Proceedings of CONF-SEML 2026 Symposium: Computational Analysis and Modeling in Complex Intelligent Systems
DOI: 10.54254/2755-2721/2026.GU32334

A Review on the Application of Large Models in the Field of Internet of Things Security

Junrui Kang

The Middle School Attached to Sichuan Normal University (Shu Yuan Campus), Chengdu, China
xingyejiekui645@gmail.com

Abstract. With the rapid development of the Internet of Things technology, the security issues of the Internet of Things have become increasingly prominent. This paper systematically reviews the research progress in the field of Internet of Things security, focusing on the analysis of traditional security methods, deep learning-based security technologies and the application of large models in the Internet of Things security. By elaborating on the characteristics and limitations of different approaches, this paper summarizes the challenges faced by current technologies, including data privacy risks, the inherent vulnerability of Internet of Things devices to attacks and practical problems in model deployment. Finally, this paper discusses the future development trends, providing a reference for the research on large models in the field of Internet of Things security. In addition, this paper analyzes the security architectures and typical threat models of the Internet of Things, and reviews the deep learning-based intrusion and anomaly detection methods. It explores the application of large models in intelligent threat detection and security management while discussing the challenges, such as high computational cost, privacy risks and deployment constraints, and introduces federated learning and edge computing as potential solutions.

Keywords: Internet of Things, Large models, Deep learning, Intrusion Detection, Cybersecurity

1. Introduction

With the rapid development of the Internet of Things, security issues have gradually become a key focus of attention. Due to factors such as the enormous quantity and long update cycle of Internet of Things devices, these devices are frequently subject to attacks, making the security problems of the Internet of Things increasingly severe. The application of deep learning in Internet of Things security can be divided into four aspects: intrusion detection, abnormal behavior detection, malware detection and privacy protection. Taking the most common intrusion detection as an example, early intrusion detection relied on manually designed rules to detect attacks, which were prone to missing new types of attacks. In recent years, deep learning has enabled intrusion detection to analyze network traffic and automatically detect anomalies, such as identifying hacker attacks, abnormal access and DDoS attacks. The rise of large models has provided solid support for Internet of Things security with their advantages of massive information acquisition, accurate and efficient

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2026.GU32334

computation and high real-time performance. This paper systematically sorts out the key issues of Internet of Things security, summarizes the security threats of the Internet of Things, generalizes the research directions, including privacy protection, intrusion detection and anomaly detection, and analyzes the limitations of traditional methods. It reviews the research on the application of large models in the field of Internet of Things security, analyzes the existing research and current challenges, and looks forward to the future development directions.

2. Internet of things security architecture and threat models

2.1. Structural characteristics and challenges of internet of things networks

The network structure of the Internet of Things features distribution and dynamics, such as frequent online and offline activities of devices and variable network topologies [1], which make attack behaviors more concealed and render traditional rule-based detection methods unable to identify abnormal behaviors in a timely manner. For instance, the Mirai botnet launched large-scale DDoS attacks by controlling a large number of Internet of Things devices in 2016, exposing the serious deficiencies in the security protection of the Internet of Things. Meanwhile, zero-day attacks and Advanced Persistent Threats (APTs) often bypass traditional detection by exploiting unknown vulnerabilities due to their highly concealed long-term latent and highly precise new attack methods [1]. Traditional intrusion detection technologies often rely on rule matching or static feature extraction, which are inadequate in the face of heterogeneous data and struggle to accurately identify abnormal patterns [1]; thus, their effectiveness is limited when confronting large-scale attacks.

2.2. Internet of things security architecture and threats

The rapid growth in the number of Internet of Things devices has made the Internet of Things networks characterized by large scale, complex structure and strong heterogeneity. Unlike the traditional Internet, the Internet of Things consists of a large number of perception devices, communication networks and cloud platforms. Different devices vary greatly in computing power, communication protocols and security protection capabilities, making the Internet of Things systems more vulnerable to security threats. Due to limited device resources, many Internet of Things terminals lack sound identity authentication and encryption mechanisms, which further increases the security risks of the systems.

From the perspective of the Internet of Things security architecture, the security of the Internet of Things usually includes three levels: perception layer security, network layer security and application layer security. The perception layer mainly involves sensors and intelligent devices, which are vulnerable to attacks such as device cloning and malicious code injection; the network layer focuses on security issues during data transmission, such as Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks and data eavesdropping. The application layer is mainly plagued by problems such as data privacy leakage, unauthorized access and service abuse. Security issues at different levels are interrelated, and an attack on any single layer will cause severe impacts on the entire system.

