Research on IoT Security Technology and Standardization in the 5G Era

Qin Qiu[1], Xuetao Du[2], Shengquan Yu[3], Chenyu Wang[4], Shenglan Liu[2(✉)], Bei Zhao[2], and Ling Chang[2]

[1] China Mobile Communications Group Co., Ltd., Beijing 100053, China
qiuqin@chinamobile.com
[2] China Mobile Group Design Institute Co., Ltd., Beijing 100080, China
{duxuetao,zhaobei,changling}@cmdi.chinamobile.com,
liushenglan94@163.com
[3] Beijing Normal University, Beijing 100875, China
yusq@bnu.edu.cn
[4] Beijing University of Post and Telecommunications, Beijing 100876, China
wangchenyu@bupt.edu.cn

Abstract. With the development of 5G technology, Internet of Things (IoT) is highly developing and deeply integrated with social life and industry productions, which brings about many security issues. In this paper, we first analyze the security risks for IoT in the 5G era, then summarize related security policies and standards. Furthermore, we propose security requirements and measures in aspects of sensor control equipment and IoT card, IoT network and transmission exchange, IoT business application and service, and IoT security management and operation. Finally, we put forward suggestions for promoting IoT security technology and the standardization work in the 5G era.

Keywords: 5G · IoT · Security · Privacy · Standardization

1 Introduction

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

1.1 5G Accelerates the Development of IoT

In recent years, new technologies such as 5G, big data, cloud computing, artificial intelligence have brought innovation vitality to IoT, making the intelligent connections of all things a reality. Main application scenarios of IoT are intelligent industry, intelligent agriculture, intelligent transportation, smart grid and so on. Therefore, the basic requirements of machine communication for 5G network are concentrated on massive terminal

D. Wang et al. (Eds.): SPNCE 2020, LNICST 344, pp. 77–90, 2021.
https://doi.org/10.1007/978-3-030-66922-5_5

access, ultra-low delay, efficient connectivity, low cost, low power consumption, and it has high level of reliability along with wide cover range [1]. The development trend of the IoT in the 5G era is mainly manifested in following aspects [2]:

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.

From Mixed Use to Exclusive Use. Traditional public network is difficult to meet the needs of industry applications. Customized and differentiated exclusive network services can meet the needs of vertical industry.

From Flat Coverage to Three-Dimensional Coverage. 5G provides all-round breadth and height coverage. Through network connection configuration and low altitude coverage optimization, it can meet the coverage of ATG, UAV and other scenes.

Improvement of Performance. The performance including time delay, reliability, security, positioning accuracy has been improved. Remote control services need high reliability and low time delay. UAV services need positioning accuracy and so on.

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 reliable, strong performance, easy to deploy private network services for the vertical industry, to better meet the customized needs of industry users. (2) New intelligent network management. According to the requirements of industry customers for the stability and reliability of 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, 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 SDN (Software Defined Network), NFV(network function virtualization), MEC(multi-access edge computing) 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 entered the communication network. At the same time, the network has become more vulnerable, bringing new risks and challenges.

Threats in Various Industries. 5G network can further strengthen the high-speed connection between not only people and things, but also things and things. It brings about Smart Healthcare, Internet of Vehicles, Intelligent Wear, etc., but it also increases the risk of network equipment being invaded, leading to further increase the threat to personal safety, industrial production, etc.

Risks Towards 5G Core Network. 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 introduce risks in enterprise networks into the core network.

Threats to SIM Based IoT Devices. Many IoT devices use SIM card within 5G network. According to security standards of 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].

Complexity of Security Protection. 5G technology connects a large number of devices, and the network is becoming more complex. Massive equipment connection, and emerging new services and application scenarios would change the current network structure, and increase the difficulty of security protection.

2 IoT Security Policies and Standards in the 5G Era

With the arrival of 5G era, the application of IoT is 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 to varying degrees, so as to promote the development of IoT in 5G era in a multi-level and all-round way.

2.1 Security Policies

Focusing on promoting the security level of the IoT, many countries in the world have formulated strategies or policies to deal with risks of the IoT [8].

