Proceedings of the 5th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/133/2025.20597

Research on Industrial Internet Intrusion Detection Based on Deep Learning Algorithms

Chengbo Jia[1,a,*]

[1]*Hebei University of Technology, Lang Fang, 065000, China*
a. jia15876637782022@163.com
**corresponding author*

Abstract: With the rapid popularization of the Industrial Internet, the connection between industrial control systems and enterprise networks has become increasingly tight, making them primary targets for cyberattacks. This trend not only intensifies the security risks of industrial control systems but also presents new challenges for cybersecurity protection. Deep learning technology in artificial intelligence, with its capability to learn complex problems from unsupervised data, is a powerful tool for protecting the cybersecurity of industrial control systems. This paper explores the foundational theories of Industrial Internet security and intrusion detection, covering basic concepts, major characteristics, and various security threats and risks faced by the Industrial Internet. It further analyzes the limitations of traditional security technologies in the context of the Industrial Internet, including their inadequacies in responding to new threats, particularly their vulnerability to system vulnerabilities and virus attacks. Moreover, the paper introduces the specific applications of three deep learning algorithms—Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Generative Adversarial Networks (GANs)—in the security of the Industrial Internet. Through systematic analysis and research, the paper reveals specific cybersecurity issues present in the Industrial Internet and proposes effective methods to address these issues using deep learning algorithms. These findings not only provide new ideas and technical support for contemporary Industrial Internet security protection but also offer valuable insights and a theoretical foundation for future research directions.

Keywords: Deep Learning Algorithms, Convolutional Neural Network (CNN), Machine Learning, Industrial Internet Intrusion

1. Introduction

In the era of a thriving global digital economy, the Industrial Internet, as an emerging technological framework, is gradually reshaping the operational models of traditional manufacturing. By connecting physical devices to the internet, the Industrial Internet not only enhances production efficiency but also facilitates intelligent management and real-time monitoring. However, this advancement is accompanied by increasingly prominent cybersecurity challenges. Due to the complexity, high integration, and real-time nature of Industrial Internet systems, these systems face more severe security threats.

The cybersecurity landscape of today's Industrial Internet systems remains serious, with incidents of external intrusions on the rise. While firewalls and other devices are deployed in network systems,

DOI: 10.54254/2755-2721/133/2025.20597

the focus of Industrial Internet intrusion detection lies in the analysis of industrial network data traffic. With the application of artificial intelligence technologies in industrial systems, many experts and scholars have applied deep learning algorithms to Industrial Internet intrusion detection, achieving excellent results [1].

This paper will first explore the foundational theories of Industrial Internet cybersecurity, assess current security threats and risks, and evaluate the application and limitations of traditional machine learning algorithms in intrusion detection. Building upon this analysis, this paper will focus on the innovative applications of deep learning algorithms, particularly Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Generative Adversarial Networks (GAN) in Industrial Internet security.

2. Overview of Industrial Internet Cybersecurity and Intrusion Detection

Industrial Internet security refers to a series of technologies and measures aimed at safeguarding Industrial Internet systems from unauthorized access, data breaches, and malicious attacks [2].

2.1. Analysis of Industrial Internet Security Threats and Risks

Industrial Internet security faces various risks and potential threats to information systems. In recent years, the security challenges and complexity of the Industrial Internet industry have grown exponentially, especially for enterprises undergoing digital transformation, which face even greater risks [3]. For example, buffer overflow vulnerabilities can enable attackers to execute arbitrary code on target systems, while SQL injection can lead to the illegal acquisition of sensitive information in databases. To address these threats and risks, a comprehensive analysis and assessment are required to develop appropriate security strategies and measures.

2.2. Industrial Internet Intrusion Detection Technologies

Industrial Internet intrusion detection technologies are essential for ensuring the security and stability of network communications. These technologies can promptly identify and respond to potential threats and attack events. The main techniques include:

Network security protection technologies: These involve the deployment of network boundary firewalls, intrusion detection systems (IDS), and other security devices that monitor network communications, detect malicious traffic, and block attacks in real time.

Network traffic analysis and behavior recognition technologies: These techniques use network traffic analysis and behavior recognition techniques to identify abnormal traffic and malicious activities within the network, enhancing the ability to detect potential threats.

Security event response and handling technologies: These techniques establish a comprehensive security event response mechanism to promptly identify and handle security incidents, reducing the impact of security events on the system.

3. Problems with Traditional Applications in Industrial Internet Security

3.1. Need for Integration with New Technologies

Traditional network security focuses on network structure, emphasizing the security of network boundaries and the devices themselves. Industrial Internet security, however, involves more than just these two protective aspects. With the rise of new cyber attack methods such as ransomware, the wave of informatization, intelligence, and digitization in the new era will inevitably reshape the architecture of Industrial Internet security. Industrial data, in particular will become the core element of change [4].

