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.

1.3 Research Scope and Methodology

This study focuses on several key technologies, including AI model development, data collection and processing, and threat detection and response. In terms of AI model development, advanced techniques such as deep learning and machine learning will be employed to build models tailored for NSSA in smart aluminium smelters. The model architecture and parameters will be optimized to enhance detection efficiency and accuracy.

For data collection and processing, this study will concentrate on acquiring and handling critical information such as log data and network traffic. By designing effective data acquisition schemes and processing workflows, the integrity, accuracy, and timeliness of the data will be ensured. Data preprocessing techniques such as data cleansing and feature extraction will also be applied to reduce dimensionality and improve model performance.

In threat detection and response, the system will utilize model outputs to enable rapid identification and handling of cybersecurity threats. By setting appropriate thresholds and alert mechanisms, threat information can be communicated to relevant personnel in a timely and accurate manner. Furthermore, customized defence strategies and emergency response plans will vary based on the specific operational context and needs of different enterprises, thereby enhancing overall security resilience.

2. Theoretical Foundation and Literature Review

2.1 Concept and Framework of NSSA

Network Security Situation Awareness (NSSA) refers to the real-time, dynamic collection, analysis, and presentation of a network's security status, threat landscape, and evolving trends through various sources such as sensors and log systems. It provides decision support and actionable insights for cybersecurity administrators and aims to enable a comprehensive, in-depth, and dynamic understanding and management of network security.

NSSA consists of several key components: data collection, data processing, situation analysis, situation presentation, and response decision-making. The data collection phase gathers various security-related information from the network environment, including log data, network traffic, and user behaviour. The data processing phase performs preprocessing tasks such as data cleansing, organization, and feature extraction, laying the groundwork for subsequent analysis. The situation analysis phase is the core of NSSA. It involves deep analysis and mining of the processed data to uncover potential threats and shifts in the security posture. The situation presentation phase delivers analysis results in an intuitive and comprehensible manner to security administrators – typically using visualization techniques to show the network's security status, threat distribution, and trend predictions. Finally, the response decision-making phase develops targeted defence strategies and emergency response plans based on the presented analysis results to address potential cybersecurity threats.

Currently, mainstream NSSA frameworks include those based on multi-source information fusion, big data analytics, and machine learning. Multi-source information fusion frameworks integrate data from various sensors and log systems to provide a comprehensive view of network security. The advantage of this approach lies in its ability to leverage the complementarity of diverse security data sources, thus improving the accuracy and completeness of NSSA. However, it also presents significant challenges, such as data alignment, deduplication, and correlation during the fusion process, and places high demands on system real-time performance and stability.

Big data analytics-based frameworks conduct in-depth analysis and mining of massive volumes of log and traffic data to detect potential threats and evolving situations. Their strength lies in handling large-scale datasets and uncovering threats that are often missed by traditional methods. The drawbacks, however, include high requirements for data storage and processing capabilities, as well as the need for specialized personnel and technical support.

Machine learning-based frameworks train models to enable intelligent perception and prediction of cybersecurity conditions. These frameworks excel in autonomously learning network security patterns and features, thereby enhancing the accuracy and intelligence of NSSA. However, the limitations of this approach lie in the fact that model training and optimization require large amounts of data and computing resources, along with high demands for model generalization and robustness.

In summary, each type of NSSA framework has its own advantages and limitations. The choice of framework should be guided by specific application scenarios and requirements. At the same time, with the continuous advancement of technology, future NSSA frameworks are expected to become more intelligent, adaptive, and scalable.

2.2 Current Applications of AI in Cybersecurity

In recent years, with the rapid development and widespread use of artificial intelligence technologies, their applications in the field of cybersecurity have expanded significantly. AI, with its powerful capabilities in data processing and analysis, has introduced new approaches and solutions for enhancing cybersecurity. Key application areas of AI in cybersecurity include:

Malware detection: AI technologies can analyse and identify malicious software based on behavioural characteristics, code structures, and other indicators, enabling rapid detection and defence. Deep learning-based malware detection models, in particular, have shown strong performance in identifying previously unknown malware, greatly improving detection accuracy and efficiency.