The United States has promoted the construction of the IoT security from the aspects of strategic formulation and policy implementation [8], issues strategic documents such as the *Strategic Principles for Securing the Internet of Things*, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, and issues laws such as the *IoT in Government Network Security Solutions* and the *IoT Cybersecurity Improvement Act*. The EU focuses on the security baseline setting of the IoT and User data protection [9], the European Union security baseline guide for the IoT in critical information infrastructure environment comprehensively summarizes the security status of the IoT and security baseline recommendations, and the *General Data Protection Regulation* sets new regulatory requirements for the data protection of enterprises.

As early as 2013, the Chinese government has incorporated the IoT security into the work system in its policy planning and successively issued the guidance of the State Council on promoting the orderly and healthy development of the IoT, etc. In September 2019, the Ministry of industry and information technology issued the implementation opinions on promoting the quality of manufacturing products and services, which clearly defined 5G and the IoT related industries [10]. In terms of law, the Chinese government

has issued laws and supported normative documents related to network security, including the *Cybersecurity Law of the people's Republic of China*, *the National Network Security Emergency Plan*, etc., which provides the legal system basis for the security supervision of the IoT industry.

2.2 Security Standards

5G and IoT security standards are constantly evolving and developing. It is a global common goal to accelerate the improvement of the IoT security standard system and the development of standards for key issues of IoT security in 5G era. At present, many standardization organizations at home and abroad have carried out research in the field of 5G and IoT security. The main research directions of the major standardization organizations are shown in Table 1.

In terms of 5G security standards, in 2016, 5G PPP released a white paper -*View on 5G Architecture* [11], which proposed the challenging problems to be solved to meet 5G requirements and discussed the impact of general 5G reference framework on 5G standardization. 3GPP has released the latest schedule of 5G global standards in June 2019, and planned to determine the second and third phase standards of 5G in March 2020 and June 2021 respectively. In addition, the NGMN organization jointly sponsored by multiple operators around the world has published a white paper on 5G, covering virtualization, privacy protection, IoT and other topics [12]. ETSI has studied NFV platform security specifications, MEC security standards and so on [13]. IETF's proposals on Internet protocol standards have also played an important reference role in the development of 5G standards [14]. In January 2020, CCSA held the release ceremony of the early 14 5G standards in China at the 5G Standard Release and Industry Promotion Conference. These 5G standards are fully in line with the global 5G standards, covering core network, wireless, antenna, terminal, security and other fields.

In terms of IoT security standards, at present, the international IoT security standards are mainly focused on the security system framework, network security, privacy protection, equipment security, etc. As 5G technology promotes the application of IoT to mature gradually, in recent years, the security standards tend to focus on the areas such as the application security and privacy protection. The industry alliance including 5GAA, IIC, GSMA, etc., has also opened in relevant key application fields development of security standards [8].The security standards of ISO/IEC for the Internet of Things are mainly focused on the architecture and security technology, etc., and ISO/IEC 30141:2018 [15], ISO/IEC 29192 [16] and so on have been issued. ITU-T has planned a series of security standards for the IoT [17], and actively carried out the security standardization of the Internet of Vehicles. ETSI has 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]. China attaches great importance to the security supervision and technical support of the IoT. And China has carried out work in security reference model, perception and wireless security technology, key industry applications and other fields. At present, TC260 has issued a series of standards related to the IoT. *The Baseline for Classified Protection of Cybersecurity* [20] specifies the requirements for the security of the IoT. The *Security Reference Model and Generic Requirements*

