International Journal of Engineering and Technology Innovation, vol. 15, no. 4, 2025, pp. 389-400

Information Security Protection System for Networked OT Environments of Industrial Control in Smart Manufacturing

Pin-Kuan Chiang, Shang-Liang Chen*, Je-Chiao Ku

Institute of Manufacturing Information and Systems, National Cheng Kung University, Tainan, Taiwan, ROC

Received 13 January 2025; received in revised form 24 August 2025; accepted 25 August 2025

DOI: https://doi.org/10.46604/ijeti.2025.14743

Abstract

This study develops an innovative information security protection system for end devices in smart manufacturing industrial control environments. By employing six key functionalities—lightweight identity authentication, traffic analysis, key management, personnel authorization control, system status monitoring, and an alarm mechanism—the system addresses the limitations of traditional firewalls. Experimental procedures involved testing the system against common threats, including phishing (fraud), physical intrusion, and Denial of Service attacks. Results demonstrate over 90% success in mitigating these attacks while maintaining operational efficiency. Furthermore, real-time monitoring and alert features enhance data protection and ensure reliable factory operations.

Keywords: Smart manufacturing, OT security, endpoint protection, cybersecurity, Industry 4.0

1. Introduction

In the era of digital transformation, the integration of Information Technology (IT) and Operational Technology (OT) has become an inevitable trend [1-2]. Many manufacturers are progressively establishing flexible production systems capable of small-batch, diversified intelligent manufacturing by incorporating Internet of Things, big data, and artificial intelligence technologies. Factory automation is evolving toward smart automated facilities [3].

However, this evolution has also made smart manufacturing systems attractive targets for cybercriminals. Attackers disrupt operations through various methods, including network intrusions, social engineering, and ransomware attacks, creating leverage for negotiations with affected businesses.

According to IBM Security X-Force statistics [4], the manufacturing industry ranked eighth among all industries for information security incidents in 2019, representing 8% of attacks within the top ten sectors. By 2021, however, it had surged to first place and maintains this position today, with attack frequencies continuing to rise annually.

This trend stems from the manufacturing industry's minimal tolerance for operational downtime, making it an attractive target for cybercriminals seeking high-profit attacks. Consequently, from an enterprise perspective, strengthening information security protection capabilities for endpoint devices has become critically urgent.

According to IBM's Cost of a Data Breach Report 2025 [5], the industrial sector, including manufacturing, faced an average breach cost of USD 5.00 million. Supply chain compromises and malicious insiders were the most expensive vectors, while incidents involving IoT/OT environments further amplified costs. These findings underscore the urgent need for stronger cybersecurity in manufacturing and industrial networks.

* Corresponding author. E-mail address: slchen@ncku.edu.tw

In traditional manufacturing, the OT environment achieves production automation through I/O port communication, allowing operators not to worry about production information being hacked during transmission. However, with the advancement of technology, the concept and technology of smart automation are gradually introduced into the manufacturing industry, enhancing its production efficiency but also breaking the physical network isolation of the past OT environment, reducing the degree of data protection. Moreover, the equipment in the OT environment often uses relatively outdated operating system versions, leading to many information security vulnerabilities [6]. This situation results in a significant information security risk for the OT environment.

Despite numerous studies on industrial cybersecurity, most focus on IT systems, leaving a gap in addressing the specific vulnerabilities of OT endpoint devices. Research on OT security technologies such as key management, identity authentication, and traffic monitoring is still in its infancy. Current approaches often fail to balance security with the real-time operational needs of industrial processes.

To address the aforementioned challenges, this study aims to develop an information security protection system for end devices in the smart manufacturing industrial control field. This system is designed to guard against common OT field cyberattacks, such as phishing attacks, physical attacks, and Denial of Service (DoS) attacks, while also encrypting all communication content to strengthen the information security defense within the OT field.

All the information security technologies developed in this study can be installed in embedded devices and connected to machines via plug-ins. They are responsible for monitoring and auditing the incoming and outgoing information flow, thereby achieving the purpose of information security protection without affecting the operation of the machines. Expected outcomes are as follows:

(1) Implement fraud attack protection with a lightweight identity authentication algorithm, achieving a success rate of over 90%, effectively preventing confidential production data from being stolen by impersonators.
(2) Achieve DoS attack protection with Traffic Analysis Technology, with a success rate of over 90% and response time below 10ms, effectively preventing zombie devices from paralyzing factory services.
(3) Implement tracking attack protection with Key Management Technology, effectively preventing information transmission from being intercepted and cracked, while also establishing a special key renewal strategy to resist concerns of keys being brute-forced.
(4) Implement physical attack protection with Personnel Authorization Control Technology, effectively preventing hackers or illegal individuals from directly invading devices to view or alter confidential data.
(5) Establish a user-friendly system status monitoring interface.
(6) Create an information security protection system suitable for smart manufacturing industrial control fields.
(7) Reference international cybersecurity standards IEC 62443 [7], ISO 27017 [8], and ISO 27018 [9].