Intrusion detection: AI can analyse network traffic and user behaviour in depth to uncover potential intrusion attempts. For example, machine learning-based intrusion detection systems can monitor traffic in real time and identify anomalies, allowing for timely detection and response to network intrusions.

Security situation prediction: AI can analyse historical security data to identify trends and patterns in evolving threat landscapes. For example, some time series-based prediction models can forecast and alarm cybersecurity conditions in the near future, offering valuable support for decision-making and incident response.

In the context of smart factories, the application of AI technologies presents unique challenges and considerations. On one hand, the highly automated and intelligent nature of production processes places high demands on the real-time performance, accuracy, and reliability of AI systems. On the other hand, the diversity and complexity of equipment and systems require AI solutions to be capable of cross-domain integration and collaborative operation.

The specific characteristics of AI application in smart factories include:

1) Large volumes and diverse types of data—Equipment and systems generate vast amounts of log and sensor data, often in various formats and with complex structures. This imposes high requirements on the data processing and analytical capabilities of AI models.

2) Complex and evolving threat landscape—The production processes in smart factories span multiple systems and stages, each of which may be targeted by increasingly sophisticated cyberattacks. This demands stronger threat detection and defence capabilities from AI systems.
3) Diverse security requirements—Different systems and devices have varying security needs, requiring AI-based solutions to deliver personalized and context-aware protection strategies.

Therefore, the application of AI in smart factories must take into account these specific challenges and adopt tailored strategies to address them effectively.

2.3 Cybersecurity Features and Requirements of Smart Aluminium Smelters

As a key component of modern manufacturing, smart aluminium smelters feature highly automated and intelligent production processes, making cybersecurity an increasingly urgent concern. However, due to the complexity of the production environment, the wide variety of equipment, and the large volume and diversity of data, smart aluminium smelters face a range of specific security risks. These risks include:
1) Equipment Failure Risks—The aluminium smelting process involves a large number of electrical and mechanical systems. Equipment failures can result in production interruptions, asset damage, and safety hazards. Given the diversity and complexity of the equipment involved, a better scheme of fault detection and diagnosis is expected to cope with different failure patterns and causes.
2) Data Leakage Risks—Smart smelters generate vast amounts of production and equipment data in the production processes. If the data are leaked or tampered with, it can lead to production disruptions, compromised product quality, and other consequences. In many cases, such data contain trade secrets or intellectual property, posing potential threats to both business interests and corporate reputation.
3) Cyber Attack Risks—Production in smart aluminium smelters heavily relies on network and communication technologies. A successful cyberattack or malware infection could cause system paralysis and data loss. In particular, attacks targeting industrial control systems pose even greater risks and destructive potential.

In summary, given the cybersecurity characteristics and requirements of smart aluminium smelters, it is essential to implement comprehensive security measures and strategic responses to ensure the safe and stable operation of the production process.

2.4 Summary of Literature Review

A review and analysis of existing researches reveal that NSSA technologies have already achieved certain lab results and practical experience in the context of smart aluminium smelters. Current studies mainly focus on the concept and frameworks of NSSA, the application status of AI technologies in cybersecurity, and the specific network security characteristics and requirements of smart aluminium smelters. However, some limitations still exist in the current research. This study proposes the following innovations and necessities:

First, the construction of an AI-based NSSA model. This study will utilize AI technologies such as deep learning and machine learning to build an NSSA model tailored for smart aluminium smelters. The model can rapidly process and deeply analyse massive data in network environments, thereby improving the accuracy and efficiency of NSSA. Meanwhile, the model can also be customized and optimized according to actual needs to adapt to various scenarios and applications.

Second, the proposal of comprehensive network security strategies and recommendations. This study will put forward integrated network security strategies and recommendations based on the network security characteristics and requirements of smart aluminium smelters. These strategies and recommendations will cover aspects such as equipment protection, data security management, and network security defence.

