Proceedings of CONF-MLA 2025 Symposium: Intelligent Systems and Automation: AI Models, IoT, and Robotic Algorithms
DOI: 10.54254/2755-2721/2025.LD30447

Security Threats and Protection Strategies for Camera-Based Internet of Things Devices

Weiqing Yan

Tsinghua International School, Beijing, China
snookerboy007@163.com

Abstract. Camera-based Internet of Things (IoT) devices are now a common part of daily life and industry, supporting smart homes, public safety, and manufacturing. As these devices become more widespread, they face growing cybersecurity risks, such as data leaks, unauthorized access, and large-scale attacks like DDoS. This paper analyzes security threats and protection strategies for camera-based IoT devices across the three main layers of IoT architecture: perception, network, and application. The study identifies key vulnerabilities and suggests practical defense methods. By reviewing literature, examining case studies, and comparing different approaches, the research looks at real-world attacks and assesses common protection tools, including lightweight encryption, authentication, and AI-based intrusion detection. The results show that IoT security needs both layer-specific and coordinated defenses, with protection built in throughout the device's life cycle. The study also finds that future IoT security will depend more on smart, flexible, and privacy-focused technologies, such as edge security and federated learning, to better handle new threats.

Keywords: Internet of Things (IoT), Security Threat, Protection Strategy

1. Introduction

In today's rapidly developing information age, the Internet of Things (IoT) has become a key medium that integrates all things in the physical world with the digital space. IoT technologies and products are widely used in areas such as smart homes, industrial manufacturing, urban security, and healthcare, transforming the way people live and work. Through these IoT devices, human life is entering an entirely new state.

However, the explosive growth of IoT has also exposed hidden security risks. Some manufacturers, lacking sufficient awareness of cybersecurity, often prioritize reducing production costs and improving performance over establishing sound security architectures. As a result, issues such as weak passwords, firmware vulnerabilities, and unencrypted data transmission remain prevalent. For camera-based IoT devices in particular, these problems are closely tied to personal privacy and even public safety. Once such devices are compromised, they can directly endanger many aspects of daily life. Therefore, enhancing the security of camera-based IoT devices is of great necessity and plays a crucial role in safeguarding the overall security of IoT systems.

This paper focuses on the security of camera-based IoT devices. It examines the typical threats faced at each layer of the IoT's three-layer architecture, analyzes the adaptability of mainstream

DOI: 10.54254/2755-2721/2025.LD30447

protection technologies, and explores systematic defense strategies.

The study adopts a literature analysis approach to establish a theoretical foundation, a case analysis method to dissect representative security incidents, and a comparative analysis to clarify the positioning of different defense technologies. The findings of this research provide useful references for helping users mitigate related risks and for promoting higher security standards within the industry.

2. IoT framework and basic security requirements

The three-layer architecture of the Internet of Things (IoT) forms the foundation of its operation. It consists of the perception layer, the network layer, and the application layer, each with its own functional roles and corresponding security threats.

The perception layer serves as the channel for data collection, primarily composed of sensors, cameras, and Radio Frequency Identification (RFID)devices. Common security issues at this layer include: sensors being deliberately damaged, RFID tags being duplicated, and cameras being attacked through software vulnerabilities—leading to image leaks or even remote control of the visual feed.

The network layer transmits data through communication technologies such as Wi-Fi and Bluetooth. The major risk at this level lies in the vulnerability of data transmission—wireless signals can be easily intercepted, resulting in the leakage of private camera footage. Transmission protocols may also contain security flaws that could be exploited for data tampering. Additionally, Distributed Denial of Service(DDoS)attacks can cause nodes to crash, severely disrupting normal data transmission.

The application layer involves user interaction interfaces that manage and report various types of data. Security issues at this layer include: platform databases being breached, leading to theft of user information associated with camera devices; vulnerabilities in access control mechanisms that allow unauthorized individuals to gain control over devices; and logical flaws that interfere with normal device operation.