2. Research Review

This study aims to establish an information security protection system for the development and deployment in the OT application domain, enhancing the security of factory machinery and equipment. Therefore, this study will explore and reference the literature from various perspectives according to different protection mechanisms.

2.1. Key Management Technology

Key management mechanisms are categorized into centralized, decentralized [10], and distributed types [11]. Centralized management [12] consolidates all keys at a single location, but this approach may compromise system availability if the central

point is attacked. Decentralized management [13] distributes keys across multiple nodes to mitigate single-point failure risks, but its effectiveness diminishes when node devices are limited.

Distributed management [14] stores a complete key set at each node to enhance security and reduce system downtime risks. In smart manufacturing and industrial control environments, preventing production line stoppages due to unidentified causes is paramount. Therefore, centralized key management poses excessive risks for enterprises and is unsuitable for current industrial applications.

In industrial control environments, machines typically do not communicate directly with each other. Instead, all machine information is exclusively requested or controlled by SCADA Servers or Database Servers. Consequently, information transmission involves only two components in this architecture.

With such limited group membership, decentralized key management becomes ineffective, significantly increasing key compromise risks. Therefore, this study adopts distributed key management as the system's primary key management technique.

Nyssanbayeva et al. [9] proposed a distributed key management mechanism that generates a set of random keys from a main terminal node and delivers them to all terminal nodes within a domain in an offline secure manner. Subsequently, each terminal node encrypts this key to generate a PRIV_KEY and a CHECK_KEY, and stores them locally in a table format. If a device wishes to transmit information to a terminal node, it first sends the relevant information to the terminal device, which then goes through a verification process. If the verification is successful, the cipher key is sent to the device, which must then restore it to the original key to encrypt subsequent transmission actions. This study will refer to the content of the aforementioned literature to redesign and implement key management technology that fits the system application scenario.

2.2. Lightweight Identity Authentication Technology

As digitalization and smart technologies advance, information security for communication and collaboration among industrial control field devices has become critically important. Identity authentication protocols represent one of the crucial technologies ensuring safe, efficient, and seamless device communication processes [15-16].

Currently, most market-available identity authentication protocols utilize complex asymmetric encryption implementations. However, industrial production processes require rapid information transmission, and overly complex algorithms can impede production line data flow. Therefore, identity authentication algorithms for OT environments must meet practical production field requirements.

Lara et al. [17] and Esfahani et al. [18] proposed a lightweight identity authentication process dividing authentication into two phases: registration and identity verification. During registration, three roles participate: the controller, router, and authentication server. When a controller needs to transmit data to a router, it must first register and provide background information for subsequent identity verification.

The authentication server's primary function involves confirming the legitimacy of devices initiating communication requests. Identity verification utilizes HMAC-based computations divided into three components: HMAC1 verifies controller identity, HMAC2 verifies router identity, and HMAC3 provides final bilateral confirmation.

When HMAC values calculated by both parties match, this indicates both are legitimate transmitters and can commence data exchange. This study references the aforementioned literature to redesign and implement lightweight identity authentication technology suitable for the target system application scenario.

2.3. Traffic Analysis Technology

In current manufacturing environments, information flow and communication volumes between machines are preset to maintain production line stability. However, unidentified anomalies or internal network attacks may cause devices to abnormally transmit packets or excessively process irregular access requests. This leads to computing resource depletion, hindering normal device connections and potentially causing production line shutdowns.

To address this challenge, Chao Wang et al. [19] proposed a credibility evaluation mechanism for anomalous packets designed to assess network packet trustworthiness. The literature divides the evaluation process into three stages: direct credibility assessment, comprehensive trust evaluation, and reliability assessment.

In the direct credibility assessment stage, statistical processing is performed on time-series packet data from identical sources. During the comprehensive trust evaluation stage, the DS algorithm integrates multi-dimensional feature data from time series to calculate a unified trust function. In the reliability assessment stage, pignistic probability transformation theory is employed to avoid DS extreme values, yielding more accurate credibility measurements.

Upon completion of calculations, a trust percentage is obtained. High percentages indicate packets closely resemble normal traffic, while low percentages suggest potential anomalies. This study references the aforementioned literature to redesign and implement the Traffic Analysis Technology suitable for the target system application scenarios.

2.4. Personnel Authorization Control Technology

According to an information security survey by Datapro Research Corporation [20], human factors account for up to 60% of information security incidents. In traditional intelligent manufacturing environments, personnel information security management typically relies solely on establishing standard regulations. However, this approach cannot guarantee universal compliance, and despite regulatory frameworks, human factors remain a significant information security challenge for enterprises.

