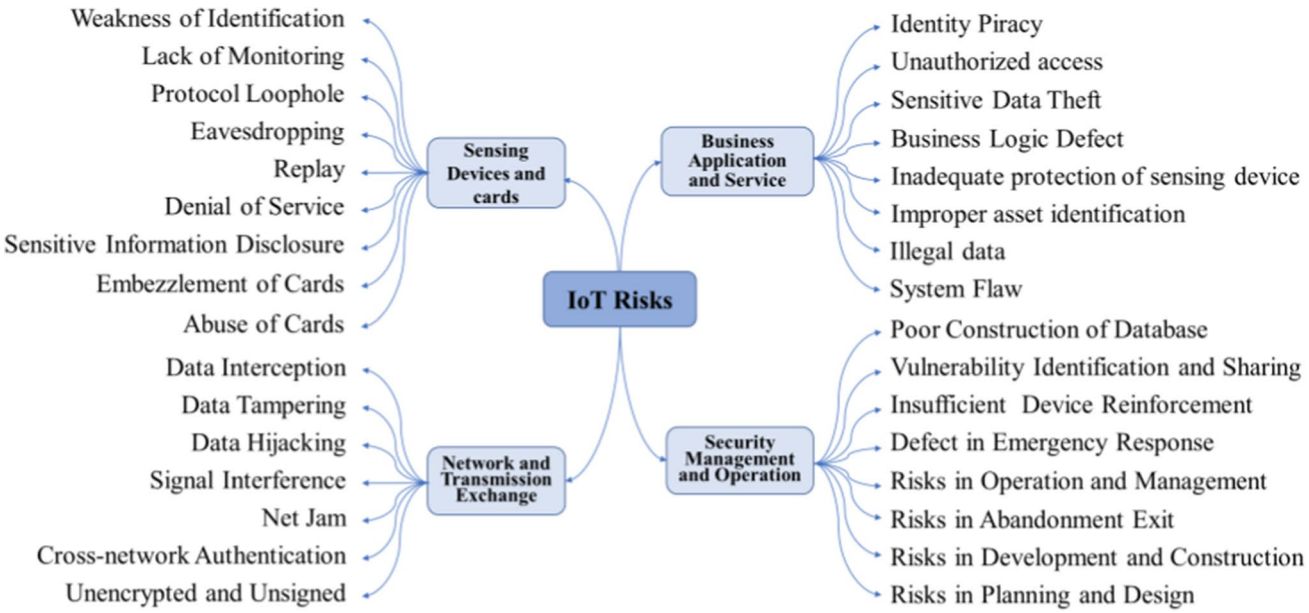

Fig. 3 Risks faced by the IoT

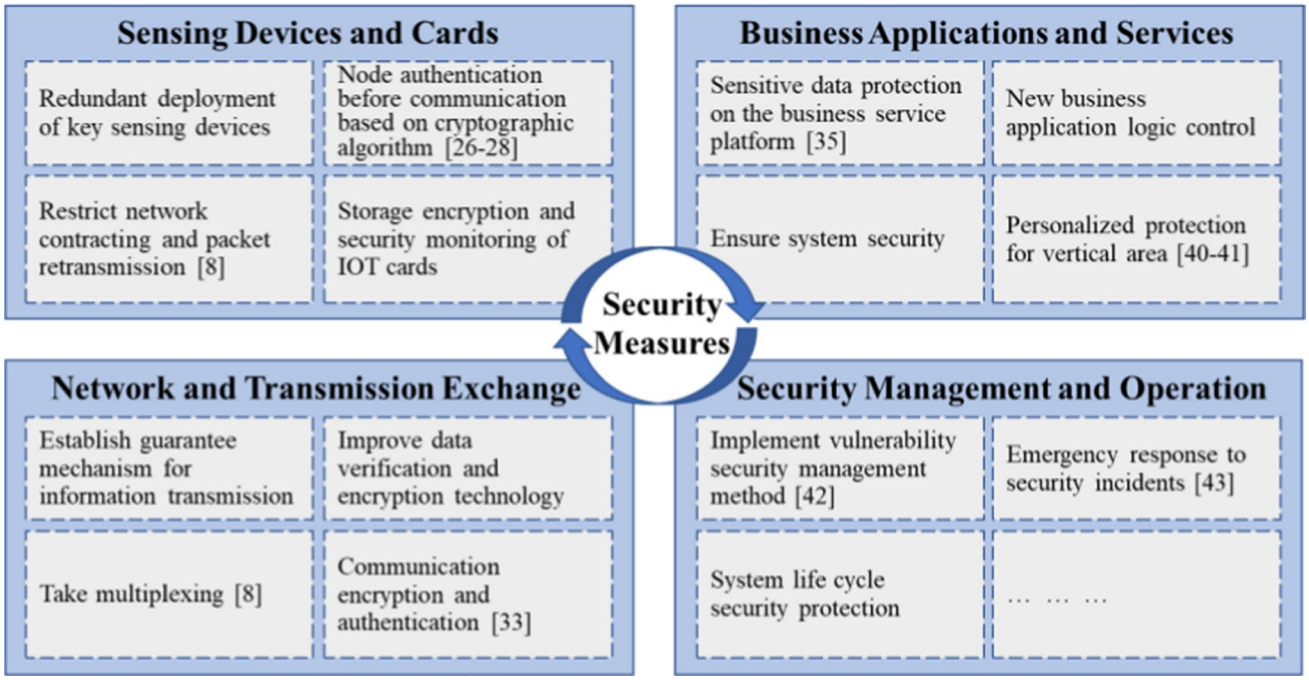

Fig. 4 Security measures of IoT in the 5G era

3.1 Sensing Devices and Cards

The main function of the sensing device is to realize the collection, identification and control of information. The smart IoT card refers to the smart card used in the field of IoT. Sensing devices and smart IoT cards have an important impact on the security of the IoT.

3.1.1 Sensing Devices

Sensing devices include sensing terminals and control devices. Sensing terminals are usually in a harsh environment without monitoring. The redundant deployment of key nodes is required to ensure that nodes can achieve network self-healing, so as to avoid work interruption in case of natural or man-made damage. Authentication between nodes before communication based on encryption algorithm is required to prevent attackers from illegally accessing the system by using the weakness of authentication mechanism [26–28]. It is necessary to limit the network sending speed and packet retransmission times to prevent the protocol vulnerability from being exploited [8]. Intelligent sensing devices are products that integrate sensor chips, communication chips, microprocessors, drivers, software algorithms, etc. It not only has a simple perception function, but more importantly, it also includes intelligent edge computing processing [29–31]. Intelligent sensing devices will play an important role in the IoT and their market applications are showing explosive growth.

3.1.2 Smart IoT Card

The smart IoT card embedded in the device in the form of software adopts the over-the-air card writing technology based on the public network, which may lead to eavesdropping, replay, denial of service, sensitive data disclosure, etc., so it is necessary to adopt the secure communication and storage encryption mechanism. In addition, the equipment is connected to the communication network based on the IoT network card as the identity, and the separation of the machine card and the card may also cause the problem of the card being misappropriated or abused, so it is essential to establish the corresponding security management and monitoring means [7].

3.2 Network and Transmission Exchange

The application of the IoT uses a complex network structure. During the process of data transmission and exchange in the network, a lot of risks will also be generated.

3.2.1 Wireless Communication

WIFI, Bluetooth, 2/3/4/5G and other wireless communication technologies have their own security problems, and security problems of the IoT are also accompanied [32]. A wide range of sensing terminals and access devices are deployed in the unmonitored environment. The number of IoT nodes is huge and wireless radio frequency signals are

used for data transmission. Attackers can send interference signals to interrupt communication, or hijack, eavesdrop, tamper with data in the process of signal transmission. Therefore, it is necessary to establish information transmission guarantee mechanisms and improve data verification and encryption technologies [7].