In terms of threat models, the Internet of Things systems face a variety of attack forms, including Distributed Denial of Service (DDoS) attacks, malware propagation, device hijacking and Advanced Persistent Threats (APTs). Among them, attackers usually take advantage of the weak security protection capabilities of Internet of Things devices to form botnets by controlling a large number of such devices and launching large-scale attacks on target systems. In addition, due to the long-term

DOI: 10.54254/2755-2721/2026.GU32334

online status and wide distribution of Internet of Things devices, attack behaviors are characterized by strong concealment, fast transmission speed and a wide influence range, posing enormous challenges to security protection.

Traditional security protection methods for the Internet of Things mostly rely on rule matching or manually designed features for attack detection. Such methods have certain effects in the face of known attacks, but are unable to identify new types of attack behaviors. With the continuous changes in the network environment and the increasing complexity of attack methods, static feature-based detection methods are difficult to adapt to dynamic network environments, leading to a decline in detection accuracy. At the same time, traditional methods usually require a great deal of manual labor and have a low degree of automation, making it difficult to meet the real-time security requirements in large-scale Internet of Things environments.

Therefore, building an efficient Internet of Things security system needs to integrate AI detection technologies to improve the system's ability to identify unknown threats. Nowadays, deep learning and large model technologies have shown strong advantages in anomaly detection and intrusion identification through automatic feature extraction and complex pattern recognition, providing a new technical path for the security protection of the Internet of Things. The application of intelligent threat detection models can effectively improve the security protection capabilities of Internet of Things systems and lay a solid foundation for the subsequent research on the application of large models in Internet of Things security.

3. Internet of things security technologies based on deep learning

3.1. Intrusion detection technology based on deep learning

The large number and wide distribution of Internet of Things devices make traditional rule-based security detection methods unable to cope with complex network attacks. Intrusion detection technology can quickly discover abnormal behaviors by detecting network traffic and device behaviors, thus improving the security of the Internet of Things.

3.2. Deep learning-based recognition technology in internet of things security

Anomaly detection discovers potential attacks by identifying abnormal patterns of network behavior. Deep learning models can learn normal behavior patterns from complex data to detect abnormal behaviors. However, this method is highly dependent on training data and prone to false positives.

3.3. Application of deep learning in intrusion detection

Deep learning adopts Bidirectional Long Short-Term Memory (BI-LSTM), standard Transformer and Graph Attention Network (GAT) [2] to improve the accuracy of the intrusion detection process. Among them, the inference delay of the GAT model is controlled within 42 ms, which meets the requirements of most test scenarios [2].

3.4. Advantages and disadvantages of deep learning

Figure 1 shows the intrusion detection process of the Internet of Things, with the core being Data—Feature—Model—Classification Result. Among them, historical data processing, feature extraction, feature selection, feature library construction and classifier design are all completed by AI. It can be seen from the process that AI contributes three key steps to the Internet of Things intrusion

DOI: 10.54254/2755-2721/2026.GU32334

detection: automatic feature extraction, feature library establishment and attack classification. Compared with traditional manually designed features, AI avoids the limitations of manual feature design, thereby improving the detection accuracy and automation level. The figure also reveals four limitations of traditional AI models. Firstly, from the step of historical data processing, it can be seen that AI requires a large amount of training data, but the attack data of the Internet of Things is scarce, making it difficult to adapt to new types of attacks. Secondly, the feature engineering is complex and the generalization ability of the model is limited. Finally, traditional AI models lack universality and language understanding capabilities, so they can only perform single tasks, thus affecting the efficiency of intrusion detection. Therefore, building a multitask and lightweight model can improve the efficiency and accuracy of intrusion detection for the Internet of Things.

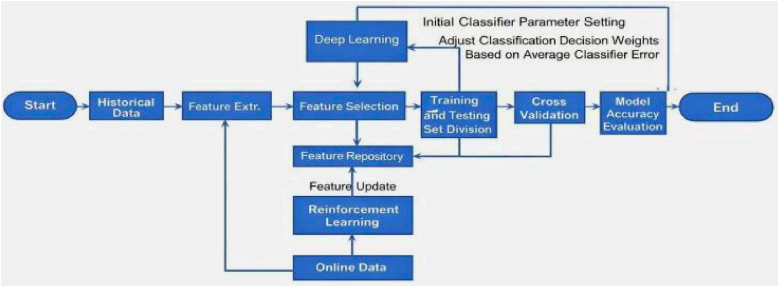

Figure 1. Feature extraction and feature library construction process for internet of things network intrusion detection