To address this dilemma, Keith Cooney [21] proposed a streamlined substation personnel authorization control mechanism. In substation operations, only engineers possess authorization to modify machine parameters or perform maintenance tasks. Therefore, this mechanism monitors two critical locations: the engineer's duty station and the machine safety protection network.

When the safety protection network activates, it indicates personnel approaching machinery. If the engineer remains in the duty station during this event, the SCADA server determines that the approaching individual is not an authorized engineer. Consequently, an alarm is triggered and management receives immediate notification.

This study references the aforementioned literature to redesign and implement personnel authorization control technology suitable for the target system application scenario.

3. Research Method

This study introduces the architecture of an information security protection system applied to smart manufacturing industrial control environments, as illustrated in Figure 1. The system employs various security protection technologies to defend against common OT field attacks, including phishing, tracking, physical, and DoS attacks, thereby ensuring comprehensive security defense capabilities in OT environments. This research further explains the system's service architecture by detailing its Key Management Technology, Lightweight Identity Authentication Technology, Traffic Analysis Technology, and Personnel Authorization Control Technology.

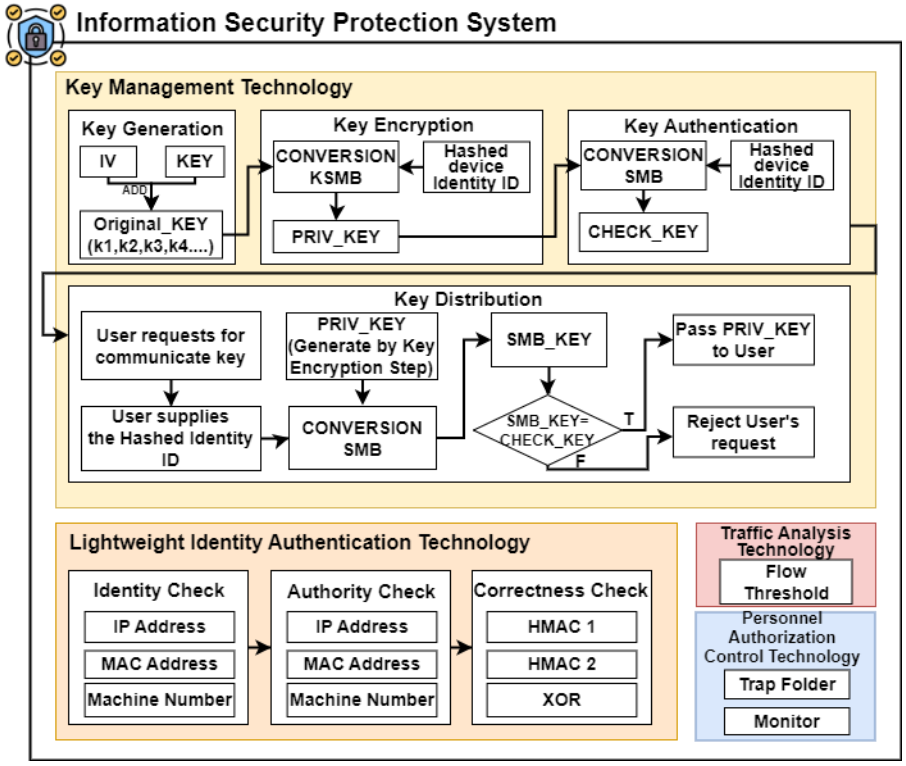


Fig. 1 The architecture of the information security protection system

3.1. Key Management Technology

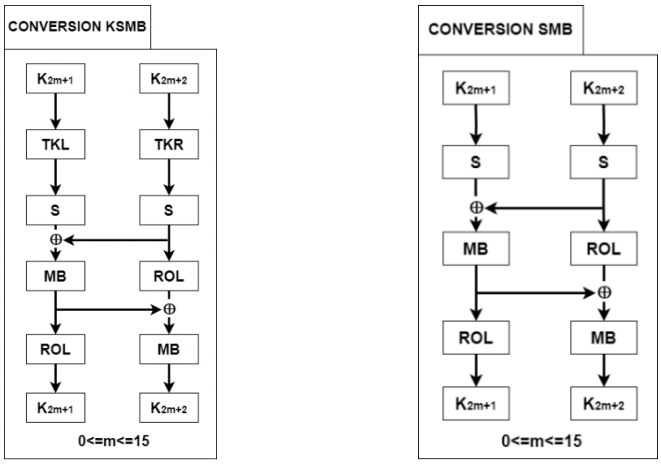
The key management technique used in this study will adopt distributed key management technology [14, 22] for its design. This ensures that the encryption and decryption processes during data transmission can be securely executed. Through this mechanism, even if data packets are intercepted by malicious devices, malicious users cannot decrypt the content without the corresponding decryption keys, thereby safeguarding the security of the information and preventing tracking attacks. The entire management process is divided into four parts: key generation, key encryption, key authentication, and key distribution.