DOI: 10.54254/2755-2721/133/2025.20597

The Industrial Internet encompasses a vast amount of security-related data from multiple perspectives and angles, including industrial production, security logs, industrial control protocols, network traffic, and enterprise information. Transforming the existing security architecture, while integrating new technologies, is a key fouces in the current environment.

3.2. System Vulnerabilities

From a technical perspective, the Industrial Internet is the integration of Operational Technology (OT) and Information Technology (IT). As the scale of industrial production expands, network systems arebecoming increasingly complex, making security control more challenging [5]and creating opportunities for system vulnerabilities. For example, in the case of the Supervisory Control and Data Acquisition (SCADA) systems connected by the Industrial Internet, inherent software vulnerabilities increase security risks. Additionally, if operating systems such as Windows or Linux fail to timely update their vulnerability patches, issues like information leakage and data theft may arise [6]. The openness of the Industrial Internet further exacerbates this issue, as it allows unrestricted access to data from any industrial production process, thereby increasing the burden on security protection measures.

3.3. Virus Attacks

During the operation of the Industrial Internet, hackers or malicious actors can exploit network vulnerabilities to launch attacks using Trojan viruses, leading to information leaks and production disruptions. For example, viruses can damage and infect computer devices, replicating themselves across the system and automatically spreading from one device to another within the same network without human intervention [7]. Ransomware can encrypt victim files, lock computer access, and demand ransom payments from businesses to regain access. Fileless malware does not require attacking hard disk code; instead, it uses parasitic attack techniques and leverages secure, legitimate tools to infect victim systems. Since fileless malware lacks executable files, fileless malware can evade file-based detection tools, allowing it to persist with malicious code.

4. Application of Deep Learning Algorithms in Industrial Internet Security

As network threats become increasingly complex, deep learning algorithms demonstrate significant potential and application value. As an advanced artificial intelligence technology, deep learning constructs multi-layer neural networks to achieve automatic feature extraction and complex pattern recognition, thereby enhancing the detection and response capabilities for security incidents. This part focues on three primary deep learning algorithms—Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Generative Adversarial Networks (GAN)—which offer innovative solutions in Industrial Internet cybersecurity. These algorithms not only effectively address the security challenges mentioned earlier but also provide new approaches to improving intrusion detection systems and advancing the overall security protection level of the Industrial Internet.

4.1. Convolutional Neural Networks (CNN)

A Convolutional Neural Network (CNN) consists of multiple neurons that are locally connected rather than fully connected, enabling the transmission of data features. CNNs use convolution operations to extract local features from input data [8]. A typical CNN is composed of convolutional layers, pooling layers, and fully connected layers [9]. Specifically, a CNN is structured with an input layer, convolutional layers, pooling layers, fully connected layers, and an output layer. The input

DOI: 10.54254/2755-2721/133/2025.20597

layer converts images into corresponding two-dimensional matrices of pixel values. Experimental results show that the algorithm proposed in this paper outperforms Support Vector Machines (SVM), and K-means algorithms in terms of intrusion detection accuracy. In terms of false positive rate, the CNN algorithm performs better than the other two algorithms. Experiments have demonstrated that applying the CNN algorithm to industrial control systems can enhance the intrusion detection rate in network traffic features and reduce the false positive rate [10].

4.2. Recurrent Neural Networks (RNN)

Early neural networks were primarily feedforward neural networks, where information flows forward through the network, making them easy to train. However, this architechture limits the network to considering only the current input without remembering previous data, treating inputs and outputs independently, thus making it difficult to handle time series data. To enable the network to have a "memory function," researchers introduced Recurrent Neural Networks (RNN), which have internal units that can retain state, mallowing them to consider previous inputs, making them more suitable for sequential data. Currently, RNNs are widely used in sequence prediction, natural language processing, and other fields.

Recent advancements have led to the development of bidirectional simple recurrent network techniques that can extract temporal features between pieces of information and improve the utilization of historical information. These techniques leverage the strong parallel processing capabilities of simple recurrent units, thus reducing model training time. Additionally, attention mechanisms are introduced to dynamically adjust the weight coefficients of the hidden states in bidirectional simple recurrent networks, highlighting strongly correlated factors and achieving security situational value prediction [11].

4.3. Generative Adversarial Networks (GAN)

Generative Adversarial Networks (GANs) consist of two modules: the Generator network (G) and the Discriminator network (D). These two modules have a competitive relationship and iteratively compete against each other during training, leading to mutual improvement of both the generation and discrimination capabilities.