The basic security requirements of IoT include ensuring that data is not accessed by unauthorized parties (for example, encrypting image data during transmission), maintaining the authenticity of data (such as verifying sensor readings), ensuring the availability and normal operation of devices, authenticating legitimate users, and protecting user information from misuse. These elements collectively form the core principles of IoT security.

3. Typical security threats and attack methods

Today, as the Internet of Things (IoT) develops rapidly, various security issues and attack techniques have increasingly threatened system integrity and user interests.

At the perception layer, device impersonation is a common problem. Attackers exploit the fact that IoT device IDs can be easily forged. In smart home environments, they may create counterfeit smart appliances by imitating legitimate device identifiers such as MAC(Media Access Control) addresses, serial numbers, service procedures or signaling information, and embedded system port numbers. These fake devices can then access the home network to steal private data, including footage from household cameras [1]. Another major threat at the perception layer is physical damage. Attackers can dismantle outdoor monitoring sensors or critical sensing equipment on industrial production lines, thereby disrupting system operations. Malfunctions in sensor performance may lead to the partial failure of system functions, resulting not only in significant

DOI: 10.54254/2755-2721/2025.LD30447

financial losses but also in the interruption of enterprises' autonomous decision-making processes [2].

At the network layer, Man-in-the-Middle (MITM) attacks pose a serious threat. By using methods such as ARP spoofing and DNS hijacking, attackers can insert themselves into the communication channel between IoT devices and servers. For example, in a public Wi-Fi environment, an attacker can set up a malicious access point to intercept and modify data transmitted between a user and an IoT device—such as a remotely controlled camera. As a result, user commands may be maliciously altered, causing abnormal device operations, while private information in the communication content may also be stolen [3]. Another critical threat is the Distributed Denial of Service (DDoS)attack. A well-known example occurred in 2016 when the U.S. Dyn DNS service suffered a massive DDoS attack. Attackers controlled large numbers of IoT devices infected with the Mirai malware—such as network cameras and smart routers—to form a botnet and send overwhelming traffic to the target. The attack paralyzed Dyn's DNS service, making many dependent websites inaccessible and causing extensive economic losses [4].

Across the three-layer IoT architecture, attackers employ a wide variety of techniques. For instance, ransomware attacks can infiltrate smart home control apps, encrypting user data and device control permissions (such as for smart locks or cameras). Victims are then forced to pay ransom to regain access. Another growing problem is data leakage, which becomes more severe as the number of IoT devices increases. When application platforms lack adequate security protections, users' sensitive information is easily exposed. In some cases, videos secretly recorded by compromised cameras may be uploaded to cloud storage and subsequently stolen, leading to serious violations of personal privacy.

4. Mainstream security protection technologies

IoT security protection spans the entire process of data transmission, with mainstream technologies building a multi-dimensional security framework.

Encryption technology is the cornerstone of data protection.

Because IoT devices are often resource-constrained, lightweight encryption algorithms are ideal choices. Algorithms such as AES-128 and SM4 ensure strong encryption while significantly reducing computational and power consumption, making them suitable for terminal devices like sensors and cameras [5]. The TLS protocol is also widely used to encrypt communications between devices and servers. Through its handshake mechanism for key negotiation, TLS effectively ensures the confidentiality and integrity of transmitted data, providing strong protection against eavesdropping and tampering attacks [6].

Digital certificates, based on Public Key Infrastructure (PKI), serve as electronic credentials issued to devices or users. Their core function is to enable different entities to verify the authenticity of devices and users. To prevent counterfeit devices from accessing networks, systems can verify the validity of certificates during device (e.g., camera) registration and connection [7]. Additionally, to enhance user login security on IoT platforms, two-factor authentication (2FA) can be implemented —combining passwords with dynamic verification codes (such as SMS codes or hardware tokens)— to reduce risks caused by password leaks.