3. Design of AI-Based NSSA Model

3.1 Overall Framework Design

This study proposes an AI-driven NSSA architecture tailored for smart aluminium smelters. The architecture follows a closed-loop system based on "data acquisition - feature engineering - model detection - response and decision-making". The design draws upon the NSSA framework proposed by the Alliance of Industrial Internet (AII) of China and is further optimized to address the specific characteristics of industrial control systems in aluminium smelting. The architecture consists of four core modules:

1) The data acquisition module extracts multi-source heterogeneous data from the industrial network, including industrial protocol traffic (Modbus/OPC UA), equipment logs, and sensor data.
2) The feature engineering module performs preprocessing and feature extraction on raw data, with specially designed features for the time series characteristics of industrial protocols.
3) The model detection module employs hybrid AI models for anomaly detection and threat identification.
4) The response and decision-making module triggers corresponding security strategies based on the detected results. The innovation of this architecture lies in the integration of deep learning models with the real-time requirements of traditional industrial control systems, achieving low-latency response through edge computing deployment.

3.2 Data Acquisition Module

In building an AI-based NSSA model, data acquisition is a crucial step. The main data sources include:

1) Log data such as system logs, application logs, and security logs. These logs record various events and activities in the network environment and serve as an important basis for analysing the network security situation.
2) Network traffic data, by capturing and analysing network packets, it is possible to understand the communication patterns and data transmission modes within the network, thereby identifying potential abnormal behaviours.
3) Other relevant data such as user behaviour data and system configuration data, which provide a more comprehensive perspective for NSSA.

Data acquisition methods are primarily divided into real-time acquisition and periodic acquisition. Real-time acquisition refers to the continuous capture and analysis of network data using network monitoring tools or log collection systems. This method enables the timely detection of and response to cybersecurity threats. Periodic acquisition refers to collecting and analysing data at fixed time intervals, making it suitable for long-term monitoring and analysis of the network security situation.

3.3 Feature Engineering Module

Feature engineering is a critical step before building AI models. Its main purpose is to clean, transform, and extract features from raw data to improve data quality and model performance. Data cleaning involves removing duplicate data, handling missing values, and correcting

erroneous data to ensure data accuracy and completeness. Data transformation includes standardizing, normalizing, or discretizing data, converting it into a format suitable for model processing. Feature extraction aims to derive useful features for NSSA from the raw data, such as statistical features, time-domain features, and frequency-domain features.

3.4 Model Detection Module

The model detection module employs a hybrid AI approach for anomaly detection and threat identification, taking into account the characteristics of the data, the performance requirements of the model, and the needs of the application scenario. When processing log data and network traffic data, which typically exhibit both time-series and high-dimensional characteristics, deep learning algorithms can be used. Long Short-Term Memory (LSTM) networks are applied to establish device-specific traffic baseline, enabling real-time monitoring of anomalies in sensor data transmission frequency and in the timing of control command sequences.

Automated vulnerability scanning tools, leveraging predefined rules and vulnerability signature databases, integrate Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Interactive Application Security Testing (IAST) to conduct systematic vulnerability detection on target systems. These tools offer efficient scanning, multi-scenario coverage, and vulnerability prioritization capabilities. In addition, Graph Neural Networks (GNNs) are used to construct device interaction graphs, analysing the communication logic among devices such as pot control machines and PLCs. This enables the automatic discovery of potential communication protocol vulnerabilities and the provision of secure firmware update patches.

3.5 Response and Decision-Making Module

The response and decision-making module primarily applies machine learning methods to identify potential cybersecurity threats from raw data. By learning the distribution characteristics of normal data, it detects anomalies that deviate significantly from normal patterns. It possesses visualized, in-depth security analysis capabilities, enabling queries and correlation of the platform's foundational data, including events, alerts, assets, vulnerabilities, and users. Through a visual workflow orchestration interface, analysts can create deep analysis playbooks that execute multi-event, multi-source, and multi-stage deep analysis rules, thereby enhancing security analytics and threat detection capabilities.

For attack path prediction and response, Bayesian networks are used to construct attack propagation models. Combined with historical security incident data, these models predict weak points that attackers may exploit. Security orchestration then integrates and coordinates various security products and management systems within a single workflow. By incorporating threat intelligence, the system identifies genuine threat events and automatically executes containment tasks to enable rapid security response. Security orchestration can also create rules-based playbooks for predefined security scenarios. Once activated, these playbooks run in real time, automatically correlating and analysing relevant events, intelligence, assets, and user data according to the defined orchestration rules, triggering alerts and executing corresponding response actions.