3.2.2 Transmission Switching

The transmission of IoT information will pass through different heterogeneous networks. When transmitting large amounts of data, it is easy to cause congestion in the core network. Therefore, multi-channel transmission is needed to alleviate the network pressure and resist the denial of service attack [8]. At the same time, heterogeneous networks in the transport layer need to be interconnected, so it also faces problems such as cross-network authentication. The point-to-point and end-to-end encryption mechanism can be used to ensure the security of the transport layer. In addition, data packets transmitted on IoT are not encrypted and signed, which is easy to be eavesdropped, tampered and forged. Thus PGP, SSL/TLS, IPsec and other protocols [33] are needed to provide communication encryption and authentication functions. In addition, data collection and calculation can be performed locally by edge computing technology [34]. Some important information, especially sensitive information, no longer be transmitted to the cloud through the network, effectively solving the problem of user privacy leakage and ensure data security.

3.3 Business Application and Service

IoT business application and service security requirements mainly include business service platform security requirements and vertical industry security requirements.

3.3.1 Business Service Platform

The business service platform needs to avoid the risks of identity counterfeiting and unauthorized access due to the variety of access devices [35]. The business service platform needs to avoid stealing, tampering, forgery and so on when collecting, storing and processing a large number of sensitive data. As the emergence of various new business applications, attention should be paid to security threats in the realization of technology, logic, control and other aspects. It is also necessary to ensure the system security requirements [7].

3.3.2 Vertical Industry

Each vertical industry faces different security risks and needs. For example, in the smart city, its security requirements mainly lie in sensing devices protection and diversified network access [36]. Edge computing will enrich the application scenarios of the smart city, provide hierarchical management and services between households, communities, communities and cities, and coordinate their development [37]. In the industrial Internet, its security requirements mainly lie in the identification of industrial control equipment assets and network boundary, industrial network isolation measures, etc. [38]. As for the Internet of Vehicles, its security requirements mainly lie in ensuring the legitimacy of sensor data, the security of core control components and so on [39]. For smart transportation, numerous surveillance cameras at intersections will generate massive video data, and real-time massive data analysis and storage in the cloud is a huge challenge to computing power and network bandwidth. If we use edge computing to store and analyze massive video data locally [40, 41], only pass videos of traffic accidents or illegal behaviors to the cloud for further analysis and long-term storage, which can effectively reduce the data transmission to the cloud, and support real-time intelligent traffic control [7].

3.4 Security Management and Operation

IoT security management and operation security requirements mainly lie in IoT security management related requirements, system life cycle operation security requirements, etc.

3.4.1 IoT Security Management

Since IoT has different characteristics from the traditional Internet in many aspects such as terminal devices, firmwares and so on, it is important to research the vulnerability management methods in the IoT industry [35], including vulnerability library construction, vulnerability identification, vulnerability sharing, equipment reinforcement, etc. In addition, the emergency response of IoT security incidents is the last defense line of IoT security [42], and it is also crucial to ensure the normal operation of IoT business.

3.4.2 System Life Cycle

A complete life cycle of the IoT system includes planning and design, development and construction, operation management, and abandonment and exit. Each stage has different missions and security requirements, thus corresponding security protection measures shall be established in each stage [7].

4 A Use Case of IoT Security Techniques and Standards

This chapter will introduce the cyber security monitoring platform as a typical use case of IoT application, as well as the security technology and related standards used in the case.

4.1 Introduction of the Use Case

The cyber security monitoring is a popular research field in recent years [43]. It integrates all available information to evaluate the security situation of the network in real-time, provides a basis for decision analysis of security administrators, and reduces risks and losses caused by insecure factors. The cyber security monitoring platform introduced in this chapter has benchmarked multiple national standards for IoT security in the process of its construction. Furthormore, based on the comprehensive consideration of the overall architecture and security features of the IoT, the cyber security monitoring related work has been carried out.

As a result, the cyber security monitoring platform has big data analysis and situational awareness capabilities on aspects of IoT cards, smart sensing devices, business applications, basic assets and early warning disposal, which can effectively improve IoT security capabilities of cyber security monitoring, early warning and handling. When the cyber security monitoring platform is operating normally, it can monitor and promptly shut down the fraudulent IoT cards to ensure IoT security. Besides, it can discover and alert various IoT risks, such as the threat from ransomwares in business applications. In addition, combined with the enterprise's internal offensive and defensive test drills, the cyber security monitoring platform can also repair vulnerablities of smart sensing devices and so on.

