Proceedings of CONF-FMCE 2025 Symposium: Semantic Communication for Media Compression and Transmission
DOI: 10.54254/2755-2721/2025.GL26240

Internet of Things Security Technology in Telecommunications Engineering

Xinpeng Tian

International College, Beijing University of Posts and Telecommunications, Beijing, China
xinpengtian923@gmail.com

Abstract. With the widespread application of Internet of Things (IoT) technology in the field of telecommunications engineering, security issues such as network attacks, privacy leakage, and system vulnerabilities have become increasingly prominent, which have become important challenges restricting the development of the Internet of Things and the integration of telecommunications infrastructure. This paper systematically analyzes the research background and current situation of IoT security at home and abroad from the application scenarios of telecommunications engineering, focuses on the classification and overview of IoT security technology, and analyzes the problems and countermeasures in security practice based on typical cases. This paper also delves into the technical challenges and development trends faced by IoT security in telecommunications engineering. The results show that the requirements of telecom engineering for IoT security are characterized by large-scale, high concurrency, heterogeneous access and low latency, which need to be coordinated in multiple dimensions such as system architecture design, protocol standards, offensive and defensive confrontation and regulatory compliance.

Keywords: Telecommunications engineering, Internet of Things, Cybersecurity, Case study, Development trend

1. Introduction

As an important part of the new generation of information technology, the Internet of Things (IoT) is profoundly changing the form and connotation of telecommunications engineering. With the rapid development of technologies such as 5G, edge computing, cloud computing, and big data, telecom operators are not only network builders and managers, but also providers and ecosystemcultivators of IoT platforms. However, the proliferation of IoT has also brought unprecedented security challenges. According to a report published by the International Telecommunication Union (ITU), the number of IoT devices worldwide is expected to exceed 25 billion by 2030. Therefore, strengthening the research on IoT security is of great significance for building a new information infrastructure for security.

The research on IoT security started early, and many countries have accumulated rich experience in standard formulation, offensive and defensive technology, and industrial ecology. Several organizations have issued multiple IoT security guidelines, which put forward requirements for device security, network security, data security, and lifecycle management. In addition, some

DOI: 10.54254/2755-2721/2025.GL26240

countries have established national IoT security certification frameworks. At the level of technical research, scholars focus on lightweight encryption algorithms, scalable key management, intrusion detection, blockchain tamper-proof, etc. Many enterprises have launched IoT security solutions to achieve unified management and security protection in large-scale deployments [1].

This paper explores the research status of IoT security technology by using the method of literature review, and analyzes the current security problems and development trends. It aims to provide theoretical support and practical reference for the security construction of IoT in the telecommunications industry.

2. Theoretical overview

2.1. Application scenarios of IoT in telecommunications engineering

In the field of telecommunications engineering, the Internet of Things has a wide range of application scenarios, covering smart cities, smart grids, Internet of Vehicles, industrial Internet, and telemedicine. In smart cities, telecom operators connect smart street lights, parking management systems, and water and electricity meter reading equipment through cellular networks such as NB-IoT and 5G to achieve intelligent and refined urban management. In the field of smart grids, power companies rely on telecommunications networks to achieve large-scale intelligent meter reading, load management, and distributed energy scheduling to improve grid operation efficiency and safety. The Internet of Vehicles (V2X) application is based on 5G C-V2X technology, which requires low-latency and high-reliability network support, and the telecom network undertakes the millisecond-level communication requirements between vehicles and vehicles and roadside units to ensure traffic safety and intelligent driving. In the industrial Internet scenario, telecom operators provide 5G private networks, edge computing, and secure access services for factories and industrial parks, supporting production process digitalization, remote operation and maintenance, and intelligent manufacturing. In telemedicine, 5G and the Internet of Things combine to support high-definition video diagnosis, remote surgery, and remote health monitoring, placing high requirements on network bandwidth, reliability and security. The common characteristics of these diverse application scenarios are the large number of terminalaccesses, wide distribution, and heterogeneous device types, which pose unprecedented challenges to the management capabilities and security protection levels of telecommunications networks [2].