Table 1. Main research directions of standardization organizations

Field	Standardization organizations	Main research directions
5G security	3GPP	Security architecture, RAN security, authentication mechanism, user privacy, network slicing [3]
	5GPPP	Security architecture, user privacy, authentication mechanism, etc. [11]
	NGMN	User privacy, network slicing, MEC security, etc. [12]
	ETSI	Security architecture NFV security, MEC security, privacy protection [13]
	IETF	Security solutions, user privacy, NSF, etc. for 5G mass IoT devices [14]
	CCSA	5G access network, core network, security and frequency, etc.
IoT security	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]
	ISO/IEC	Architecture, security technology, including encryption, lightweight, authentication, privacy control, etc. [15, 16]
	ITU-T	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]
	TC260	Grade protection, IoT security reference model, IoT security standardization white paper, etc. [20, 21]
	CCSA	Communication network and system, security framework [22, 23]

for Internet of Things [21] clarify the reference framework for the security of the IoT. CCSA focuses on communication networks and systems, and has completed the industry

standards for the IoT such as *the General Framework and Technical Requirements of IoT* [22], and *the General Requirements for Cellular Narrowband Radio Access for Internet of Things* (NB-IoT) [23], which provides a reference for the security construction of the IoT.

3 Security Requirements and Measures of IoT

According to the entity classification of ISO/IEC 30141:2018 [24] and the reference model of GB/T 37044-2018 [21], the 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. 1. There are four areas that work together as an organic whole to guarantee the security of IoT systems. The sensing security area focus on the security requirements of sensing devices and corresponding system. In the network security area, the security requirements major in the network and transmission exchange. The application security area is mainly to meet the 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 the security requirements of the operation and maintenance management, and it is an indispensable part to ensure the security operation of the above three areas.

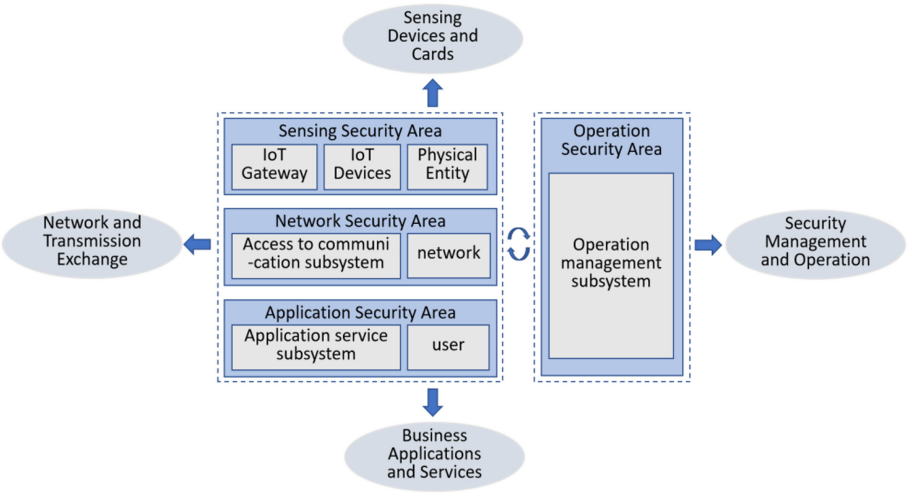

Fig. 1. Security requirements of IoT

Based on the Fig. 1, the existing security risks are considered, and the results are shown in Fig. 2. Combined with the risk points, the security requirements and key technologies are analyzed. In addition, security measures of IoT in the 5G era are summarized and shown in Fig. 3.

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.

Sensing Devices. Sensing devices include sensing terminals and control devices. Sensing terminals are usually in a harsh environment without monitoring. 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 [25–27]. It is necessary to limit the network sending speed and packet retransmission times to prevent the protocol vulnerability from being exploited [8].

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.

