Proceedings of the 3rd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/138/2025.21359

Research on Secure Communication in the Internet of Things

Shilin Geng[1,a], Elena I. Kozlova[1,b,*]

[1]*The Faculty of Radiophysics and Computer Technologies, Belarusian State University, 4 Nezavisimosti Ave, 220030, Minsk, Republic of Belarus*
a. gengshilinzz@gmail.com, b. elena.kozlova1310@gmail.com
**corresponding author*

Abstract: With the widespread penetration of the Internet of Things in various fields, its secure communication issues have become a key factor restricting the further development of the Internet of Things. This study deeply analyzes the many challenges faced by secure communications in the Internet of Things, including security risks of IoT cards , difficulties at the device and network levels, etc. The role of key technologies such as identity authentication, encryption, security analysis and threat prediction in ensuring secure communications in the Internet of Things is elaborated in detail. At the same time, the development trend of secure communications in the Internet of Things is discussed, such as the gradual improvement of standards and specifications and the application prospects of new technologies in security protection. Finally, strategies for dealing with secure communications issues in the Internet of Things from the technical level, management and cooperation level are proposed, aiming to provide comprehensive reference and guidance for research and practice in the field of secure communications in the Internet of Things, and promote the healthy and sustainable development of the Internet of Things industry.

Keywords: IOT, secure communications, security challenges, trend

1. Introduction

In today's digital age, the Internet of Things (IoT) technology has shown an explosive growth trend and is widely used in many fields such as industrial manufacturing, smart homes, smart transportation, and healthcare. According to relevant statistics, the number of connected IoT devices worldwide is increasing by billions every year. By connecting various physical devices to the Internet, the IoT realizes data interaction and collaborative work between devices, greatly improving production efficiency and improving people's quality of life. For example, in the scenario of Industry 4.0, the interconnection between smart sensors, robots and other equipment in the factory realizes the automation and intelligent monitoring of the production process; in the smart home environment, users can remotely control home appliances through mobile phones to achieve convenient home management. However, the widespread application of the Internet of Things has also brought unprecedented security challenges. As the cornerstone of ensuring the stable operation of the entire Internet of Things system, the importance of IoT secure communication is self-evident. Once the security of IoT communication is threatened, it may lead to serious consequences such as user privacy leakage, enterprise production interruption, and paralysis of critical infrastructure. For example, IoT

DOI: 10.54254/2755-2721/138/2025.21359

medical devices have been hacked due to communication security vulnerabilities, resulting in the theft of patients' medical data, which seriously infringes on patients' privacy rights; in intelligent transportation systems, if the communication between vehicles is maliciously interfered with, it may cause traffic accidents and endanger the safety of life and property[1].Therefore, in-depth research on IoT secure communications and exploration of effective security protection mechanisms and development strategies are of great practical significance for promoting the healthy and stable development of the IoT industry.

2. Challenges of secure communication in IoT

2.1. Security risks related to IoT cards

IoT cards serve as the linchpin for IoT devices to establish network connections. However, this crucial role exposes them to a plethora of security risks. In recent years, the frequency of data leakage incidents associated with IoT cards has been on the rise, sending shockwaves through various industries. One particularly notable case involves a large e-commerce company. Its logistics IoT system, which heavily relied on IoT cards for device connectivity, fell victim to a malicious hack. As a result, a vast amount of sensitive user data, including order details, delivery addresses, and payment information, was leaked. This incident had far-reaching consequences. It not only severely violated the personal privacy of countless users but also dealt a heavy blow to the company's reputation. The company faced public outcry, with customers losing trust in its ability to safeguard their data. Moreover, it was plunged into a legal quagmire, facing potential lawsuits from affected users and regulatory investigations.

The security risks of IoT cards are predominantly manifested in two key areas: data leakage and unauthorized access. IoT cards are often linked to a staggering volume of sensitive data. Device operation data, which can reveal crucial information about how a device functions, its usage patterns, and potential vulnerabilities, is stored and transmitted through these cards. Additionally, user identity information, such as names, social security numbers, and contact details, is also associated with IoT cards. This rich trove of data makes IoT cards highly attractive targets for hackers.

Furthermore, the widespread distribution of IoT cards in the network makes them extremely difficult to manage effectively. They are deployed in diverse environments, from industrial settings to residential homes, and from remote monitoring stations to mobile vehicles. This dispersion, combined with the large number of cards in use, makes it challenging for organizations to keep track of their security status. Regular security audits and updates become cumbersome tasks, leaving many IoT cards vulnerable to attack. Hackers can exploit these weaknesses to gain unauthorized access to the data stored on or transmitted through the cards. They can intercept data packets in transit, modify the data, or steal it outright, leading to data leakage and potential misuse.