4.2 Related Security Techniques

In the 5G era, more and more IoT devices are connected to the network. As for the cyber security monitoring platform, due to the limited computing resources and storage resources of most IoT devices, traditional defense technologies such as firewalls and IDS are difficult to deploy effectively. Thus, the edge computing technology needs to be put into use to improve the performance of IoT. The breakthrough in the edge computing technology means that many commands will be achieved by local devices without going to the cloud, and the data processing will be completed at the local edge nodes. It will undoubtedly improve the processing efficiency and reduce the load on the cloud.

For example, if a traditional security monitoring system needs to store videos, it requires a cloud platform for video analysis and processing, which consumes a lot of storage, computing, and broadband resources. However, after using the edge computing technology, real-time video preprocessing, intelligent storage and AI inference can be completed at edge nodes, as shown in Fig. 5., which could greatly not only simplify the dependence on the cloud, but also reduce the processing delay and the resource consumption. Due to this feature of edge computing techniques, it promotes the effective operation of the cyber security platform.

The cyber security monitoring platform is based on basic data such as communication bills, network traffic, and business logs, combined with edge computing techniques, as well as big data and artificial intelligence, to provide security guarantee for the smooth operation of IoT services. In the edge computing mode, with the help of the platform of the edge computing center, through the analysis of the logs and alarms of the devices in the network, the security status can be analyzed and evaluated. Even edge computing centers can collaborate with each other to build a distributed cyber security monitoring platform, to improve system detection and response analysis capabilities. Cyber security monitoring is of great significance to the security of the IoT, and the role played by edge computing techniques is indispensable.

4.3 Related Security Standards

In the construction of the cyber security monitoring platform, many IoT security releated standards are referred to, including ISO / IEC 27030 “Information technology—Security techniques—Guidelines for security and privacy in Internet of Things (IoT)”, GB/T 37044–2018 “Information

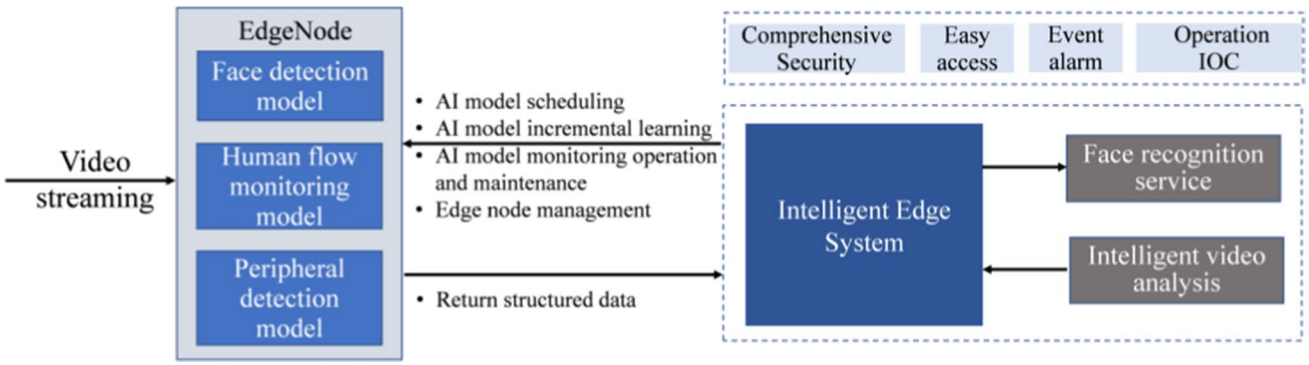

Fig. 5 Edge computing techniques in security monitoring

security technology—Security reference model and generic requirements for Internet of things", GB/T 36951-2018 "Information security technology—Security technical requirements for application of sensing terminals in Internet of things", GB/T 36635–2018 "Information security technology—Basic requirements and implementation guide of network security monitoring", etc., which are conducive to the healthy and sustainable development of the IoT. Besides, the overall architecture and security features of the IoT are fully considered, so as to carry out the work related to cyber security monitoring of the IoT.

In addition, according to ISO/IEC 30141 "Internet of things(IoT)—Reference architecture" and ISO/IEC 27403 "Information technology— Security techniques—Guidelines for IoT-domotics security and privacy", the end-to-end security protection of the IoT application is achieved, which also provide an important reference for the construction of the cyber securiy monotoring platform.