2.2. Basic scope of IoT security technology

The application of IoT security technology in telecommunications engineering mainly covers multiple levels such as equipment, communication, network, platform and application, and security management, forming a multi-level and three-dimensional protection system. At the device level, security technology includes hardware-level tamper-proof design, secure boot mechanism, security chip embedding, and firmware trusted updates to ensure the security of the terminal at the physical level. At the communication level, it pays attention to the confidentiality and integrity of data during transmission, and usually uses lightweight encryption algorithms, identity authentication protocols, key negotiation mechanisms, and end-to-end encryption to ensure the security of data transmission in complex heterogeneous network environments. Network security technology focuses on border protection and attack detection, including security gateways, firewalls, intrusion detection and prevention systems (IDS/IPS), traffic anomaly analysis tools, etc., to resist common network-layer attacks such as denial-of-service attacks, malicious scanning, and ARP spoofing. At the platform and

DOI: 10.54254/2755-2721/2025.GL26240

application level, security policies involve user identity management, access rights control, encrypted storage of sensitive data, application vulnerability scanning, and automatic patch update mechanisms to avoid illegal operations or data leakage caused by platform software vulnerabilities. In addition, with the expansion of the scale of IoT systems and the increase in management complexity, security management and monitoring have become the key to ensuring the overall security of the system. In short, the IoT security technology system presents the characteristics of hierarchical collaboration, dynamic update, and integration of software and hardware, and only by realizing a security closed loop at all levels can it meet the high security and high availability requirements of telecommunications engineering for large-scale IoT access [3].

3. Research progress

3.1. Safety issues and improvements of smart meter systems

Smart meters are an important scenario for large-scale deployment by telecom operators in the field of IoT, mainly through NB-IoT or 4G networks to achieve data meter reading, power consumption analysis and remote control. Early smart meter designs often failed to introduce dedicated security chips or end-to-end encryption mechanisms to minimize costs, resulting in a wide attack surface and easy to crack. For example, in 2018, a foreign research team demonstrated an attack method to infer key information from smart meters through electromagnetic side channel analysis, and inject malicious backdoor programs through firmware upgrade interfaces to tamper with electricity consumption data and bypass the charging system. Such security vulnerabilities not only cause financial losses but can also be exploited on a large scale to launch denial-ofservice attacks, affecting the normal operation of the power system. In order to cope with these problems, domestic power companies have introduced secure boot mechanisms, secure element chips, firmware signature verification and periodic key rotation mechanisms in subsequent smart meter upgrade projects. Telecom operators have also built a unified secure access authentication platform based on NB-IoT links to realize end-to-end encrypted communication of meters and effectively prevent data from being stolen or tampered with during transmission. However, such system upgrades are accompanied by problems such as rising deployment costs and complex key management, and there is an urgent need for standardized solutions and ecological collaboration to reduce the difficulty of security operation and maintenance throughout the life cycle [4].

3.2. Research and practice of Internet of Vehicles communication security

The Internet of Vehicles (V2X) is considered the core support of the future intelligent transportation system, requiring telecommunications networks to provide low-latency and highreliability communication capabilities to ensure safe driving. Security has become a common concern in several pilot projects in the United States, the European Union and China. In order to reduce communication overhead, the early DSRC (Dedicated Short-Range Communication) and C-V2X standards often lacked strong identity authentication and end-to-end encryption, resulting in attackers forging legitimate nodes to broadcast false traffic information, inducing misjudgments in rear vehicles, and even causing traffic accidents. In addition, replay attacks and man-in-themiddle attacks have also been verified as viable threats in actual tests, and attackers can intercept and replay emergency braking messages and disrupt normal driving order. In response to these risks, NHTSA has promoted the establishment of a PKI (public key infrastructure)-based security certificate management system, assigning verifiable identity certificates to each vehicle, and introducing digital

DOI: 10.54254/2755-2721/2025.GL26240

signature mechanisms at the message layer to achieve source authentication and integrity protection. China has also clearly incorporated security certificates, privacy protection, and key management into the system design in the C-V2X standard, and has conducted pilot verification in many places, including multi-factor identity authentication, key rotation, and pseudonymous certificate mechanisms, aiming to balance the contradiction between security and communication latency in large-scale deployment. Telecom operators not only provide private network slicing and low-latency links in Internet of Vehicles projects, but also need to support security certificate distribution, remote updates, and threat detection capabilities, which puts forward higher requirements for the construction of their security management platforms [5].

