Analysis and Research on Secure Access Control Technology of Industrial Internet of Things Based on ZTM Model

Yanliu Nie

School of Information Engineering and Big Data, Zhengzhou Technical College, Zhengzhou, 450000, Henan, China
E-mail: zz109109109@163.com

Received 15 December 2023; Accepted 05 February 2024

Abstract

The security threat of IIoT is becoming increasingly serious. In order to address this challenge, security access control technology based on the ZTM model has become a hot research topic. The aim of this study is to conduct in-depth analysis and research on the security access control technology applied by the ZTM model in industrial Internet of Things environments. By analyzing the current challenges of IIOT security and the limitations of traditional security models, this paper proposes a series of security access control technologies related to the ZTM model, aiming to quantify and evaluate the effectiveness of access control policies, zero trust of the system, and comprehensive risk assessment. By using empirical research methods, this study verified the feasibility of the proposed technology in actual industrial Internet of Things environments and demonstrated the significant effect of the ZTM model in reducing security risks and improving system credibility.

Journal of Cyber Security and Mobility, Vol. 13_4, 585–604.
doi: 10.13052/jcsm2245-1439.1341

The experimental results showed that the optimized security access control technology improved security performance by 28% and the missed detection rate was as low as 3.2%. This study provides useful insights for practical applications in the field of secure access control and provides a solid foundation for future research.

Keywords: Industrial Internet of Things, zero-trust model, secure access control technology, comprehensive risk assessment.

1 Introduction

With the rapid development of information technology, the IIoT (Industrial Internet of Things) has emerged in the field of industrial production, which not only greatly improves production efficiency and flexibility, but also opens up a new era of digital transformation for enterprises. In this digital wave, the interconnection of devices and real-time data communication have become the key elements driving innovation in the production process [1, 2]. However, it is accompanied by new challenges facing cyber security, especially with the growing scale of the IIoT. The rapid development of the IIoT has brought unprecedented opportunities, but also accompanied by risks and challenges. As the number of devices increases dramatically and the complexity increases, traditional cyber security measures have become inadequate. The special nature and real-time needs of the IIoT show a series of limitations, forcing us to seek innovative security solutions.

Adopting zero trust methods can help protect complex OT systems and reduce potential risks to network security in manufacturing and critical infrastructure. The zero-trust method helps to protect critical industrial infrastructure. Ritesh Agrawal, CEO and co-founder of Aircap Networks, stated that while this is not the only option, it is an excellent solution for Information Technology (IT) and Operations Technology (OT). In the given context, comprehensively characterizing the evaluation practices of intrusion detection methods for smartphones is of paramount significance [3]. Amidst the prevailing landscape, addressing the pressing challenge of safeguarding data and systems within the intricacies of smartphone security emerges as a critical imperative. This necessitates a meticulous exploration not only into the intricacies of access control technology but also calls for groundbreaking innovations in established cybersecurity concepts [4].

The zero-trust model (ZTM) has attracted much attention because of its unique concept, providing a new path to solve the security problem of the IIoT [5, 6]. The core idea of ZTM is to distrust any component of the network, always requiring verification and authorization. This innovation of traditional cybersecurity methods makes ZTM a powerful tool to address the security challenges of industrial IoT. Zero trust is a security model that continuously verifies and dynamically authorizes all users based on as many trust elements as possible, such as access subject identity, network environment, and terminal status. Zero trust is very different from the traditional security model. The traditional security model evaluates the entity risk through the way of "one verification + static authorization", while zero trust builds the security cornerstone of the enterprise [7, 8] based on the mode of "continuous verification + dynamic authorization". The idea behind zero-trust networks is to assume that there are attackers both inside and outside the network, so no user or machine should be automatically trusted [9].