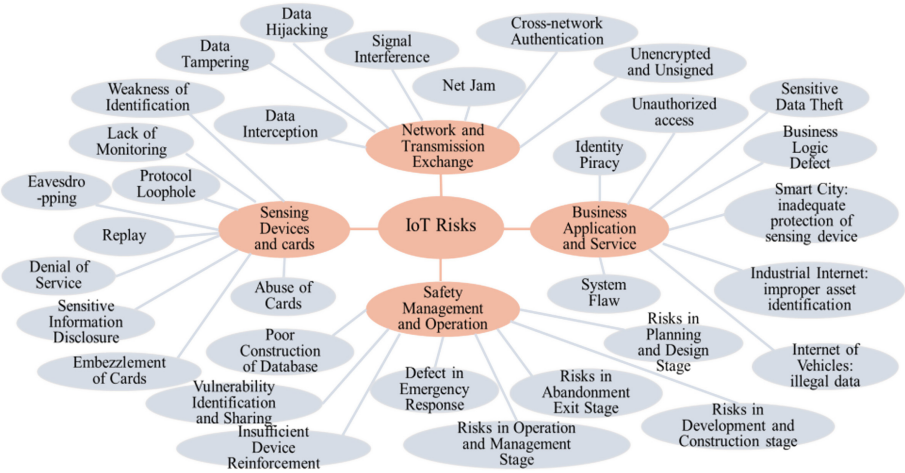

Fig. 2. Risks faced by the IoT

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.

Wireless Communication. WIFI, Bluetooth, 2/3/4/5G and other wireless communication technologies have their own security problems, and the security problems of the IoT are also accompanied [28]. 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 mechanism and improve data verification and encryption technology.

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, the 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, the 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 [29] are needed to provide communication encryption and authentication functions.

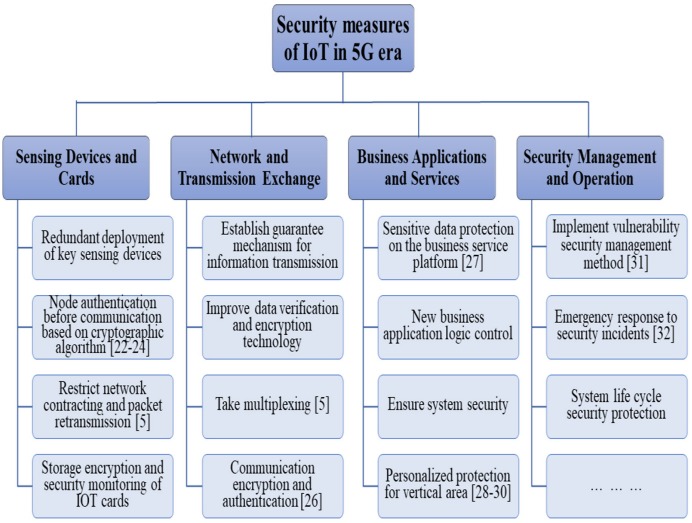

Fig. 3. Security measures of IoT in the 5G era

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.

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 [30]. 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.

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 [31]. 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. [32]. 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 [33].

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.

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 [30], 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 [34], and it is also crucial to ensure the normal operation of IoT business.

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.

4 Suggestions on the Development of IoT in the 5G Era

While 5G speeds up the rapid construction of the IoT security technology, in order to meet the 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, and the key points of all suggestions are also extracted and shown in Fig. 4.

4.1 Sensing Devices and Cards

5G promotes the rapid development and application of Pan terminal, and the IoT sensing devices presents 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 [28], and formulate relevant application implementation guidelines.

4.2 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, temporary identification of the device can be used to replace the permanent identification, such as media access address, IPv6 address, etc. [35]. It is suggested to strengthen the research on key technologies of privacy protection and data security technology system, strengthen the application and implementation of 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.