4. Experimental Design and Result Analysis

4.1 Experimental Environment and Dataset Description

The experiment was conducted on a high-performance computing cluster equipped with multiple high-performance computing nodes. Each node is configured with dual Intel Xeon CPUs, 256 GB

of DDR4 memory, and multiple GPUs. In addition, the Hadoop Distributed File System (HDFS) was used for data storage and management, and Apache Spark was used for large-scale data processing and analysis. For the software environment, the experiment used the Python programming language and its related libraries for model construction and training, as well as tools such as Wireshark and tcpdump for network traffic data capture and analysis.

The dataset was sourced from the actual production environment of a certain smart aluminium smelter. The log data mainly came from the smelter's production management system, equipment monitoring system, and security auditing system, while network traffic data was captured by traffic monitoring devices deployed at the network perimeter. To ensure diversity and representativeness, the experiment selected data from different time periods and production scenarios as the training and testing sets.

4.2 Experimental Design and Implementation

This experiment aims to verify the effectiveness and performance of the AI-based NSSA model in smart aluminium smelters. The experimental plan is as follows: first, preprocess and extract features from the collected raw data; second, construct and train the AI model; third, evaluate the model using the test set; finally, optimize and adjust the model based on the evaluation results. During the experiment, particular attention was paid to indicators such as detection efficiency, false alarm rate, and the effectiveness of defence strategies.

Data Preprocessing and Feature Extraction: First, the collected raw data was cleaned and deduplicated to remove invalid and redundant entries. The log data was parsed and formatted to extract key information such as event type, timestamp, and source IP address as features. For network traffic data, traffic analysis tools were used for parsing and statistical processing to extract features such as traffic volume, transmission speed, and protocol type. Finally, the extracted features were normalized and standardized to facilitate subsequent model training.

Model Construction and Training: Following the experimental design, we selected the Long Short-Term Memory (LSTM) network from deep learning algorithms for modelling. A multi-layer LSTM structure was built, with Dropout layers added after each layer to prevent overfitting. The Adam optimizer and cross-entropy loss function were used for model training, with mini-batch gradient descent for parameter updates. An early stopping mechanism was applied to monitor performance changes and prevent overfitting.

Model Evaluation and Testing: Considering the specific requirements of industrial control systems, this study designed a multi-dimensional evaluation index system. For detection performance, traditional metrics were used: Detection Rate (DR), False Alarm Rate (FAR), and Average Detection Latency (ADL). DR is defined as the ratio of correctly detected attack samples to the total number of attack samples. FAR is defined as the ratio of false alarm occurrences to the total monitoring time. ADL measures the time interval between the occurrence of an attack and its detection by the system. Given the real-time requirements of the aluminium electrolysis process, detection latency was categorized into three levels: ≤ 100 ms (real-time response), 100–500 ms (near real-time response), and > 500 ms (delayed response), to evaluate the system's impact on production processes.

Model Optimization and Adjustment: Based on the evaluation and comparative analysis results, the model was optimized and adjusted. Optimization focused on algorithm improvement, feature engineering, and model integration. Algorithm improvement: experimenting with different network architectures and hyperparameter settings to find optimal configurations. Feature engineering: extracting additional useful features and improving the selection and transformation

of existing ones. Model integration: employing methods such as Bagging and Boosting to combine outputs from multiple models and improve overall performance.

4.3 Results Analysis

Following the experimental design and implementation, the AI-based NSSA model detected a total of 93 762 553 alarm logs in the test set from the smart aluminium smelter. The test results are given in Table 1:

Table 1. Test results of the aluminium smelter test set.