Implementing a zero-trust approach towards individuals, terminals, and applications through unified identity management is crucial. Establishing an access control mechanism centered around identity involves implementing timeouts after login and connection establishment. This compels users and devices to undergo dynamic authentication based on identity, network environment, and terminal status. Continuous monitoring of potential violations and abnormal behaviors during the access process is essential to ensure the ongoing trustworthiness of network users and terminals [10].

Zero trust network using differential, differential is a kind of security boundary is divided into small areas, to maintain access to each part of the network, at the same time also can access target access to application level, function level, data level, only open to access the application, function or data, meet the principle of minimum authority, greatly shrink potential attack. At the same time, the security control strategy is based on the access subject, the target object and the environment attributes, to realize the fine and dynamic control [11, 12] of application, function, data and other dimensions.

This study aims to explore innovative solutions of secure access control technology through in-depth analysis and research based on ZTM model. Through the analysis of existing problems and the exploration of innovative solutions, this research aims to provide practical solutions for the industrial Iot security field, promote the sustainable development of IIoT, this study will be the application of ZTM model from different angles, deeply discuss all aspects of IIoT security access control technology, to provide readers with a comprehensive and in-depth understanding.

2 Overview of ZTM Model

2.1 Core Principles of ZTM

The main concept of the zero-trust security model is "never trust, always verify", which means that devices should not be trusted by default, even if they are connected to a licensed network and have previously been verified. Most modern enterprises have complex network structures, including numerous interconnected regions, cloud services, and infrastructure, as well as connections to remote and mobile environments, and unconventional IT connections. The zero-trust principle is due to the fact that traditional methods are not suitable for the complexity of enterprise networks. Zero trust advocates mutual authentication, including checking device identity and integrity without considering location, and combining user authentication based on confidence in device identity and condition to provide access permissions to applications and services [13]. This includes security measures such as multi-factor authentication and biometric identification to ensure that only legitimate entities have access to system resources, reducing the risk of access for potential attackers. The minimum permission principle emphasizes in the ZTM design that each entity should be granted the minimum required permission, regardless of its location within the system. By limiting access to sensitive resources, the ZTM model helps to reduce the possibility of lateral diffusion, thereby improving the overall security of the system. At the same time, real-time access control, network segmentation, differential isolation and other strategies are all designed to provide a more flexible and powerful security defense mechanism in the face of increasingly complex security threats. Through visibility and intelligent analysis, the ZTM model aims to fully understand the network and user behavior, and identify potential threats in time to maintain the security and stability of the system.

2.2 Optimization Method of ZTM

To enhance the effectiveness and adaptability of the ZTM model, a range of optimization methods can be implemented [14]. The integration of advanced authentication techniques, including biometric identification and multifactor authentication, can significantly enhance the accuracy of user, device, and application identities within ZTM models. This enhancement effectively mitigates the risks associated with identity camouflage and unauthorized access, contributing to an overall improvement in the security posture of the system.

Intelligent access control strategy conducts dynamic and intelligent access control by combining real-time context information, such as user

location, device status, network status, etc. [15]. It can not only improve the flexibility of the system, but also timely respond to potential threats to ensure the timeliness of security defense. The optimization of network segmentation and differential isolation can limit the communication between different regions through more refined network division, which can reduce the risk of lateral diffusion and improve the overall security of the system. This differential isolation strategy requires more intelligent, dynamic network management to ensure a balance between security and efficiency [16, 17]. The optimization method of ZTM model should focus on improving the accuracy of authentication, developing intelligent access control strategies, and optimizing the implementation of network segmentation and differential isolation. Through these optimization means, the ZTM model can better adapt to the evolving threat environment and improve the resistance to various attack means.

The optimization of the ZTM model should concentrate on three key areas: enhancing authentication accuracy, developing intelligent access control strategies, and refining the implementation of network segmentation and differential isolation. By embracing these optimization measures, the ZTM model can effectively adapt to the evolving threat landscape, fortifying its resilience against various attack vectors. This proactive approach ensures that the ZTM framework remains at the forefront of secure access control technologies, providing robust protection in the face of ever-changing cybersecurity challenges.