The combination of MQTT + TLS is commonly used in industrial IoT systems, as MQTT is lightweight and optimized for device-to-device communication, while TLS adds the necessary layer of security to compensate for MQTT's inherent limitations. Similarly, CoAP + DTLS is designed for resource-constrained devices; DTLS (Datagram Transport Layer Security) provides an encryption

DOI: 10.54254/2755-2721/2025.LD30447

and authentication layer for datagram-based protocols, ensuring the security of communications in domains like smart homes.

An Intrusion Detection System (IDS) enhances security by monitoring for abnormal high-traffic patterns in camera data transmissions (such as sudden spikes in bandwidth usage) to identify and alert potential attacks. Furthermore, AI-based monitoring technologies use machine learning to model normal device behavior—such as camera rotation angles or login locations—and detect deviations from these patterns. By distinguishing between normal and abnormal behavior in real time, AI-powered IDS solutions can identify unknown threats and provide intelligent, proactive protection for IoT systems.

5. Conclusion

This paper primarily explores the typical security threats faced by camera-based IoT devices within the three-layer IoT architecture—namely, the perception layer, network layer, and application layer—as well as the application of mainstream security protection technologies. IoT security is a systematic project encompassing all three layers, requiring protection strategies that integrate layered defense, technological synergy, and full life-cycle security management.

The study draws the following conclusions:

First, security protection for camera devices must adopt layer-specific and coordinated defense strategies, targeting threats unique to each layer—for example, device impersonation at the perception layer, man-in-the-middle (MITM) attacks at the network layer, and database intrusions at the application layer.

Second, a defense-in-depth system should be established by combining lightweight encryption algorithms (e.g., AES-128), secure communication protocols (e.g., TLS/DTLS), identity authentication technologies (e.g., digital certificates and two-factor authentication), and intelligent detection systems (e.g., AI-based intrusion detection).

Third, security must be embedded throughout the entire life cycle of devices—from design and development to deployment and maintenance—to reduce vulnerabilities at the source.

However, this research still has areas for improvement. On one hand, it lacks firsthand experimental data comparing different protection technologies in real-world or simulated environments, and thus does not provide a quantitative performance evaluation. On the other hand, it does not deeply analyze the cost-effectiveness of various security schemes, nor does it sufficiently explore the practical application and effectiveness of advanced privacy-preserving technologies such as federated learning and differential privacy in camera-based IoT devices.

Looking forward, IoT security is expected to evolve toward greater intelligence and precision. Edge security technologies will enable real-time protection at the source, significantly reducing cloud workloads, while AI-driven defense systems will identify unknown attack patterns through adaptive learning. Furthermore, privacy-preserving approaches that balance data utilization and protection—such as federated learning and differential privacy—will continue to be refined and applied in future IoT security frameworks.

References

[1] Sivan, N., Bitton, R., & Shabtai, A. (2019). Analysis of location data leakage in the Internet traffic of Android-based mobile devices. In 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019) (pp. 243-260).

[2] Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. Future Generation Computer Systems, 100, 144-164.

DOI: 10.54254/2755-2721/2025.LD30447

[3] Xiao Daoju, Guo Jie, & Chen Xiaosu. (2004). A Study on a Defense Strategy Against Man-in-the-Middle Attacks. Computer Engineering and Science, 26(9), 7.
[4] Greenstein, S. (2019). The aftermath of the dyn DDOS attack. Ieee Micro, 39(4), 66-68.
[5] Toshihiko, O.. (2017). Lightweight cryptography applicable to various iot devices. NEC TECHNICAL JOURNAL.
[6] Ferst, M. K., Figueiredo, H. F. M. D. , Denardin, G., & Lopes, J. (2018). Implementation of secure communication with modbus and transport layer security protocols. IEEE.
[7] Georgiev, M., Iyengar, S., Jana, S., Anubhai, R., & Shmatikov, V. (2012). The most dangerous code in the world: validating ssl certificates in non-browser software. ACM.