Attack Type	Detection Rate (%)	Average Latency (ms)	FAR (%)
Modbus Command Input	97.2	92	4.8
SCADA Data Tampering	99.1	78	3.5
Edge Node Penetration	96.5	115	6.2
Cross-Protocol Coordinated Attack	93.8	142	5.7

For quantitative analysis, detection rate, average latency, and false alarm rate were calculated to evaluate the model performance. The experimental results show that the model achieves an accuracy of over 95 % on the test set, with an average latency of less than 150 ms and a false alarm rate below 6.5 %. This indicates that the model demonstrates high accuracy and reliability in detecting cybersecurity threats. We also examined the false alarm rates of different models to comprehensively evaluate their performance. The performance metrics are shown as below:

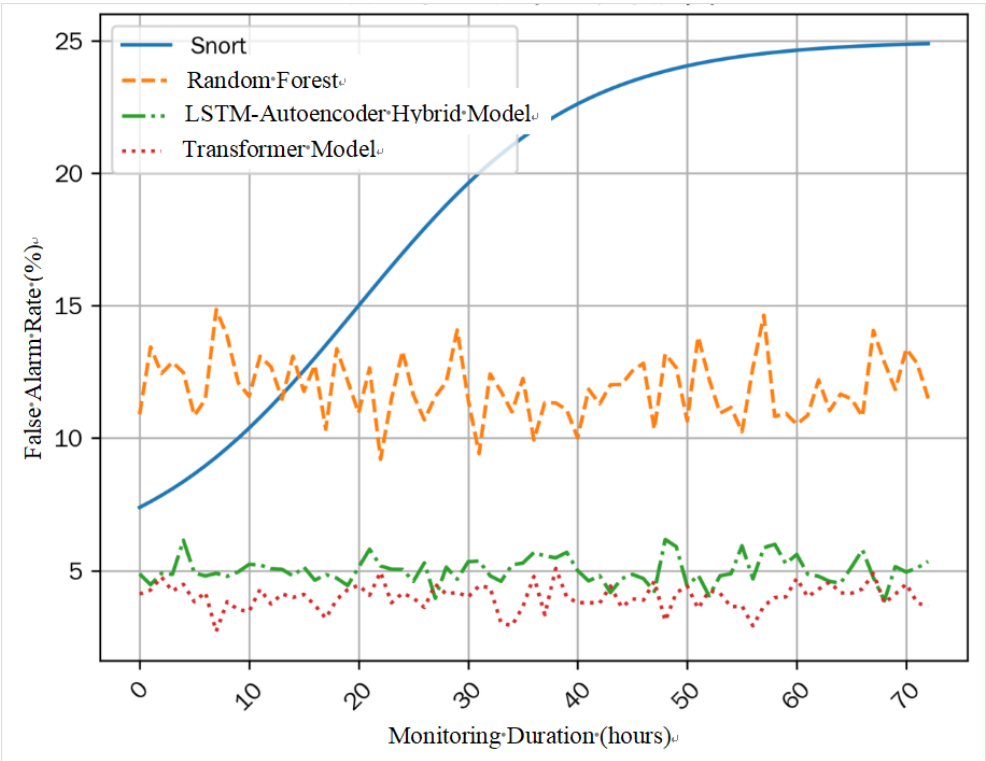

Figure 1. Performance metrics of different models.

From a qualitative perspective, we conducted comparative analyses of the model's performance across different scenarios. The results reveal certain variations and complementarities in its performance under different conditions. For example, in handling specific types of attacks (such as external malicious intrusions), the model exhibited high detection efficiency and accuracy; whereas in dealing with other types of attacks (such as unauthorized external connections), its performance was relatively poorer. This may be related to the distinct characteristics and patterns of different attack types. Therefore, future research could focus on more in-depth analysis and modelling for various attack types to further enhance the model's detection capability and generalization ability.

A detailed discussion and analysis of the experimental results is presented below. First, we analysed the factors contributing to the model's strong performance in detecting cybersecurity threats. These can be attributed to several aspects:

1) The use of the LSTM learning algorithm for modelling, which offers robust feature extraction and pattern recognition capabilities;
2) Sufficient data preprocessing and feature engineering, enabling the extraction of key and highly relevant features; and
3) The use of well-designed optimization methods and strategies during model training to ensure convergence and stability.