4. Core applications of large models in internet of things security

4.1. Applications of large models in daily life

Large models are widely used in various fields of daily life. Classified by task type, large models can be divided into general language large models, multi-modal large models and domain-specific large models. Classified by deployment form, large models can be divided into cloud-side large models, edge-side large models and end-side large models. Moreover, large models are extensively applied in the Internet of Things, such as firewall optimization and protection, data encryption, access control and a series of other fields. With the popularization of Internet of Things devices in daily life, the network attack surface has gradually expanded. For example, the commonly used communication protocols in the Internet of Things, such as Bluetooth, WiFi and ZigBee, are prone to security vulnerabilities and thus vulnerable to hacker attacks [3].

4.2. Applications and advantages of large models in the field of internet of things security

With their strong feature learning ability and generalization ability, large models show broad application prospects in the field of Internet of Things security. Compared with traditional machine learning models, large models are usually pre-trained based on massive data, which can automatically learn complex data features and reduce the dependence on manual feature engineering, thereby improving the accuracy and efficiency of security detection.

In the security protection of the Internet of Things, large models can be applied to intrusion detection, abnormal behavior identification, malicious code detection and security strategy optimization. Firstly, in terms of intrusion detection, large models can automatically extract attack behavior features by analyzing a large amount of network traffic data, realize the identification of unknown attacks, and improve the accuracy and real-time performance of detection. Secondly, in

DOI: 10.54254/2755-2721/2026.GU32334

terms of abnormal behavior detection, large models can identify abnormal activities that deviate from normal patterns by learning normal network behavior patterns, thus discovering potential security threats. In addition, large models can also be used for malware detection to improve the ability of malicious code identification by analyzing program behaviors and features.

In terms of security strategy formulation, large models can comprehensively analyze network threat intelligence, predict potential attack trends, and automatically generate protection strategies to realize intelligent security management. At the same time, large models can also be used for vulnerability detection and risk assessment, discovering system security hidden dangers by analyzing system operation data, and improving the overall security level of Internet of Things systems.

Compared with traditional deep learning methods, large models have stronger generalization ability and cross-scenario adaptability. Traditional models are usually trained for specific tasks and lack transferability, while large models can be applied to different Internet of Things scenarios through transfer learning and fine-tuning technologies, expanding the application scope of the models. At the same time, large models have a certain semantic understanding ability, which can process complex security logs and network data, improving the efficiency of security analysis.

However, the application of large models in Internet of Things security still faces certain challenges. Firstly, the training and deployment of large models require a lot of computing resources, while Internet of Things devices usually have limited computing power and are difficult to run complex models directly; secondly, the training of large models requires a large amount of data, which may bring the risk of data privacy leakage. In addition, large models have weak interpretability, and it is difficult to explain their judgment basis in the security decision-making process, which limits their application in actual systems. With the development of artificial intelligence technology, large models are widely used in daily life, such as intelligent cameras, safe door locks and mobile phone voiceprint recognition systems. However, despite their rich applications, personal information leakage caused by hacker attacks will pose a serious threat to users' privacy.

Therefore, in future research, it is necessary to combine edge computing, federated learning and model compression technologies to realize the lightweight deployment of large models and improve their application capabilities in resource-constrained environments. At the same time, strengthening the research on model security and interpretability will further promote the development and application of large models in the field of Internet of Things security.

5. Privacy protection and new technologies

5.1. Application of federated learning in internet of things privacy protection

With the rapid increase of Internet of Things devices, traditional deep learning training models still have the risk of data leakage in the field of intrusion detection. In the federated learning framework, Internet of Things devices complete collaborative training by regularly exchanging and aggregating the parameters and gradients of deep learning models on a central server instead of uploading their raw data [4]. Federated learning effectively protects data privacy by replacing the upload of raw data. Federated learning has been applied to Internet of Things network behavior detection and intrusion detection, which improves the detection accuracy and reduces the risk of data leakage. However, due to the large scale and huge number of Internet of Things devices, and the fact that federated learning methods require clients to frequently upload their local model parameters and

DOI: 10.54254/2755-2721/2026.GU32334

gradients, federated learning faces problems such as high overhead and slow model convergence speed.

5.2. Application of edge computing in internet of things security

Edge computing is a computing mode that migrates computing tasks, data storage and some application services from centralized cloud data centers to edge nodes of the network [5]. Edge computing reduces security risks during data transmission by processing data at network edge nodes. In the Internet of Things environment, edge computing can realize real-time anomaly detection and security protection, improving the system response speed. At the same time, edge computing reduces the computing pressure on the cloud side. However, edge devices have limited computing power and still face the problem of resource constraints.