5 Suggestions on the Development of IoT

While 5G speeds up the rapid construction of the IoT security technology, in order to meet current needs of the IoT industry, it is suggested to focus on the following aspects to promote the development of IoT security technology and standardization [2], as shown in the Table 2.

5.1 Sensing Devices and Cards

5G promotes the rapid development and application of Pan terminals, and IoT sensing devices present the characteristics of complexity and diversity. It is suggested to strengthen the security protection technology for the sensing devices in key application scenarios, and propose relevant standards, including UAV equipment security management requirements, intelligent medical equipment security technology and evaluation requirements.

Due to the limitation of energy, power consumption and storage space, the terminal sensing devices in the IoT system usually cannot work well, or needs too much cost to run complex cryptographic algorithms and security protocols. It is recommended to develop lightweight cryptographic algorithms [22] for resource constrained IoT equipment [32], and formulate relevant application implementation guidelines.

In addition to ensuring the confidentiality, integrity and availability of the IoT system, the trustworthiness of devices and components should also be considered. In order to guarantee the trustworthiness of devices, it is recommended to use the trusted computing technology to form a trusted execution environment by combining hardware, firmware and software. In view of the eavesdropping, replay, denial of service, and privacy leakage caused by the use of IoT cards, the air card writing technology must be developed along with secure mechanisms. Besides, it is also necessary to build an identity resolution system and adopt corresponding security measures.

5.2 Network and Transmission Exchange

The IoT has penetrated into smart home, health care, public services and other scenarios, which will generate a large number of sensitive personal data, so it is necessary to strengthen the relevant security technology. In order to prevent risks from the identification and association of the device and identity, if necessary, the temporary identification of the device is recommended to be used to replace the permanent identification, such as media access address, IPv6 address, etc. [44].

Table 2 Suggestions for the development of IoT security in the 5G era

Field	Development of IoT Security Technology	Development of IoT Security Standardization
Sensing Devices and Cards	Sensing devices protection Lightweight encryption [22] Trusted computing technology Air card writing technology	UAV devices secuirty management Intelligent medical equipment Lightweight encryption [22]
Network and Transmission Exchange	Privacy protection Device identification [44] Data processing on edge nodes	Data life cycle security management Personal data transaction Data security implementation
Business Applications and Services	Encryption algorithm [45–48] Data protection, authentication and access control [49]	Vertical industry security Data security, authentication and access control [49]
Security Management and Operation	Abnormal monitoring Security measures at all stages [50, 51]	Security operation and maintenance Incident emergency response [54]
Edge Computing and Cloud	Edge intelligence [55, 56] Centralized processing of big data in cloud computing	Edge-cloud collaboration [55, 56] Data processing in threat intelligence, cyber security monitoring, etc

To deal with risks in the network and transmission exchange, it is suggested to strengthen the research on key technologies of the privacy protection and the data security technology system, strengthen the application and the implementation of the data life cycle security management, personal information, data transaction and other relevant standards in key fields such as industrial Internet and smart city, and develop corresponding national standards such as data security implementation guides. In addition, by the edge computing technology, devices will process data on edge nodes locally, and data does not need to be returned to the central processor, which will reduce DDoS attacks on the network and also help to protect the user privacy.

5.3 Business Application and Service

The 5G technology is widely used in various IoT scenarios. The application security of the vertical industry of the IoT based on 5G shows the trend of expanding attack area, ubiquitous attack mode and blurring border. Traditional security mechanisms and defense means, such as authentication encryption algorithm, firewall, key management system, intrusion detection system, etc., need to be optimized in a targeted way [45]. Light-weight encryption algorithms are important methods to ensure the network security, and protect the data confidentiality along with the integrity [46–48]. From the national perspective, the industrial Internet is an important area worthy of our attention, and it is advised to speed up technologies research and standards promotion such as network facility security, platform and industrial application security, data security protection, test and experimental environment of the industrial IoT. In addition, it is advised to promote the security of the business platform and the edge computing technology of IoT applications such as the Internet of Vehicles.