3 Industrial Internet of Things Security Challenges and Access Control Technology

3.1 IIoT Security Challenges

The rapid development of the IIoT has brought about many innovations and efficiency improvements, but it is also accompanied by a series of severe security challenges. Device diversity and complexity make security management even more difficult [18, 19]. In industrial environments, there are various types of IoT devices that may come from different manufacturers and use different communication protocols and standards, so uniform security standards and management become very challenging. The requirements of real-time performance and high availability increase the difficulty of security. Industrial systems have a high demand for real-time data and responsiveness, but it also makes the introduction of security measures more sensitive. Any

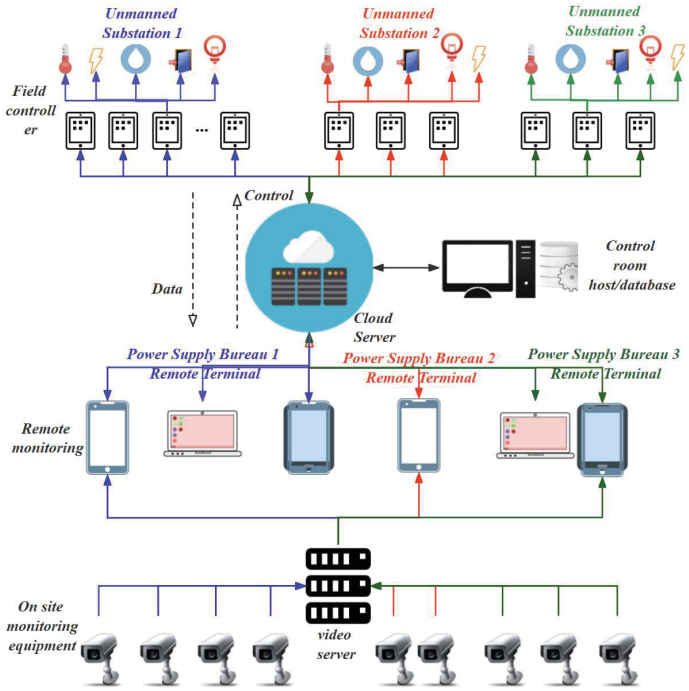

Figure 1 Internet of Things device architecture.

introduction of security measures to the system must ensure that real-time and availability of the system is not sacrificed.

Figure 1 illustrates the device architecture of the Internet of Things. In IIoT, a multitude of sensors and device communications may handle significant volumes of sensitive information, including production data and process parameters. As highlighted by [20], ensuring the privacy and protection of this data poses a considerable challenge. The processing of such information necessitates a guarantee of confidentiality, integrity, and availability to prevent unauthorized access or tampering. Industrial systems often operate continuously, presenting challenges for security updates and maintenance. The conventional security update approach may disrupt system operations, emphasizing the need for well-defined update policies that ensure safety without compromising production. The complexity of IIoT security challenges is notably evident in the requirements for device diversity, real-time and high availability, data privacy protection, as well as security updates and maintenance [21].

In response to the evolving nature of these challenges, security strategies must be tailored to accommodate the unique characteristics of IIoT environments. This entails the development and implementation of solutions that not only fortify data privacy and protection but also seamlessly integrate with the uninterrupted operational demands of industrial systems. Moreover, strategies should encompass real-time threat detection and response mechanisms, ensuring that any potential security incidents are identified and addressed promptly.

3.2 Current Status of Access Control Technology

Access control technology in the field of information security mainly ensures the security of data and systems by limiting and managing access to resources by users, devices or systems. Currently, access control technology presents diversity and complexity of [22, 23].

Different security access control models and technologies, such as free access, mandatory access, role-based access, and attribute-based access, as well as access control lists, access matrices, and access control policies, have their own characteristics and differences, mainly reflected in permission allocation, security, flexibility, scalability, implementation complexity, performance, and manageability.