(1) Key Generation: The KEY and IV of the AES encryption methods are merged for computation, serving as the Original_KEY (k1, k2, k3, k4...) for this key management.

(2) Key Encryption: A terminal device is required to generate a random identity code, which is then hashed to obtain the Hashed Device Identity ID. Subsequently, the Original_KEY and the Hashed Device Identity ID are input as bits into the CONVERSION KSMB for the encryption of the key. The CONVERSION KSMB consists of a new encryption architecture composed of bit substitution encryption, non-positional encryption, and linear transformation encryption methods (as shown in Fig. 2(a)). Here, S represents the bit substitution encryption method, TKR and TKL represent the non-positional encryption methods, ROL refers to the aforementioned Hashed Device Identity ID, MB denotes the linear transformation encryption method, and ⊕ represents the XOR operation. Finally, a PRIV_KEY is produced.

(3) Key Authentication: The key authentication will require a CONVERSION SMB using PRIV_KEY and Hashed Device Identity ID, as shown in Fig. 2(b). "S" stands for substitution cipher, "ROL" refers to the Hashed Device Identity ID mentioned above, "MB" is a linear transformation cipher, and "⊕" represents the XOR operation. Finally, a CHECK_KEY will be generated and stored along with the PRIV_KEY in a key table on the local side.

(4) Key Distribution: Before the Database Server requests machine data, it must first request its communication key. Therefore, it will transmit the hash value of the key device's identity code to Device 1, allowing Device 1 to generate an identity verification code through CONVERSION SMB. If the identity verification code matches the stored CHECK_KEY, it means that this Database Server is a qualified communication partner. Thus, the encrypted key (PRIV_KEY) is sent back to the Database Server for it to decode and use for subsequent message encryption.



(a) CONVERSION KSMB Algorithm (b) CONVERSION SMB Algorithm

Fig. 2 Key Management Technology Algorithm

3.2. Lightweight Identity Authentication Technology

The study's Lightweight Identity Authentication Technology performs identity verification between a proxy device and an authentication server before a device requests data from a machine or terminal sensors. This ensures that the requesting device has the necessary credentials, thereby preventing fraudulent attacks. The protocol is divided into three steps: identity verification, permission verification, and correctness verification.

(1) Identity Check: The equipment initially requests machine information from the agent device of the machine. At this point, the agent device sends the requesting device's background information to the authentication server for the first stage of identity verification, ensuring that this equipment is a legitimate device within the current factory premises, rather than a device illegally brought in by an employee or infiltrated by hackers.

(2) Authority Check: The proxy device then transmits the requesting device's identity information to the authentication server for a second stage of authorization verification. This ensures that the requesting device remains within the factory premises and has the proper permissions to make the request, rather than being impersonated by a hacker.

(3) Correctness Check: The requesting device performs an XOR operation on its identity information with a randomly generated nonce key, then applies a hash function to generate a unique identity verification code, HMAC1, which is sent to the proxy device. Upon receipt, the proxy device calculates HMAC1_1 using the same algorithm and the previously stored information about the requesting device. If the two codes match, the proxy device performs an XOR operation on its own identity information with a randomly generated nonce key and applies a hash function to generate a new identity verification code, HMAC2, which is sent back to the requesting device. Once HMAC2 is received, the requesting device calculates HMAC2_1 using the same algorithm and the previously stored information about the proxy device. If these two codes match, it indicates that the device authentication is successful, and data requests or other subsequent actions can be carried out with the machinery.

3.3. Traffic Analysis Technology

The Traffic Analysis Technology developed in this study employs packet sniffing techniques to continuously monitor all IP traffic within manufacturing environments over specified time intervals. This system establishes baseline traffic patterns for different operational zones and production cycles, enabling administrators to configure dynamic thresholds based on historical network behavior data. The technology utilizes statistical analysis algorithms to distinguish between legitimate traffic variations caused by normal production activities and potentially malicious network anomalies.

When the system detects packet volumes significantly exceeding established baselines, the anomaly detection mechanism immediately triggers a comprehensive response protocol. The system first notifies administrators through multiple communication channels, then initiates automated threat mitigation procedures, including antivirus scanning of affected devices and controlled network isolation capabilities. For severe threats, the system can execute power-off procedures for compromised equipment to prevent DoS attacks from disrupting critical production operations.

The Traffic Analysis Technology integrates seamlessly with existing industrial control systems while maintaining detailed activity logs for forensic analysis and continuous security improvement. This proactive approach ensures robust network protection while minimizing impact on manufacturing productivity and operational continuity.