In the IoT ecosystem, there are some traditional industries, such as transportation, medical treatment, logistics, home furnishing, etc., which are not able to get through the IoT ecological chain, so the business operation needs to rely on the common business service platform. In order to cope with risks and challenges faced by platforms in providing the IoT business assistance for enterprises, it is necessary to strengthen data security protection, access control, identity authentication [49] and other technologies, accelerate the construction of security capacity of the general business service platform of the IoT, and support the development of relevant technical requirements, implementation guidelines and other specifications.

5.4 Security Management and Operation

IoT business involves responsibilities and interests of various parties, including users, equipment manufacturers, network operators, service providers, etc. When security issues arise, it is difficult to divide responsibilities. Therefore, in order to achieve secure operation and maintenance, on the basis of effective organization of all parties, we can enhance the security and reliability of the IoT system by strengthening the abnormal behavior implementation monitoring technology. According to missions and security requirements in each stage of the IoT business, establish corresponding security measures and improve the corresponding protection technologies [50, 50].

Simultaneously, it is proposed to speed up the development of security standards in the security operation of the IoT, emergency response and other aspects [52], so as to promote the effective coordination of the security ecology of the IoT.

5.5 Edge Computing and Cloud

The development of IoT will bring many challenges that cannot be completely solved by IoT terminals and cloud computing alone, thus edge computing is introduced to effectively alleviate or solve these challenges. As a distributed computing method, edge computing optimizes speed and latency by processing and storing information at edge nodes, which can reduce the network load and improve the flexibility along with the security performance. In the future, edge computing will play an important role in privacy protection, cyber security monitoring device update, security protocol, etc., providing impetus for the development of IoT.

Key checkpoints ought to be set up in the whole life cycle of edge computing for IoT, and measures such as security development management, code audit, vulnerability assessment, penetration testing should be implemented to ensure that problems can be solved in time [53, 53]. Furthermore, the security capability of edge computing can be improved by edge-cloud collaboration, which is also the future development trend of edge computing [55, 55]. Edge computing can overcome some shortcomings of cloud computing, but cloud computing also has many advantages, such as centralized big data processing in fields of threat intelligence, cyber security monitoring, security operation and management, etc. Through the edge-cloud collaboration, advantages of cloud computing can be used to enhance the security capabilities of edge computing for IoT. It is also suggested to develop the technical requirements for edge-cloud collaboration and the implementation guidelines for data processing in various scenarios.

6 Conclusion

The advancement of the 5G technology and massive IoT applications facilitates our lives unprecedentedly, but also brings some new risks and challenges. Focusing on the

future development of the IoT, effectively guaranteeing the security of the IoT has become an urgent issue in the 5G era. This paper first introduces the development trend and security risks of IoT, and summarizes IoT security policies and standards in the 5G era. Besides, IoT security requirements and measures are analyzed, which has a positive significance for the secure operation of the IoT. After then, the paper introduces the cyber monitoring platform as a use case of IoT security techniques and standards, and suggestions are provided finally for the future development of the IoT. In order to ensure the security of the IoT, we need to strengthen industry security management, improve security technologies and standards, build effective security protection systems, and explore new technologies, such as the edge computing. It is suggested that industry regulatory authorities, technical research institutions and other relevant parties work together to actively promote the secure development of the IoT.

Acknowledgements The authors thank the anonymous reviewers for their invaluable comments. Ding Wang is the corresponding author. This paper was presented in part at the Proceeding of 3rd EAI International Conference on Security and Privacy in New Computing Environments (SPNCE 2020). This work is in part supported by Key Lab of Information Network Security of Ministry of Public Security (The Third Research Institute of Ministry of Public Security).