3.3. Security attack and defense cases in the industrial internet

Operators provide high-bandwidth, low-latency, and security-isolated network services for manufacturing enterprises through the construction of 5G private networks, edge computing nodes, and VPN tunnels. However, the security challenges of the industrial Internet far exceed those of traditional IT systems, and most of the Operational Technology (OT) devices in its production environment are old systems and lack security update mechanisms, making it difficult to resist modern cyber attacks. In 2021, the industrial Internet platform deployed by a large domestic steel company suffered a ransomware attack, and the attacker obtained the VPN credentials of operation and maintenance personnel through spear phishing emails, successfully broke through the remote access entrance provided by the telecom operator, and moved laterally within the industrial control network, and finally encrypted the key production control system files, resulting in the production line being forced to shut down. The investigation showed that the system lacked multi-factor authentication and fine-grained access control, and the security log audit and alarm mechanism failed to detect intrusion traces in a timely manner. Such incidents have prompted telecom operators to introduce zero-trust security architectures when building 5G private networks for industrial customers, deploy multi-factor authentication, fine-grained access control, microisolation technology, security operation and maintenance audits, and provide continuous security monitoring and threat intelligence sharing services to help enterprises improve their overall defense capabilities.

3.4. Reference of international IoT security solutions

International telecommunications and IT giants provide integrated solutions in the field of IoT security, with high maturity and scalability. For example, Cisco's IoT. The Threat Defense platform can implement traffic segmentation and security policy distribution on the network side of telecom operators, and can identify abnormal traffic and block attacks bycombining intrusion detection systems (IDS), sandbox analysis, and situational awareness dashboards. IBM's Watson IoT platform includes built-in security event management (SIEM), identity and access management (IAM), and data encryption modules to support end-to-end security and compliance auditing. In addition, the European Union Agency for Cybersecurity (ENISA) and the National Institute of Standards and Technology (NIST) has published security frameworks and technical guidelines specifically for the Internet of Things, providing security requirements for the entire life cycle from design principles to operation and maintenance management. In contrast, our country's telecom operators have also vigorously promoted the construction of IoT security platforms in recent years, such as China Mobile's OneNET security management platform, NB-IoT secure access authentication platform and 5G private network security solutions, which have integrated security management and control capabilities across access technologies. However, there is still a gap between the international

DOI: 10.54254/2755-2721/2025.GL26240

advanced level in terms of security chip coverage, end-to-end encryption penetration, and threat intelligence sharing mechanism, and needs to be continuously improved in terms of standardization, upstream and downstream ecological cooperation, and supply chain security management [6].

4. Challenges and development trends

4.1. Key security challenges

IoT deployments in telecom engineering are huge, with a wide variety of terminals, manufacturers, and protocol standards. The coexistence of diverse access technologies from NB-IoT to 5G, Wi-Fi, Bluetooth, LoRa, and other diverse access technologies makes it difficult to achieve consistent distribution and automated execution of security policies across the network. Especially in the uneven distribution of urban and rural areas, it is difficult to upgrade equipment and lag behind in updating security patches for old equipment, forming long-term potential security hazards [7].

A large number of low-cost IoT devices have limited computing power, limited storage space, and limited battery power, making it difficult to deploy traditional encryption algorithms or complex authentication protocols. Common public-key encryption algorithms such as RSA or ECC can be too "heavy" for these devices, leading developers to choose weak passwords, hardcoded keys, orsimply omit encrypted communications, making them easy entry points for attackers to break through. Although progress has been made in the research and development of lightweight security protocols, it still faces resistance at the level of standardization and popularization of applications, requiring more resources from all parties in the industrial chain to collaborate on key problems.

IoT devices are usually produced through complex global supply chains, covering chip design, firmware development, system integration, third-party components, and other links. Attackers may implant hardware backdoors or malicious firmware during the manufacturing process, forming "hard wounds" that are difficult to completely detect and eliminate even in later O&M. In the field of IoT, due to fragmented manufacturers and fierce price competition, secure traceability and authentication have not yet formed a feasible universal mechanism [8].

Telecommunications networks are the underlying infrastructure that carries a variety of key services such as smart cities, Internet of Vehicles, and industrial Internet. Once the security policy is weak, attackers may use an IoT terminal as a "springboard" to enter the telecom core network, cloud platform, or third-party business system to achieve complex chain attacks such as horizontal movement, data theft, and DDoS attacks. For example, the Mirai botnet exploited millions of IoT devices with weak password vulnerabilities around the world to launch large-scale distributed denial-of-service attacks, resulting in disruptions to major telecommunications services. With the slicing of 5G networks, edge computing nodes, and the deployment of MEC platforms, the attack surface becomes more dispersed, and the difficulty of security monitoring increases [9].