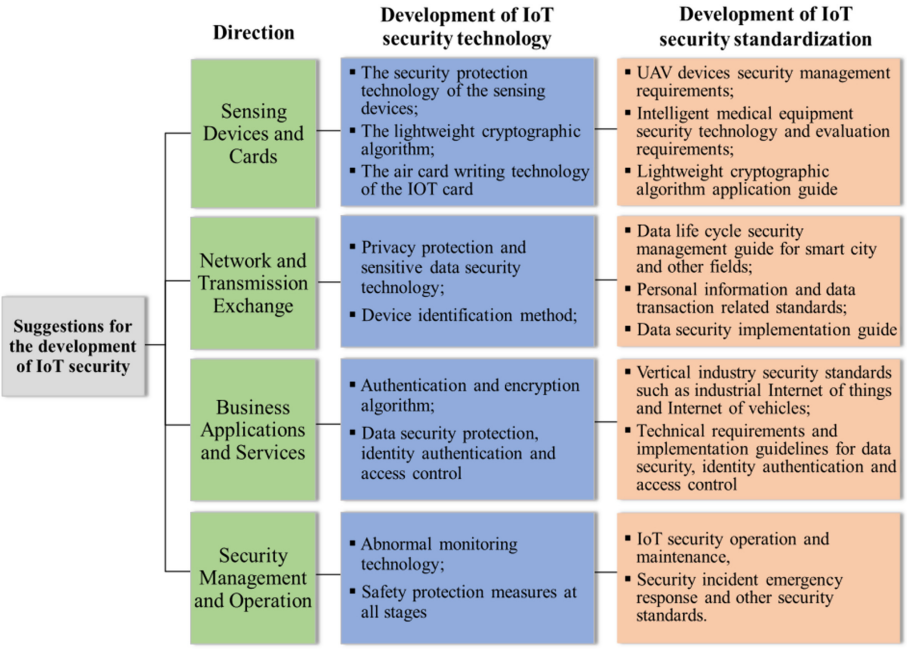

Fig. 4. Suggestions for the development of IoT security in the 5G era.

4.3 Business Application and Service

The 5G technology is widely used in 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 [36]. Light-weight encryption algorithms are important methods to ensure the network security, and protect the data confidentiality along with the integrity [37–39]. Industrial Internet is an important field of national concern, 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 industrial IoT. In addition, It is advised to promote the security of business platform and edge computing of 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 IoT business assistance for enterprises, it is necessary to strengthen data security protection, access control, identity authentication [40] and other technologies, accelerate the construction of security capacity of the general business service platform of IoT, and support the development of relevant technical requirements, implementation guidelines and other specifications.

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

5 Conclusion

The advancement of the 5G technology and 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. 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. It is suggested that the industry regulatory authorities, technical research institutions and other relevant parties work together to actively promote the secure development of the IoT.

References

1. Schulz, P., Matthe, M., Klessig, H.: Latency critical IoT applications in 5G: perspective on the design of radio interface and network architecture. IEEE Commun. Mag. **55**(2), 70–78 (2017)
2. Skubic, B., Bottari, G., Rostami, A., et al.: Rethinking optical transport to pave the way for 5G and the networked society. Lightwave technol. **33**(5), 1084–1091 (2015)
3. Ahmad, I., Kumar, T., Liyanage, M., et al.: Overview of 5G security challenges and solutions. IEEE Commun. Stand. Mag. **2**(1), 36–43 (2018)
4. Ahmad, I., Kumar, T., Liyanage M., et al.: 5G security: analysis of threats and solutions. In: IEEE Conference on Standards for Communications and Networking (CSCN). IEEE Press (2017)
5. Huang, Q., Yang, C.: 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 (2011)
6. He, R., Zhao, G., Chang, C., et al.: A PK-SIM card based end-to-end security framework for SMS. Comput. Stand. Interfaces **31**(4), 629–641 (2009)
7. Jia, F., Yang, Y., Peng, J.: Security mechanism for end to end SMS based on smart card. Appl. Res. Comput. **24**(5), 259–261 (2007)
8. TC 260, Communication security standards working group.: white paper on Internet of Things security standardization (2019)