The training objective of the generator is to produce samples that closely match the distribution of real-world samples, making them indistinguishable to the discriminator. Meanwhile, the discriminator’s objective is to differentiate between real and fake samples. When the adversarial training reaches its goal, the generator produces samples that nearly perfectly match the real samples, and the discriminator's accuracy stabilizes at 50%, meaning it cannot distinguish between the generated fake samples and the real samples. GAN can effectively learn the distribution characteristics of real network traffic, enabling the detection and identification of traffic anomalies, thus effectively addressing various network intrusion attacks [12].

5. Conclusion

With the rapid development of the Industrial Internet, traditional cybersecurity measures are increasingly inadequate in addressing emerging challenges. This paper systematically analyzes and studies these challenges, revealing that their essence lies in system complexity, the insufficiency of traditional security technologies, system vulnerabilities and misconfigurations, the threat of virus attacks and malware, and the need for new technologies. The paper proposes deep learning algorithms as a novel approach to effectively address cybersecurity issues in the Industrial Internet. The application of Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Generative Adversarial Networks (GAN) not only demonstrates the potential of deep learning in

DOI: 10.54254/2755-2721/133/2025.20597

network intrusion detection but also provides a solid theoretical foundation and practical guidance for future technological development. Further research and practice are expected to continuously optimize and integrate these advanced technologies, ultimately contributing to the development of a more robust and intelligent Industrial Internet security protection system. This will not only enhance the overall level of cybersecurity but also provide a strong guarantee for the digital transformation and intelligent development of the industrial sector.

References

[1] *Zhi, Z. L. (2024). Research on the Application of Deep Learning Algorithms in Industrial Internet Intrusion Detection. Modern Industrial Economy and Informatization (07), 77-79. doi:10.16525/j.cnki.14-1362/n.2024.07.026.*

[2] *Ji, K. Y. (2024). Research on Industrial Internet Security Technology. Cybersecurity and Informatization (1).*

[3] *Cao, Y., Zhang, X. F., Zhang, Z. Y., & Ren, X. R. (2024). Analysis and Prevention of Data Security Risks in Industrial Internet. Confidentiality Work (08), 60-62. doi:10.19407/j.cnki.cn11-2785/d.2024.08.016.*

[4] *Dong, Y. C., Zhang, Q., Li, B. Q., Li, Y., & Dong, Y. (2024). Research on Industrial Internet Security Technology and Applications Based on Generative AI. Information and Communication Technology and Policy (08), 32-37.*

[5] *Zhang, Y. F. (2024). Research on Security Challenges and Protection Mechanisms in Industrial Internet. Digital Communication World (08), 189-191.*

[6] *Zhang, Y. C., Ke, H. R., Li, Y., & Cai, L. L. (2024). Research on Cybersecurity Protection System for Industrial Internet Supply Chain. Communication World (08), 6-8. doi:10.13571/j.cnki.cww.2024.08.009.*

[7] *Yang, W. Y., Wu, S. C., Liu, H. T., Wang, S. Y., & Wang, W. (2024). Application of the "Industrial Internet + Safety Production" Platform in Group-Level Enterprises. China Informatization (04), 59-61.*

[8] *Zhang, W. A., Hong, Z., Zhu, J. W., & Chen, B. (2019). Review of Network Intrusion Detection Methods in Industrial Control Systems. Control and Decision (11), 2277-2288. doi:10.13195/j.kzyjc.2019.1302.*

[9] *Jiao, P. P., Yang, R., Zheng, Q. Y., Wang, L., Chen, Z. Y., & Liu, X. H. (2023). Application of Deep Learning Technology in Renal Cancer Diagnosis. Wuhan University Journal of Natural Sciences (Medical Edition), 1-6. doi:10.14188/j.1671-8852.2023.0287.*

[10] *Zhao, Y. W. (2023). Research on the Application of Machine Learning Algorithms in Industrial Scenarios (Master's Thesis, University of Electronic Science and Technology of China). Master's thesis. https://link.cnki.net/doi/10.27005/d.cnki.gdzku.2023.002064 doi:10.27005/d.cnki.gdzku.2023.002064.*

[11] *Tian, Z. G. (2022). Research on Industrial Internet Security Situation Awareness Based on Recurrent Neural Networks (Master's Thesis, Chongqing University of Posts and Telecommunications). Master's thesis. https://link.cnki.net/doi/10.27675/d.cnki.gcydx.2022.001176 doi:10.27675/d.cnki.gcydx.2022.001176.*

[12] *Online Resource: Baidu Wenku, 2024-1-21, Application of Generative Adversarial Networks in Cybersecurity, https://wenku.baidu.com/view/32fe6e45b7daa58da0116c175f0e7cd185251816.html?_wkts_=1730606161403&bdQuery=*