2.2. Challenges at the device and network levels

2.2.1. Device-level challenges

The device level in the IoT ecosystem presents a complex and multi-faceted set of challenges for secure communication. The diversity and complexity of IoT devices are at the heart of these issues. Consider the example of a casino's IoT thermostat. Hackers were able to exploit vulnerabilities in this seemingly innocuous device. They gained access to the thermostat and then used it as a gateway to infiltrate the casino's internal network. Once inside, they were able to steal a significant amount of financial data and customer information, causing substantial financial losses and reputational damage to the casino.

DOI: 10.54254/2755-2721/138/2025.21359

One of the primary reasons for the vulnerability of IoT devices is their limited resources. Many IoT devices are designed to be small, low-power, and cost-effective. As a result, they often lack the computing power, memory, and storage capacity required to implement complex security protection mechanisms. Advanced encryption algorithms, intrusion detection systems, and real-time threat monitoring tools, which are standard in more powerful computing devices, are often beyond the capabilities of IoT devices. This makes them easy targets for hackers who can quickly identify and exploit their weaknesses.

Moreover, security updates for IoT devices are often not timely. Manufacturers may prioritize new product development over maintaining and updating the security of existing devices. In some cases, they may not even provide security updates for older models, leaving them exposed to emerging threats. Additionally, the process of pushing security updates to a large number of dispersed IoT devices can be logistically challenging. Devices may be offline, in hard-to-reach locations, or have limited connectivity, making it difficult to ensure that all devices receive the necessary updates.

Another significant issue at the device level is compatibility problems. IoT devices are produced by a multitude of manufacturers, each with their own design standards, communication protocols, and security features. This lack of standardization leads to compatibility issues when different devices are integrated into a single IoT system. These compatibility problems can create security vulnerabilities, as hackers can exploit the differences in device security mechanisms to gain unauthorized access.

2.2.2. Network-level challenges

At the network level, the rapid growth in the number of IoT devices has brought about a host of challenges for secure communication. The sheer volume of IoT devices connected to the network has placed an enormous strain on network bandwidth. As more and more devices transmit data, the available bandwidth becomes saturated, leading to unstable connections and slow data transfer speeds. This not only affects the performance of IoT applications but also creates opportunities for attackers to disrupt or intercept data transmissions.

In addition to bandwidth issues, the lack of a robust regulatory mechanism in the IoT field is a major concern. The IoT ecosystem is relatively new and has evolved at a breakneck pace, outpacing the development of comprehensive regulations. This regulatory gap means that there are few standards and guidelines in place to govern the security of IoT devices and networks. As a result, some manufacturers may cut corners on security to reduce costs or speed up product development. Malicious actors can take advantage of this lack of oversight to introduce malicious devices into the network or engage in illegal communication behaviors. These malicious devices can be used to launch attacks on other devices, steal data, or disrupt network operations.

Furthermore, the decentralized nature of IoT networks makes it difficult to enforce security policies. In traditional network architectures, there are central points of control that can be used to monitor and manage network traffic. However, in IoT networks, devices are often connected in a peer-to-peer or mesh topology, making it challenging to identify and isolate malicious activities. Without a comprehensive regulatory framework and effective security management strategies, the risk of secure IoT communications will continue to increase, threatening the integrity, confidentiality, and availability of data in the IoT ecosystem.

In conclusion, the challenges of secure communication in IoT, both at the IoT card level and at the device and network levels, are significant and complex. Addressing these challenges will require a concerted effort from manufacturers, service providers, regulators, and researchers to develop and implement robust security solutions, standardize security practices, and enforce strict regulations. Only then can we ensure the safe and reliable operation of IoT systems and protect the privacy and security of users and organizations.

DOI: 10.54254/2755-2721/138/2025.21359

3. Key technologies for secure communication in IoT

3.1. Identity Authentication Technology

Identity authentication is an important means to ensure the legitimacy and security of IoT devices. In the field of smart healthcare, for example, when various medical devices in hospitals are connected to the medical network, strict identity authentication is required. The use of two-factor authentication, that is, combining the device hardware identification (such as the device serial number) and the dynamic password (such as a one-time verification code), can effectively prevent the access of illegal devices. At the same time, biometric technology is also gradually being applied to the field of IoT identity authentication. For example, some high-end medical devices identify the fingerprint or iris information of medical staff to ensure that only authorized personnel can operate the equipment. Through these identity authentication technologies, the identity of the device can be accurately identified when the device is connected to the network to prevent illegal access, thereby ensuring the security of IoT communications.