Second, we examined the reasons behind the model's underperformance in certain scenarios. Potential causes include: 1) variations in the characteristics and patterns of different attack types, which the current model may not fully capture; 2) potential deviation or limitations in the dataset, preventing the model from sufficiently learning the features of all attack categories; and 3) possible overfitting of the model, which can lead to reduced performance on the test set.

To address these issues, we propose the following improvements:

1) Conducting deeper analysis and modelling for different attack types to enhance detection capability and generalization;
2) Expanding the dataset in both scale and diversity to include a wider range of attack features and patterns;
3) Applying more advanced regularization techniques to mitigate overfitting; and
4) Exploring ensemble learning approaches to combine the outputs of multiple models, thereby improving overall performance.

5. Network Security Policies and Recommendations

5.1 Model-Based Cybersecurity Defence Strategies

AI model-based NSSA not only enables real-time, accurate identification of potential threats within the network but also provides smart aluminium smelters with a range of targeted defence strategies. These strategies are designed to dynamically respond to cybersecurity incidents, reduce security risks, and ensure the continuity and stability of production operations.

AI model-based NSSA can be integrated with firewalls to analyse network traffic and log data in real time, detect abnormal behaviours and potential threats, and dynamically adjust firewall rules accordingly. For example, it can block malicious IP addresses or restrict access to specific ports, thereby effectively cutting off attack paths and reducing security risks.

AI model-based NSSA can also be combined with intrusion detection systems (IDS) to enhance detection accuracy and efficiency. By performing in-depth analysis of network traffic and log

data, the AI model can identify more covert and sophisticated attack patterns, enabling more accurate intrusion detection and triggering corresponding defence measures.

5.2 Development Plan and Outlook

With the deepening of Industry 4.0, NSSA technology in smart factories will continue to evolve and improve. In the future, this field is expected to exhibit the following trends:

Future NSSA solutions will place greater emphasis on integration with emerging technologies. These synergies and innovations will drive NSSA technology to a higher level.

As NSSA technology sees broader adoption in smart factories, its standardization will become an inevitable trend. Establishing unified technical standards and specifications will ensure interoperability and compatibility among devices and solutions from different vendors, reduce integration and maintenance costs. Meanwhile, it will enhance the credibility and reliability of NSSA systems. This, in turn, will provide a stronger guarantee for industrial cybersecurity.

AI model-based NSSA will bring significant security benefits to smart aluminium smelters and even the whole Industry 4.0 ecosystem. By accurately detecting potential threats in real time and formulating targeted defence strategies, the technology will substantially improve smart factory cybersecurity, mitigate risks, and safeguard continuous and stable production operations. At the same time, this technology will accelerate the shift of smart factories toward smarter, more automated, and more efficient industrial environments. This will provide robust support for achieving Industry 4.0 objectives. As technology continues to advance, AI-based NSSA will play an increasingly pivotal role in securing industrial networks, acting as a guardian for smart factories in the future.

6. Conclusions

This study focuses on enhancing the NSSA capability of smart aluminium smelters through AI models, aiming to address the current cybersecurity threats and challenges faced by smart factories. During the research process, we thoroughly explored the concepts and frameworks of NSSA and its critical role in smart factories, and analysed the current applications and specific challenges of AI technology in the field of cybersecurity. Based on these theoretical foundations, we designed and implemented an AI-based NSSA model capable of real-time collection and processing of log data, network traffic, and other data within smart aluminium smelters, employing advanced algorithms such as deep learning for threat identification and early warning.

The main findings and contributions of this study can be summarized as follows:

First, we successfully constructed an AI-based NSSA model that demonstrated high detection efficiency and accuracy within the smart aluminium smelter environment. Through comparative experiments and result analyses, we proved the model's effectiveness and superiority in improving NSSA capability. This finding provides a new approach and method for cybersecurity protection in smart factories.

Second, this study conducted in-depth exploration and practice of AI model applications in network security situation awareness. We analysed the performance and characteristics of different AI algorithms in threat identification and selected the deep learning algorithm, best suited for the smart aluminium smelter environment for modelling. At the same time, we optimized the model's structure and parameters to enhance its detection efficiency and accuracy.

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).