9. Neisse, R., Steri, G., Baldini, G.: 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 (2014)
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. G PPP Architecture Working Group. View on 5G Architecture (2016)
12. Iwamura, M.: NGMN view on 5G architecture. In: Vehicular Technology Conference. IEEE Press (2015)
13. Jaeger, B.: Security orchestrator: introducing a security orchestrator in the context of the ETSI NFV reference architecture. In: IEEE Trustcom/ BigDataSE/ISPA, vol. 1, pp. 1255–1260. IEEE Press (2015)
14. Omheni, N., Bouabidi, I., Gharsallah, A., et al.: Smart mobility management in 5G heterogeneous networks. IET Netw. **7**(3), 119–128 (2018)
15. ISO/IEC 30141:2018 Information Technology - Internet of Things Reference Architecture (2018)
16. ISO/IEC 29192 Information Technology - Security Techniques - Lightweight Cryptography (2012)
17. Kafle, V., Fukushima, Y., Harai, H.: Internet of Things standardization in ITU and prospective networking technologies. IEEE Commun. Mag. **54**(9), 43–49 (2016)
18. ETSI, ETSI releases first globally applicable standard for consumer IoT security. China Standardization (2019)
19. Sheng, Z., Yang, S., Yu, Y., et al.: A survey on the IETF protocol suite for the Internet of Things: standards, challenges, and opportunities. IEEE Wirel. Commun. **20**(6), 91–98 (2016)
20. GB/T 22239-2019. Information Security Technology - Baseline for Classified Protection of Cybersecurity (2019)
21. GB/T 37044-2018. Information Security Technology - Security Reference Model and Generic Requirements for Internet of Things (2018)
22. YD/T 2437-2012. General Framework and Technical Requirements of IoT (Internet of Things) (2012)
23. YD/T 3331-2018. General Requirement for Cellular Narrowband Radio Access for Internet of Things (NB-IoT) (2018)
24. ISO/IEC 30141:2018. Internet of Things (IoT) - Reference Architecture (2018)
25. Wang, D., Wang, P., Wang C.: Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs. ACM Trans. Cyber-Phys. Syst. (2019). https://doi.org/10.1145/3325130
26. Wang, C., Wang, D., Tu, Y., Xu, G., Wang, H.: Understanding node capture attacks in user authentication schemes for wireless sensor networks. IEEE Trans. Dependable Secure Comput. (2020). https://doi.org/10.1109/tdsc.2020.2974220
27. Wang, D., Li, W., Wang, P.: Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans. Indu. Inf. **14**(9), 4081–4092 (2018)
28. Burg, A., Chattopadhyay, A., Lam, K.: Wireless communication and security issues for cyber-physical systems and the Internet-of-Things. Proc. IEEE **106**(1), 38–60 (2018)
29. Granjal, J., Monteiro, E., Silva, J.: Security for the Internet of Things: a survey of existing protocols and open research issues. IEEE Commun. Surv. Tutor. **17**(3), 1294–1312 (2015)
30. Cai, H., Xu, L., Xu, B., et al.: IoT-based configurable information service platform for product lifecycle management. IEEE Trans. Indu. Inf. **10**(2), 1558–1567 (2014)
31. Zhang, K., Ni, J., Yang, K., et al.: Security and privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **55**(1), 122–129 (2017)
32. Li, J., Yu, F., Deng, G., et al.: Industrial Internet: a survey on the enabling technologies, applications, and challenges. IEEE Commun. Surv. Tutor. **13**(3), 1504–1526 (2017)

33. Joy, J., Gerla, M.: Internet of vehicles and autonomous connected car - privacy and security issues. In: International Conference on Computer Communication and Networks. IEEE Press (2017)
34. Qiu, T., Lu, Y., Xia, F., et al.: ERGID: an efficient routing protocol for emergency response Internet of Things. J. Netw. Comput. Appl. **72**, 104–112 (2016)
35. Norrman, K., Dubrova, E.: Protecting IMSI and user privacy in 5G networks. In EAI International Conference on Mobile Multimedia Communications. ICST (2016)
36. Li, S., Xu, L., Zhao, S.: 5G Internet of Things: a survey. J. Indu. Inf. Integr. **10**, 1–9 (2018)
37. Singh, S., Sharma, P.K., Moon, S.Y., et al.: Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J. Ambient Intell. Hum. Comput. 1–8 (2017)
38. Alizadeh, M., Hassan, W.H., Zamani, M., et al.: Implementation and evaluation of lightweight encryption algorithms suitable for RFID. J. Next Gener. Inf. Technol. **4**, 65–77 (2013)
39. An-Ping, L., Ji-Min, Y., Feng, L.I., et al.: A comparative study of several lightweight encryption algorithms. Modern Electronics Technique (2014)
40. Wang, D., Wang, P.: Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans. Dependable Secur. Comput. **15**(4), 708–722 (2018)