Research on Cybersecurity Technologies for Smart Aluminium Smelters Based on AI Models

Yan Li[1], Zhuan Song[2], Shuo Zhang[3] and Fangshu Wei[4]
1. Third-level Researcher
2. Manager Assistant
3. Fourth-level Researcher
4. Engineer
Zhengzhou Non-ferrous Metals Research Institute of Chalco (ZRI), Zhengzhou, China
Corresponding author: Yan Li, 13526591608@qq.com

https://doi.org/10.71659/icsoba2025-al091

Abstract

As smart aluminium smelters increasingly integrate industrial internet and automation technologies, Network Security Situation Awareness (NSSA) in complex network environments has become critical to ensure production continuity and data security. This paper addresses the challenges of frequent multi-source heterogeneous data exchange and the limitations of traditional defence mechanisms in aluminium smelting. It explores the application of AI models in enhancing NSSA. A Long Short-Term Memory (LSTM) network-based model is developed to analyse the time-series behaviour of equipment, enabling real-time monitoring of anomalies in cell control commands and sensor data. Additionally, the Graph Neural Network (GNN) is used to construct a device interaction graph, facilitating the automated detection of vulnerabilities in communication protocols. Experimental results show that the proposed system achieves over 95 % accuracy on test datasets, with an average response latency below 150 ms and a false alarm rate under 6.5 %. This provides an innovative and practical approach to building proactive, intelligent cybersecurity systems for the aluminium industry.

Keywords: Smart aluminium smelters, Aluminium smelting, Industrial internet security, Deep learning, Adaptive defence.

1. Introduction

1.1 Research Background and Significance

Smart aluminium smelters, as a vital component of modern manufacturing, represent the cutting edge of intelligent production in the era of Industry 4.0. By integrating advanced automation, information technologies, and artificial intelligence, these facilities have achieved highly automated, intelligent, and flexible production processes. They have not only improved production efficiency and reduce energy consumption but also significantly enhanced product quality and overall competitiveness. As a bridge between the physical and digital worlds, smart aluminium smelters serve as exemplary models for intelligent manufacturing and smart factory development.

In recent years, the rapid advancement of smart factories has been accompanied by escalating cybersecurity threats. Frequent incidents involving hacking, malware, and insider breaches have posed serious risks to production safety, data integrity, and operational continuity. For smart aluminium smelters, classified as critical infrastructure, the impact of a successful cyberattack can be severe, potentially resulting in production halts, equipment damage, and data leaks. Such events not only harm corporate interests but may also threaten national security and social stability ［1］.

Currently, smart factories face several critical cybersecurity challenges. First, attack methods have become increasingly diversified, ranging from traditional viruses and trojans to advanced persistent threats (APTs), as attackers continuously exploit emerging technologies and new vulnerabilities [2]. Second, defence systems are growing more complex. The interconnected systems, devices, and networks within a smart factory form a highly intricate ecosystem, where any weak link may serve as an entry point for attacks [3]. Third, incident response is exceptionally demanding. Given the high reliance on automated control systems in production, any cyberattack requires immediate fault localization and rapid recovery, placing significant pressure on an organization's emergency response capabilities [4].

NSSA refers to the process of collecting and analysing various data within the network environment to obtain real-time, accurate insights into the system's security status and its evolving trends. It provides scientific support for timely and informed decision-making [5]. In smart factories, NSSA plays a particularly vital role. It enables enterprises to detect and respond to threats in a timely manner, helping prevent potential cyber incidents. Additionally, by mining and analysing historical data, it can uncover latent security risks and vulnerabilities, offering forward-looking guidance for security planning.

Specifically, NSSA's applications in smart factories include: 1) Real-time monitoring of network traffic and log data to detect abnormal behaviour; 2) Leveraging big data analytics and machine learning to predict and issue early warnings of potential threats; 3) Integrating various security resources to build a coordinated defence system that enhances overall protection capabilities. Therefore, strengthening the research and application of NSSA technologies is of great significance for enhancing the overall cybersecurity of smart factories.

1.2 Research Purpose and Objectives

This study aims to enhance the cybersecurity protection capabilities of smart aluminium smelters by developing an AI-driven NSSA model. AI technologies, with their powerful capabilities in data processing and analysis, have demonstrated significant potential in the field of cybersecurity. By introducing AI models, it becomes possible to process massive volumes of network data rapidly and perform in-depth analysis, enabling more accurate understanding of network security status and evolving threat trends.

This study focuses on applying AI models to NSSA in smart aluminium smelters, covering key stages such as data collection, preprocessing, feature extraction, and model training. By optimizing model architecture and parameters, the goal is to improve detection efficiency and accuracy, providing strong technical support for enterprise-level cybersecurity defence.

The specific objectives of this study include: 1) Improving threat detection efficiency – by leveraging AI models, the system can rapidly identify and respond to abnormal behaviours within the network, minimizing the time from threat detection to incident response; 2) Reducing false alarms – by refining model algorithms and parameter settings, the accuracy and robustness of detection are enhanced, reducing both false alarms and missed detections; 3) Enhancing the effectiveness of defence strategies – based on AI model outputs, targeted defence measures can be developed, such as dynamically adjusting firewall rules or deploying intrusion detection systems, thereby improving overall security capabilities.

In addition, this study will explore the application of AI models in NSSA forecasting by analysing and mining historical data, aiming to predict future threat patterns and trends and provide proactive security guidance for enterprises who want to detect and respond to potential cybersecurity threats as early as possible, thereby reducing security risks.

These efforts offer valuable references and insights for AI technology applications in cybersecurity.

Finally, this study proposed AI model-based cybersecurity defence strategies and recommendations. Based on the model outputs, we formulated a series of specific defence measures, such as dynamic adjustment of firewall rules and deployment of intrusion detection systems. These strategies and recommendations provide comprehensive guidance and support for cybersecurity protection in smart factories.

In summary, this study achieved significant results in enhancing the NSSA capability of smart aluminium smelters, providing strong technical support and assurance for smart factory cybersecurity protection. These results not only hold important theoretical and practical significance but also offer useful references and guidance for future related research.

7. References

1. Wei Wang, Hua Li. Research on network security risk assessment methods for smart factories [J], *China Safety Science and Technology*, 2020, 16(5), 45–50 (in Chinese).
2. Qiang Zhang, Yang Liu. A review of network intrusion detection techniques based on deep learning [J], *Electronics Technology and Software Engineering*, 2021(3): 12–17 (in Chinese).
3. Ming Li, Gang Chen. A review of network security for industrial control systems [J], Computer Science, 2022, 49(2): 1–10 (in Chinese).
4. Liang Zhao, Hua Zhang. Analysis of technology development trends in smart aluminium smelters [J], *Light Metals*, 2021(4): 55–60 (in Chinese).
5. Fang Wang, Gang Li. Research on network security situation awareness based on Artificial Intelligence [J], *Network Security Technology and Applications*, 2023(1): 25–29 (in Chinese).