3.4. Personnel Authorization Control Technology

The Personnel Authorization Control Technology proposed in this study will continuously monitor confidential information (such as code and secret production data) on field equipment. When a command or operation attempts to execute this confidential data, the mechanism will detect the abnormal behavior and immediately notify the system. In the engineer's duty room, a dedicated camera will record the engineer's real-time status. Through the YOLO v7 deep learning model for real-time image recognition, the identity of the personnel in the duty room is verified, and this information is updated to the system in real time.

To establish an effective image recognition model, this experiment pre-recorded 10 minutes of video footage of engineers at their workstations, extracting approximately 594 engineer images for training. The dataset was split using a 7:3 ratio, with the training set containing 417 images and the test set containing 177 images. After model training, a 2-minute validation test was conducted in the actual workplace environment, achieving an image recognition accuracy rate of 94.6%, ensuring reliable personnel identity verification.

When the system detects that the confidential data is being accessed while the engineer is in the duty room, it suggests that someone without modification rights is physically tampering with the machine. Therefore, the system will promptly notify the manager, enabling them to quickly understand the situation and respond accordingly.

4. Research Experiment

This study will design corresponding experimental testing scenarios for the four developed cybersecurity protection technologies to verify the system's practical results. The experiments are intended not only to simulate real-world attack vectors that may threaten smart manufacturing environments but also to validate whether the proposed methods can effectively resist them. By constructing realistic factory-level scenarios, the tests will demonstrate how the technologies respond to unauthorized access, network interception, denial-of-service attempts, and physical tampering.

(1) Key management technology:

Network Packet Sniffing is a network monitoring technology that allows users to capture data packets flowing through the network. Thus, an unauthorized PC might use the Wireshark tool to monitor the network and intercept packets transmitted within the factory area, attempting to steal confidential information. However, due to the factory's implementation of Key Management Technology, even if the unauthorized PC can sniff packets, it cannot decrypt them. This test scenario aims to evaluate whether Key Management Technology can provide robust protection for enterprises, effectively resisting Pursuit Attacks, a method of intercepting and analyzing network traffic.

(2) Lightweight identity authentication technology:

The unauthorized PC attempted to request machine information from the agent device in an effort to obtain confidential machine data under fraudulent pretenses. However, due to the implementation of Lightweight Identity Authentication

Technology within the factory domain, the request from the unauthorized PC was denied. This test scenario primarily aimed to assess whether Lightweight Identity Authentication Technology could provide protective measures for enterprises and effectively resist Cheat Attacks.

(3) Traffic analysis technology:

Due to a malfunction in the Database Server, continuous brute-force requests were sent to the agent devices, potentially crippling their services and causing partial production line shutdowns. By implementing Traffic Analysis Technology in the factory domain, the agent devices can promptly block the sources of these brute-force requests and alert the system, requesting assistance from technical personnel. This testing scenario primarily evaluates whether Traffic Analysis Technology can effectively protect enterprises and mitigate DoS attacks.

(4) Personnel authorization control technology

Personnel intend to directly modify confidential information (such as code and sensitive production data) on agent equipment, despite not being engineers or technicians authorized to perform modifications at the factory site. This behavior could potentially lead to system operation errors. However, due to the implementation of Personnel Authorization Control Technology in the factory, the agent equipment can immediately monitor this activity and promptly report it to the system, alerting the factory administrator to address the situation. This scenario primarily tests whether Personnel Authorization Control Technology can provide protective services for enterprises and effectively resist physical attacks.

5. Experimental results and analysis

This study will conduct experimental tests as illustrated in Fig. 3. Throughout the process, various types of attacks and their corresponding defense mechanisms will be documented. The effectiveness of these mechanisms will also be analyzed. The results aim to demonstrate how the proposed cybersecurity defense system enhances the security of OT environments in enterprises. The following sections will present the experimental results based on different testing scenarios.

5.1. Key Management Technology test results

During the testing process of Key Management Technology, although the unauthorized PC can monitor the packets transmitted within the factory domain through Wireshark, the packets themselves have been encrypted using AES encryption, as shown in Fig. 3, preventing unauthorized PCs from viewing complete packet information. Additionally, AES itself possesses strong resistance to brute-force attacks, meaning that even if hackers attempt to decrypt packet information through brute-force computation, it would be unlikely to succeed within a short period of time. In addition, the mechanism proposed in this research updates keys every 30 seconds, and the keys configured and updated for each device are randomly generated, effectively preventing malicious individuals from brute-forcing the keys.