5.3. Data access and security mechanisms

In addition to the above technologies, mechanisms such as data access control, security authentication and encrypted transmission are also important means of privacy protection for the Internet of Things. These technologies jointly build a multi-level security protection system, effectively improving the overall security of Internet of Things systems.

6. Challenges and development

At present, the security of the Internet of Things still faces various challenges in practical applications. Firstly, the large number and wide distribution of Internet of Things devices make it difficult to fully deploy device firmware updates and security patches, leaving the system exposed to known vulnerability risks for a long time [6]. At the same time, deep learning models have a large number of parameters and high requirements for computing resources, while most Internet of Things devices have limited computing power and are unable to support the operation of complex models, making the computing power problem an important factor restricting the application of related technologies. In addition, data sources in the Internet of Things environment are complex and unevenly distributed, and the cost of data annotation is high, which affects the model training effect and detection accuracy. Meanwhile, Internet of Things systems involve a large amount of user-sensitive information, and how to realize efficient data utilization on the premise of ensuring data privacy is still an important problem to be solved at present.

To address the above problems, future research needs to focus on lightweight model design and efficient deployment technologies to improve the operation capability of models in resource-constrained environments. At the same time, unsupervised learning or self-supervised learning methods can be used to reduce the dependence on manually annotated data and improve the performance and generalization ability of models. In addition, realizing the distributed deployment of models by combining edge computing and other technologies can improve the real-time performance and scalability of the system, and enhance the overall protection capability while ensuring data security. By optimizing the model structure and deployment mechanism, it is expected to promote the development of Internet of Things security systems towards a more efficient, reliable and intelligent direction.

DOI: 10.54254/2755-2721/2026.GU32334

7. Conclusion

This paper provides a systematic review of the applications of large models and artificial intelligence technologies in the field of Internet of Things security, focusing on the analysis of Internet of Things intrusion detection technologies, deep learning methods, and the application of self-supervised learning and federated learning in network behavior detection, as well as key technologies related to privacy protection and data security. Through the review of existing research results, it can be seen that deep learning-based intrusion detection methods are significantly superior to traditional methods in feature extraction capability and detection accuracy, and can effectively improve the security protection capability of Internet of Things systems. Meanwhile, new technologies such as federated learning, homomorphic encryption and edge computing provide new ideas for solving the problem of data privacy protection in the Internet of Things environment.

However, current research still has certain limitations. Firstly, the computational overhead of models is large, training data relies on manual annotation, and there is a trade-off between privacy protection and detection performance. Secondly, the issues of model deployment and real-time performance in large-scale Internet of Things environments still need further optimization. Future research can focus on lightweight model design, edge intelligent deployment and optimization of privacy protection mechanisms to improve the overall performance and practicality of Internet of Things security systems.

In summary, large models and artificial intelligence technologies have broad application prospects in the field of Internet of Things security, but continuous improvements are still needed in algorithm efficiency, data security and adaptation to practical application scenarios to promote the development of Internet of Things security technologies toward intelligence and high efficiency.

References

[1] Wang X., Xi X., Chen S. Q. (2026) Application of Intrusion Detection Technology in the Security Protection of the Internet of Things. China Broadband, 22(01). DOI: 10.20167/j.cnki.ISSN1673-7911.2026.01.28

[2] Wang C. X., Li F. C. (2026) Deep Learning-based Automatic Detection Technology for Computer Network Intrusion Behaviors. Information Recording Materials, 27(01). DOI: 10.16009/j.issn.1009-5624.2026.01.033

[3] Tang Y. (2025) Countermeasures for the Security Protection of Internet of Things Devices. Informatization Construction, (08): 62-63.

[4] Han H. L., Wang X. J. (2025) An Efficient Intrusion Detection Method for the Internet of Things Based on Semi-supervised Federated Learning. Journal of Beijing University of Posts and Telecommunications, 48(05). DOI: 10.13190/j.jbupt.2024-122

[5] Gong Y. (2025) Research on the Application of Edge Computing in the Internet of Things. Information Recording Materials, 26(12): 158-160. DOI: 10.16009/j.cnki.cn13-1295/tq.2025.12.047

[6] Shi Q. H. (2025) Cybersecurity Threats and Mitigation Measures for Industrial Internet of Things Systems. Yangtze River Information Communication, 38(07). DOI: 10.20153/j.issn.2096-9759.2025.07.048