4.2. Development trends and cutting-edge research directions

To solve the problem that resource-constrained devices are difficult to carry traditional encryption algorithms, academia and industry are actively developing lightweight symmetric encryption, public key cryptography, and hashing algorithms. These protocols are designed to balance security and compute/energy overhead for true end-to-end encrypted communication. At the same time, standardization organizations are also promoting security extensions of IoT communication protocols to natively integrate security features into application layer protocols to reduce the security design burden for developers.

DOI: 10.54254/2755-2721/2025.GL26240

Blockchain, with its decentralized, traceable, and tamper-proof nature, is seen as a potential technological path to address IoT device authentication, access control, and supply chain security.Implement a distributed PKI system through blockchain to avoid single points of failure and trust risks caused by traditional centralized CAs. Smart contracts can be used to achieve automatic security policy negotiation and auditing between devices. Although the current throughput and storage overhead of blockchain limit large-scale implementation, it has been piloted in high-value, low-frequency transaction IoT scenarios, and telecom operators can provide it to industry customers as part of security services [10].

As the complexity and attack surface of IoT environments continue to expand, using artificial intelligence and machine learning technology, abnormal patterns can be mined in massive network traffic, log data, and user behavior to achieve behavior-based threat detection and automatic response. The federated learning framework can realize multi-party threat intelligence sharing and model collaborative training under the premise of protecting user privacy. As the "hub" of network traffic, telecom operators have unique network-wide visibility capabilities, and are expected to build an AI-driven security situational awareness platform to enhance the awareness and defense capabilities against distributed attacks and new threats.

5. Conclusion

With the widespread deployment of IoT in telecommunications engineering, security has become a core challenge for its sustainable development. The heterogeneous access, large-scale terminals, and cross-industry applications of the Internet of Things have led to the diversification and complexity of security threats. At present, positive progress has been made in research on lightweight encryption, end-to-end secure communication, identity authentication, situational awareness, etc., but it still faces problems such as limited equipment resources, inconsistent standards, difficult control of supply chain security, and increased pressure on privacy protection. As a key player in IoT access and bearing, telecom operators must build a multi-level, full-life cycle security system, strengthen security management platforms and threat monitoring capabilities, and promote the implementation of standardized, zero-trust architectures and AIdriven defense technologies. In the future, only by collaborative innovation and strengthening regulatory supervision and compliance governance can we build a safe, credible and sustainable telecommunications Internet of Things ecosystem and support the high-quality development of the digital economy.

However, there are still some shortcomings in this paper. Firstly, there is a lack of in-depth case studies and empirical data support. Second, the special needs of different regions and industries are not fully considereds. These deficiencies provide a direction for improvement in subsequent research, which can further deepen the understanding of IoT security through more systematic empirical research and diversified perspectives in the future.

References

[1] Qian, Z. H., & Wang, Y. J. (2012). Research on IoT Technology and Applications.
[2] Wu, C. K. (2015). Key technologies and challenges in IoT security. Journal of Cryptologic Research, 2(1), 40-53.
[3] Ande, R., Adebisi, B., Hammoudeh, M., et al. (2020). Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society, 54, 101728.
[4] Suo, H., Wan, J., Zou, C., et al. (2012). Security in the internet of things: a review. In 2012 International Conference on Computer Science and Electronics Engineering (Vol. 3, pp. 648-651). IEEE.
[5] Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems, 67(3), 423-441.

DOI: 10.54254/2755-2721/2025.GL26240

[6] Zhu, H. B., Yang, L. X., & Yu, Q. (2010). Research on the technical concept and application strategy of IoT. Journal of Communications, (11), 2-9.
[7] Bakar, K. B. A., Zuhra, F. T., Isyaku, B., et al. (2023). A review on the immediate advancement of the internet of things in wireless telecommunications. IEEE Access, 11, 21020-21048.
[8] Li, K. H., & Li, W. Q. (2025). Research on the application of artificial intelligence in the operation and maintenance of telecommunications engineering. Information and Computer, 37(1), 113-115.
[9] Liu, Y. (2024). Research on network security and privacy protection technology in telecommunications engineering. Information Recording Materials, 25(6), 80-82. https: //doi.org/10.16009/j.cnki.cn13-1295/tq.2024.06.037
[10] Baskaran, S. B. M., Arumugam, S., & Prasad, A. R. (2019). Internet of things security. Journal of ICT Standardization, 7(1), 21-42.