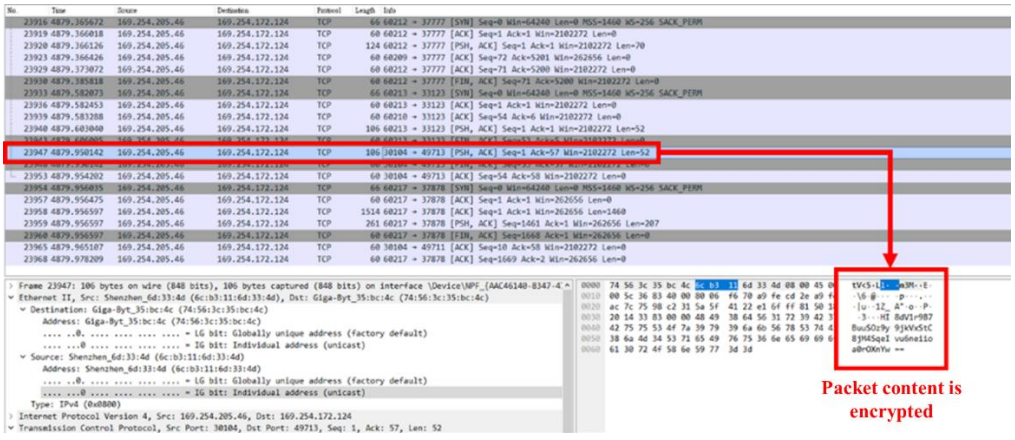
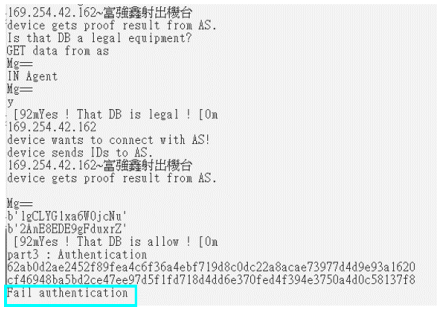


Fig. 3 Key Management Technology Test Result Diagram

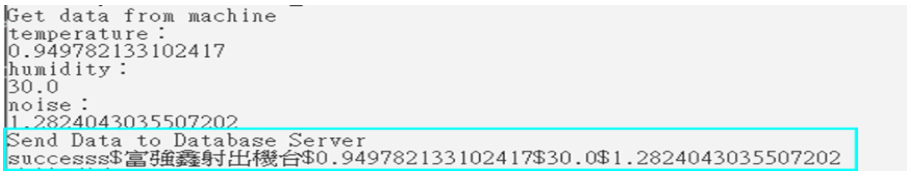
5.2. Lightweight Identity Authentication Technology test results

During the testing phase of the Lightweight Identity Authentication Technology, the system was able to effectively intercept devices that lacked legitimacy, proper authorization, or correctness every time, thereby ensuring the confidentiality of machine information and sensor data. The interception success rate reached 100%, indicating that the Lightweight Identity Authentication Technology is capable of providing reliable and effective services. As shown in Fig. 4(a), it is evident that a device intends to request confidential machine data from a CNC machine. However, upon authentication by the proxy device and the NCKU_IIoT_LWA Server, it was found that the request lacked correctness, resulting in its interception. Conversely, if the requesting device successfully passes verification, the proxy device will return the machine or sensor data, as shown in Figs. 4(b) and 4(c).



(a) Certification failed

(b) Certification succeeded



(c) Return machine values

Fig. 4 Lightweight Identity Authentication Technology Test Result Diagram

5.3. Traffic Analysis Technology

During the testing of Traffic Analysis Technology, the system continuously monitors traffic for different IPs. Consequently, when the Database Server sends excessive requests to a particular agent device, Traffic Analysis Technology can detect this abnormal behavior and immediately issue a notification. This ensures uninterrupted service for field devices, achieving a 100% detection success rate. As shown in the system-monitoring interface in Fig. 5, when the Database Server launches a ten-minute DoS attack against a single machine, the simulation generates 1,000 data-request packets—exceeding the 500-packet threshold set by the enterprise's domain experts—and consequently triggers an alert.