3.2. Encryption Technology

Encryption technology plays a vital role in secure communication in the Internet of Things. Different types of IoT devices may require different encryption algorithms and key management strategies, which increases the difficulty and complexity of managing encryption technology[3]. Symmetric encryption technology, such as AES, uses the same key for encryption and decryption, which is efficient but complex to manage. Asymmetric encryption technology, such as RSA, uses public keys for encryption and private keys for decryption, which solves the key distribution problem but has high computational overhead. Hash functions, such as SHA-256, can generate a unique summary of data for verifying data integrity. Digital certificates are based on asymmetric encryption and are issued by authoritative organizations to ensure that the device identity is authentic. There are also encryption algorithms based on elliptic curves, which are more efficient and secure. During the transmission process, tunnel encryption technology is used to establish a secure channel. In addition, lightweight encryption algorithms are designed for resource-constrained devices in the Internet of Things, taking into account both security and low energy consumption. These technologies work together to ensure that data in the Internet of Things is confidential, complete, authentic, and available, and resist various security threats.

3.3. Security analysis and threat prediction technology

In the face of increasingly complex IoT security threats, security analysis and threat prediction technology has become a key line of defense to ensure secure IoT communications. For example, in an incident where a global IoT suffered a large-scale cyber attack, the lack of an effective security analysis and threat prediction mechanism resulted in the inability to take effective countermeasures in a timely manner after the attack occurred, causing huge losses. Security analysis and threat prediction technology monitors and analyzes various security-related data in IoT systems in real time, such as device logs, network traffic data, etc., and uses advanced algorithms and artificial intelligence applications, such as cluster analysis and anomaly detection algorithms in machine learning algorithms, to detect potential security threats in a timely manner and predict possible future attacks. This provides strong support for IoT systems to take defensive measures in advance and effectively reduces security risks.

DOI: 10.54254/2755-2721/138/2025.21359

4. Development Trend of IoT Security Communications

4.1. Gradual improvement of standards and specifications

As IoT security issues become increasingly prominent, governments and international organizations have stepped up their efforts to develop IoT security standards and specifications. For example, the Internet of Things Label Program, a network trust mark launched by the White House in the United States, aims to establish a unified set of security standards and certification mechanisms for IoT devices. Through this program, consumers can more intuitively understand the security performance of IoT devices and make more informed purchasing decisions. At the same time, the International Organization for Standardization (ISO) is also actively developing IoT security-related standards, such as the application expansion of the ISO/IEC 27000 series of standards in IoT security management. The gradual improvement of these standards and specifications will prompt IoT device manufacturers and service providers to pay more attention to the standardization of secure communication protocols and strengthen the protection of user privacy, thereby providing a more solid institutional guarantee for IoT secure communications.

4.2. New technologies help with security protection

The continuous emergence of emerging technologies has brought new opportunities for IoT security communications. Machine learning technology has broad application prospects in IoT security protection. By conducting machine learning training on the normal operation data of a large number of IoT devices, a device behavior model can be established. When a device exhibits abnormal behavior, such as a sudden increase in data traffic or a long device response time, the machine learning-based security detection system can detect and issue an alarm in a timely manner[4].In addition, with the widespread application of open source software in the field of IoT, open source security issues are also receiving increasing attention. In the future, the IoT industry will pay more attention to the security management of open source software. By establishing an open source security vulnerability monitoring platform and strengthening open source code audits, security vulnerabilities in open source software can be discovered and repaired in a timely manner, thereby reducing security risks caused by open source software.

5. Strategies for addressing IoT secure communication issues

In the contemporary digital age, the Internet of Things (IoT) has emerged as a revolutionary force, seamlessly integrating various devices and systems to enhance efficiency and convenience. However, the security of communication within the IoT ecosystem has become a critical concern that demands immediate and effective strategies.

5.1. Technical aspects

On the technical level, IoT companies have a plethora of measures at their disposal to guarantee secure communications. Regular updates of the software system of IoT cards are of paramount importance. By promptly addressing known security vulnerabilities, the potential risks of unauthorized access and data breaches can be significantly mitigated. For instance, IoT card manufacturers can leverage over-the-air (OTA) technology to push security patches to user devices. This not only ensures the timeliness of security enhancements but also simplifies the update process for users, reducing the likelihood of their devices remaining exposed to known threats.

Establishing a secure communication channel is another crucial aspect. The utilization of technologies such as virtual private networks (VPNs) and transport layer security protocols (TLS)

DOI: 10.54254/2755-2721/138/2025.21359

provides robust encryption and protection for data transmission between IoT devices. These technologies create a secure tunnel, shielding the data from interception and tampering during transit. Moreover, continuous vulnerability scanning and repair work on IoT devices are essential. Regular security inspections should be conducted on these devices to proactively identify and rectify security risks. This could involve comprehensive checks for software and hardware vulnerabilities, as well as ensuring that the devices' firmware and operating systems are up to date.