References

1. Schulz P, Matthe M, Klessig H (2017) Latency critical IoT applications in 5G: perspective on the Design of Radio Interface and Network Architecture. IEEE Commun Mag 55(2):70–78
2. Qiu Q, Du XT, Yu SQ et al (2020) Research on IoT security technology and standardization in the 5G era. International conference on security and privacy in new computing environments, pp. 77–90
3. Ahmad I, Kumar T, Liyanage M et al (2018) Overview of 5G security challenges and solutions. IEEE Commun Std Mag 2(1):36–43
4. Ahmad I, Kumar T, Liyanage M et al (2017) 5G security: analysis of threats and solutions. In: IEEE conference on standards for communications and networking (CSCN). IEEE Press
5. Huang Q, Yang C (2011) A lightweight RFID authenticate protocol based on smart SIM card. In: Proceedings of the 1st international conference on logistics, informatics and service science, pp 647–650. IEEE Press
6. He R, Zhao G, Chang C et al (2009) A PK-SIM card based end-to-end security framework for SMS. Comput Std Interfaces 31(4):629–641
7. Liu SL, Qiu Q, Zhao B et al (2020) 5G-based IoT security technology. In: Proceedings of 5G network innovation seminar, pp 119–123
8. TC 260 (2019) Communication security standards working group. White paper on Internet of Things security standardization
9. Neisse R, Steri G, Baldini G (2014) Enforcement of security policy rules for the Internet of Things. In: The 3rd international workshop on internet of things communications and technologies (IoT-CT), IEEE Press
10. Ministry of industry and information technology: accelerate the development of 5G and Internet of Things related industries, http://www.sohu.com/a/339209778_166680
11. Cao J, Yu P, Ma M et al (2019) Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network. IEEE Internet Things J 6(2):1561–1575
12. Popovski P, Trillingsgaard KF, Simeone O et al (2018) 5G wireless network slicing for eMBB, URLLC, and mMTC: a communication-theoretic view. IEEE Access 6:55765–55779
13. Bockelmann C, Pratas NK, Wunder G et al (2018) Towards massive connectivity support for scalable mMTC communications in 5G networks. IEEE Access 6:28969–28992
14. Chakrapani A (2017) Efficient resource scheduling for eMTC/NB-IoT communications in LTE Rel. 13. In: IEEE conference on standards for communications and networking (CSCN), pp 66–71. IEEE Press
15. ISO/IEC (2012) ISO/IEC 29192 Information Technology - Security Techniques - Lightweight Cryptography
16. ISO/IEC (2018) ISO/IEC 30141 Information Technology - Internet of Things Reference Architecture
17. Kafle V, Fukushima Y, Harai H (2016) Internet of Things standardization in ITU and prospective networking technologies. IEEE Commun Mag 54(9):43–49
18. ETSI (2019) ETSI releases first globally applicable standard for consumer IoT security. China Standardization
19. Sheng Z, Yang S, Yu Y et al (2016) A survey on the IETF protocol suite for the Internet of Things: standards, challenges, and opportunities. IEEE Wirel Commun 20(6):91–98
20. GB/T (2018) GB/T 37044-2018. Information Security Technology- Security Reference Model and Generic Requirements for Internet of Things
21. GB/T (2019) GB/T 22239–2019. Information Security Technology - Baseline for Classified Protection of Cybersecurity
22. YD/T (2012) YD/T 2437-2012. General Framework and Technical Requirements of IoT (Internet of Things)
23. YD/T (2018) YD/T 3331-2018. General Requirement for Cellular Narrowband Radio Access for Internet of Things (NB-IoT)
24. Lu H, Chen D, Fan B, Wang Y, Wu Y (2018) Standardization progress and case analysis of edge computing. J Comput Res Dev 55(3):487–511
25. ISO/IEC (2018) ISO/IEC 30141:2018. Internet of Things (IoT) - Reference Architecture
26. Wang D, Wang P, Wang C (2019) Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs. ACM Trans Cyber-Phys Syst. https://doi.org/10.1145/3325130(2019)
27. Wang C, Wang D, Tu Y, Xu G, Wang H (2020) Understanding node capture attacks in user authentication schemes for wireless sensor networks. IEEE Trans Depend Secure Comput. https://doi.org/10.1109/TDSC.2020.2974220
28. Wang D, Li W, Wang P (2018) Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans Ind Inf 14(9):4081–4092
29. Xi Z, Qixuan Z (2018) Hierarchical caching for statistical QoS guaranteed multimedia transmissions over 5G edge computing mobile wireless networks. IEEE Wirel Commun 25(3):12–20
30. Li F, Chen J, Wang Z (2019) Wireless map reduce distributed computing. IEEE Trans Inf Theory 65(10):6101–6114
31. Cordelli E, Pennazza G, Sabatini M et al (2018) An open-source smart sensor architecture for edge computing in IoT applications
32. Burg A, Chattopadhyay A, Lam K (2018) Wireless communication and security issues for cyber-physical systems and the Internet-of-Things. Proc IEEE 106(1):38–60
33. Granjal J, Monteiro E, Silva J (2015) Security for the Internet of Things: A survey of existing protocols and open research issues IEEE Communications Surveys & Tutorials. IEEE Press