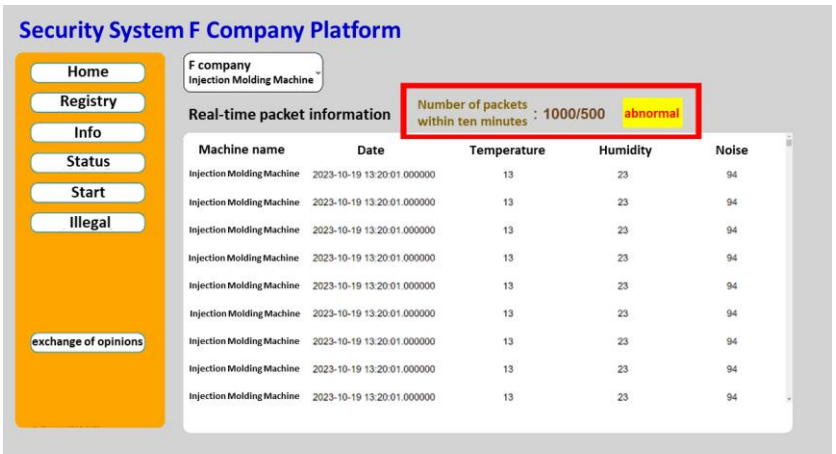


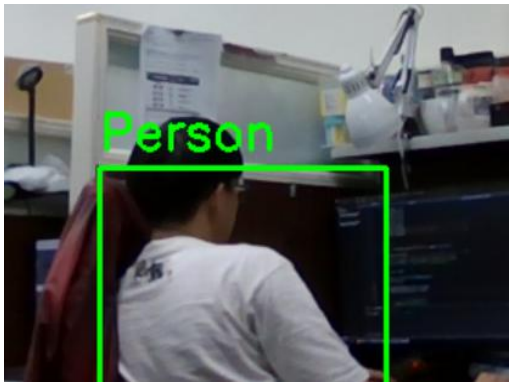
Fig. 5 Traffic Analysis Technology Test Result Diagram

5.4. Personnel Authorization Control Technology

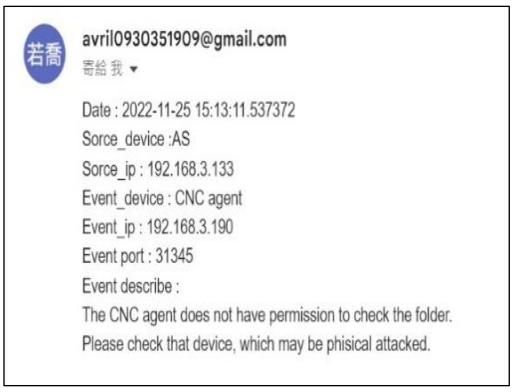
During the testing of Personnel Authorization Control Technology, the system successfully detected unauthorized users attempting to modify confidential data each time. It took appropriate measures to report and handle such incidents, thereby ensuring the confidentiality of sensitive information with a detection success rate of 100%. As shown in Fig. 6(a), the system captures the behavior of unauthorized users attempting to access devices equipped with Personnel Authorization Control Technology, recording the actions taken. As shown in Fig. 6(b), the system integrates video recognition results from the control room to infer that the current operator of the device is unauthorized. As illustrated in Fig. 6(c), the system immediately notifies the factory manager of further action.

```
send: AS_192.168.3.133_CNC agent_192.168.3.190_31345_3_2022-11-25 15:12:43.300242
ACCESS event: /home/pi/Desktop/old/data
send: AS_192.168.3.133_CNC agent_192.168.3.190_31345_3_2022-11-25 15:12:43.305749
CLOSE_NOWRITE event: /home/pi/Desktop/old/data
send: AS_192.168.3.133_CNC agent_192.168.3.190_31345_3_2022-11-25 15:12:43.315344
```

(a) Somebody is performing access operations on the equipment



(b) The engineer has been detected to currently on duty in the control room



(c) Report to the Site Administrator

Fig. 6 Personnel Authorization Control Technology Test Result Diagram

6. Conclusion

This study has developed a robust information security protection system for OT endpoint devices in smart manufacturing environments. The system incorporates technologies such as lightweight identity authentication, traffic analysis, key management, and personnel authorization control. By addressing common cyber threats and enhancing endpoint security, the proposed system ensures both operational efficiency and data confidentiality. The conclusions are summarized as follows:

(1) Key Management Technology: The proposed system adopts distributed key management technology to ensure secure encryption and decryption of communication. This mechanism effectively prevents tracking attacks and brute-force decryption attempts, safeguarding sensitive data transmission in industrial environments.

(2) Lightweight Identity Authentication Technology: The lightweight identity authentication technology achieves a 100% success rate in detecting unauthorized access requests, ensuring the integrity and confidentiality of machine data and sensor information without affecting production line efficiency.

(3) Traffic Analysis Technology: The system detects and mitigates abnormal traffic, such as DoS attacks, with a 100% success rate. This capability ensures uninterrupted factory operations by preventing service disruptions caused by excessive traffic or malicious requests.

(4) Personnel Authorization Control Technology: The personnel authorization control mechanism effectively identifies and responds to unauthorized access to sensitive information or system components. This feature enhances security by notifying managers immediately and preventing potential tampering or data breaches.

The system has been successfully implemented and validated through various experimental scenarios, demonstrating its ability to enhance endpoint security in OT environments. This study provides a comprehensive solution that balances security and operational needs in smart manufacturing. By integrating these innovative technologies, this study contributes to the development of a secure and reliable smart manufacturing ecosystem. The patented system (Patent No. 822417) ensures effective protection against diverse cyber threats while maintaining high production efficiency.

Acknowledgments

Part of the research results were funded by the National Science and Technology Council of ROC under Grant No. MOST 111-2218-E-006-015- and 110-EC-17-A-05-S5-011. The financial support is gratefully acknowledged.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] P. Lipnicki, D. Lewandowski, D. Pareschi, W. Pakos, and E. Ragaini, "Future of IoTSP – IT and OT Integration," Proceedings of IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 203-207, 2018.