5.2. Management and co-operation level

In addition to the technical strategies, management and cooperation strategies play an equally vital role in addressing IoT secure communication issues. At the management and cooperation level, IoT companies must forge strong partnerships with regulatory agencies. By actively responding to relevant policies and regulations, they can contribute to the standardized development of IoT secure communications. For example, the establishment of an IoT security monitoring platform in collaboration with regulatory agencies allows for real-time monitoring of the operational status and communication security of IoT devices. This enables prompt detection and response to any potential security incidents, minimizing the impact and damage.

Formulating a comprehensive IoT device management strategy is also indispensable. Clearly defining the security responsibilities at each link, including equipment procurement, deployment, and maintenance, ensures that all aspects of the IoT ecosystem are covered. This clarity helps prevent any ambiguity or oversight in security measures and promotes a coordinated and effective security framework.

Furthermore, conducting training and education activities on IoT security is of great significance. By enhancing the security awareness of enterprise employees and users, they become better equipped to understand the importance of IoT secure communications and the fundamental knowledge of security protection. This empowers them to make informed decisions and take appropriate actions to safeguard the integrity and confidentiality of data within the IoT environment.

In conclusion, addressing the challenges of IoT secure communication requires a multi-faceted approach that combines technical prowess with effective management and collaborative efforts. Only through such a holistic strategy can we ensure the seamless and secure operation of the Internet of Things, unlocking its full potential while safeguarding the interests and privacy of users.

6. Conclusion

This study comprehensively and deeply explores the relevant issues in the field of secure communication of the Internet of Things. Through a detailed analysis of the challenges faced by secure communication of the Internet of Things, including the security risks of IoT cards and many difficulties at the device and network levels, the current severe situation of secure communication of the Internet of Things is clarified. The important role and application principles of key technologies such as identity authentication, encryption, security analysis and threat prediction in ensuring secure communication of the Internet of Things are explained, providing a theoretical basis for the technical guarantee of secure communication of the Internet of Things. The development trend of secure communication of the Internet of Things is discussed, such as the gradual improvement of standards and specifications and the application prospects of new technologies in security protection, which points out the direction for the future development of secure communication of the Internet of Things.

With the continuous innovation and development of IoT technology, IoT secure communication will face more new challenges and opportunities. For example, the development of quantum computing technology may have an impact on existing encryption technology. IoT secure communication needs to explore new encryption mechanisms to deal with the threats brought by

DOI: 10.54254/2755-2721/138/2025.21359

quantum computing. At the same time, with the deep integration of IoT with emerging technologies such as edge computing and 5G, how to ensure secure communication across technology fields will become the focus of future research. In addition, establishing a more unified and complete IoT secure communication standard system on a global scale and strengthening international IoT security cooperation and exchanges will also be important directions for the future development of IoT secure communication [7]. We look forward to continuously overcoming the difficulties in the field of IoT secure communication in future research and practice, and achieving the safe and sustainable development of the IoT industry.

References

[1] *Gui Zhuang. Research on cryptographic application technology for secure communication in Internet of Vehicles[D]. University of Electronic Science and Technology of China, 2020. DOI: 10.27005/d.cnki.gdzku.2020.000382.*

[2] *Gao Yun. Research on lightweight secure communication protocol for ubiquitous Internet of Things[D]. East China Normal University, 2022. DOI: 10.27149/d.cnki.ghdsu.2022.000447.*

[3] *Chen Jiasheng, Wang Liangliang. Research and Prospect of Smart Home Communication Security[J]. Journal of Shanghai University of Electric Power, 2021, 37(01): 67-72.*

[4] *Li Mingshi. Research on key technologies of secure communication of industrial Internet of Things[D]. University of Chinese Academy of Sciences (Shenyang Institute of Computing Technology, Chinese Academy of Sciences), 2022. DOI: 10.27587/d.cnki.gksjs.2022.000001.*

[5] *Luo Hanguang. Research on lightweight security protocols and key technologies for the Internet of Things[D]. University of Electronic Science and Technology of China, 2019.*

[6] *Zhu Jingwen, Liu Qingmei, Cao Zhiyuan. Design and evaluation of secure communication protocols in the Internet of Things environment[J]. China Informatization, 2024, (10): 92+78.*

[7] *Zhang Gang. Research on information security and privacy protection of the Internet of Things[J]. China Information Industry, 2024, (06): 40-42.*