34. Alnoman A, Sharma SK, Ejaz W et al (2019) Emerging edge computing technologies for distributed IoT systems. IEEE Netw 99:1–8
35. Cai H, Xu L, Xu B et al (2014) IoT-Based configurable information service platform for product lifecycle management. IEEE Trans Ind Inf 10(2):1558–1567
36. Zhang K, Ni J, Yang K et al (2017) Security and privacy in smart city applications: challenges and solutions. IEEE Commun Mag 55(1):122–129
37. Song Y, Yau S, Yu R et al (2017) An approach to QoS-based task distribution in edge computing networks for IoT applications. In: IEEE international conference on edge computing. IEEE
38. Li J, Yu F, Deng G et al (2017) Industrial Internet: A Survey on the enabling technologies, applications, and challenges. IEEE Communications Surveys & Tutorials. IEEE Press
39. Joy J, Gerla M (2017) Internet of vehicles and autonomous connected car - privacy and security issues. In: International conference on computer communication & networks. IEEE Press
40. Li H, Ota K, Dong M (2018) Learning IoT in edge: deep learning for the internet of things with edge computing. IEEE Netw 32(1):96–101
41. Gusev M, Dustdar S (2018) Going back to the roots—the evolution of edge computing. An IoT perspective. IEEE Internet Comput 22(2):5–15
42. Qiu T, Lu Y, Xia F et al (2016) ERGID: an efficient routing protocol for emergency response Internet of Things. J Netw Comput Appl 72:104
43. Rongrong X, Xiaochun Y, Zhiyu H (2019) Framework for risk assessment in cyber situational awareness. IET Inf Secur 13(2):149–156
44. Norrman K, Dubrova E (2016) Protecting IMSI and user privacy in 5G networks. In: EAI international conference on mobile multimedia communications. ICST
45. Li S, Xu L, Zhao S (2018) 5G internet of things: a survey. J Ind Inf Integr 10:1–9
46. Singh S, Sharma PK, Moon SY et al (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Hum Comput 4:1–18
47. Alizadeh M, Hassan WH, Zamani M et al (2013) Implementation and evaluation of lightweight encryption algorithms suitable for RFID. J Next Gen Inf Technol 4:65
48. An-Ping L, Ji-Min Y, Feng LI et al (2014) A comparative study of several lightweight encryption algorithms. Mod Electron Tech
49. Wang D, Wang P (2018) Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans Depend Secure Comput 15(4):708–722
50. Sivanathan A, Gharakheili H, Sivaraman V (2020) Managing IoT cyber-security using programmable telemetry and machine learning. IEEE Trans Netw Serv Manage 17(1):60–74
51. Bertino E (2020) IoT security a comprehensive life cycle framework. In: 2019 IEEE 5th international conference on collaboration and internet computing (CIC)
52. Rathore M, Ahmad A, Paul A et al (2016) Real-time medical emergency response system: exploiting IoT and big data for public health. J Med Syst 40(12):283
53. Roman R, Lopez J, Mambo M (2018) Mobile edge computing, Fog et al. A survey and analysis of security threats and challenges. Fut Gen Comput Syst 78(2):680-698.
54. Pahl C, Ioini NE, Helmer S (2018) A decision framework for blockchain platforms for IoT and edge computing. In: International confernce on internet of things, big data & security
55. Li R, Zhou Z, Chen X et al (2019) Resource price-aware offloading for edge-cloud collaboration: a two-timescale online control approach. IEEE Trans Cloud Comput 99:1–1
56. Han Q, Yang S, Ren X et al (2020) Online learning for edge-cloud collaborative learning on heterogeneous edges with resource constraints. IEEE Commun Mag 58(5):49–55