[2] I. Ivanković, A. Kekelj, R. Rubeša and I. Kuzle, "SCADA Maintenance and Refurbishment with Security Issue in Modern IT and OT Environment," Proceedings of Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MEDPOWER 2018), pp. 1-6, 2018.

[3] R. Paes, D. C. Mazur, B. K. Venne, and J. Ostrzenski, "A Guide to Securing Industrial Control Networks: Integrating IT and OT Systems," IEEE Industry Applications Magazine, vol. 26, no. 2, pp. 47-53, 2020.

[4] IBM, "IBM X-Force Threat Intelligence Index 2024," https://github.com/jacobdjwilson/awesome-annual-security-reports/blob/main/Annual%20Security%20Reports/2024/IBM-X-Force-Threat-Intelligence-Index-2024.pdf, accessed in 2024.

[5] IBM Security, "Cost of a Data Breach Report 2025: The AI Oversight Gap," https://www.ibm.com/reports/data-breach, accessed in 2025.

[6] M. Marali, S. D. Sudarsan, and A. Gogioneni, "Cyber Security Threats in Industrial Control Systems and Protection," Proceedings of International Conference on Advances in Computing and Communication Engineering (ICACCE), pp. 1-7, 2019.

[7] B. Leander, A. Čaušević, and H. Hansson, "Applicability of the IEC 62443 Standard in Industry 4.0/IIoT," Proceedings of the 14th International Conference Availability, Reliability and Security (ARES), article no. 101, pp. 1-8, 2019.

[8] N. A. Kamaruddin, I. Mohamed, A. D. Jarno, and M. Daud, "Cloud Security Pre-assessment Model for Cloud Service Provider Based On ISO/IEC 27017:2015 Additional Control," International Journal of Innovation and Industrial Revolution, vol. 2, no. 5, pp. 1-17, 2020.

[9] P. de Hert, V. Papakonstantinou, and I. Kamara, "The New Cloud Computing ISO/IEC 27018 Standard Through the Lens of the EU Legislation on Data Protection," vol. 32, no. 1, pp. 16-30, 2014.

[10] J. Ni, G. Fang, Y. Zhao, J. Ren, L. Chen, and Y. Ren, "Distributed Group Key Management Based on Blockchain," Electronics, vol. 13, no. 11, article no. 2216, 2024.

[11] O. Pal, B. Alam, V. Thakur, and S. Singh, "Key Management for Blockchain Technology," ICT Express, vol. 7, no. 1, pp. 76-80, 2021.

[12] J. Liu, X. Tong, Z. Wang, M. Zhang, and J. Ma, "A Centralized Key Management Scheme Based on McEliece PKC for Space Network," IEEE Access, vol. 8, pp. 42708-42719, 2020.

[13] W. Zhou, Y. Xu, and G. Wang, "Decentralized Group Key Management for Hierarchical Access Control Using Multilinear Forms," Concurrency and Computation: Practice and Experience, vol. 28, no. 3, pp. 631-645, 2016.

[14] S. E. Nyssanbayeva, N. A. Kapalova, and A. Haumen, "On a Certain Model of Cryptographic Key Management," Eurasian Journal of Mathematical and Computer Applications, vol. 8, no. 4, pp. 15-22, 2022.

[15] G. J. Simmons, "Symmetric and Asymmetric Encryption," ACM Computing Surveys, vol. 11, no. 4, pp. 305-330, 1979.

[16] A. Garba, D. Khoury, P. Balian, S. Haddad, J. Sayah, and Z. Chen, "LightCert4IoTs: Blockchain-Based Lightweight Certificates Authentication for IoT Applications," IEEE Access, vol. 11, pp. 28370-28383, 2023.

[17] E. Lara, L. Aguilar, M. A. Sanchez, and J. A. García "Lightweight Authentication Protocol for M2M Communications of Resource-constrained Devices in Industrial Internet of Things," Sensors, vol. 20, no. 2, article no. 501, 2020.

[18] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, and A. Bicaku, "A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment," IEEE Internet of Things Journal, vol. 6, no. 1, pp. 288-296, 2019.

[19] C. Wang, "IoT Anomaly Detection Method in Intelligent Manufacturing Industry Based on Trusted Evaluation," The International Journal of Advanced Manufacturing Technology, vol. 107, pp. 993-1005, 2020.

[20] INFO SECURITY, "The Greatest Threat to Information Security—Personnel Security, " https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=672, accessed in 2024.

[21] K. Cooney, "Operational Technology Intrusion Detection Application for Power Grid Security Operations Centres," Master Thesis, National College of Ireland, Dublin, Ireland, 2021.

[22] S. B. Sarvaiya and D. N. Satange, "Security in IP-Based IoT Node and Device Authentication," Proceedings of IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), pp. 1-5, 2022.