Traditional access control models mainly include role-based access control (RBAC) and attribute-based access control (ABAC). RBAC simplifies permission management by assigning users to different roles and then defining the corresponding privileges for each role. The ABAC determines its access to the resource according to the user's attributes. These traditional models provide the basic framework for access control to some extent, but they struggle to meet the complex and changeable access needs. In recent years, with the development of information technology, advanced access control technologies are constantly emerging. Dynamic access control technologies, such as context-aware access control (CAC) and subjective logic access control (SAC), enable flexible access control decisions based on the real-time environmental context and the user's subjective logic. This access control model based on event, environment and user context is more suitable for today's complex and changeable information system needs. Emerging technologies such as attribute-based dynamic access control (DABAC) and risk-based access control (RAC) are also emerging on the horizon. DABAC enables more flexible access control [24, 25] by dynamically managing and adjusting user attributes. RAC, on the other hand, relies on risk assessment

and more intelligently and dynamically adjusts visits to the changing threat environment.

3.3 Integration of the IIoT and Access Control

The rise of the IIoT is leading a radical change in the industrial production mode. With the widespread application and large-scale deployment of Internet of Things devices, industrial production systems have gradually entered an era of high digitalization and interconnection. However, this change is also accompanied by new challenges, and one of the most pressing issues is how to effectively implement secure access control to ensure the security of data and systems in industrial IoT environments [26, 27].

The IIoT refers to a system that realizes real-time communication and data exchange between devices through the Internet to connect and integrate sensors, actuators and other devices. Compared with the traditional Internet of Things, the IIoT pays more attention to real-time, stability and reliability, and is widely used in manufacturing, energy, transportation and other industrial fields. In the highly interconnected IIoT environment, the role of access control cannot be ignored. Access control is a way of limiting access to a system, a network, or a specific resource by defining and implementing rules. In the IIoT, access control is not only a part of network security, but also a cornerstone of ensuring the safe operation of physical equipment and production systems. The systematic dynamic risk assessment can be expressed as a weighted sum of the various risk factors as shown in Equation (1).

$$Risk = \sum_{i=1}^{n} (Weight_i \times Risk\ Factor_i) \tag{1}$$

Adaptive access control systems may use scoring mechanisms based on contextual factors. The score can be calculated as described in Equation (2):

$$Access\ Score = \sum_{j=1}^{m} Factor_j \times Weight_j \tag{2}$$

Considering the context-aware threat, the probability of threat occurrence can be calculated using the Bayesian probability, as shown in Equation (3):

$$P(Threat|Context) = \frac{P(Context|Threat) \times P(Threat)}{P(Context)} \tag{3}$$

Figure 2 shows the application framework of the Internet of Things. Access control in the IIoT environment faces unique challenges, including

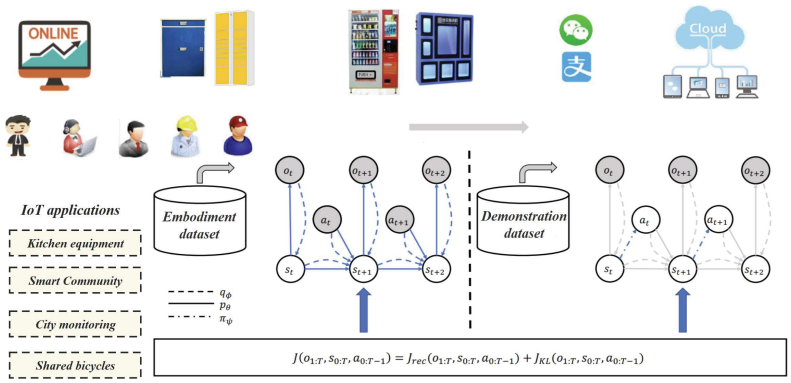

Figure 2 Internet of Things device architecture.

huge device scale, diversified device types, real-time data flow, etc. Therefore, how to integrate the traditional access control method with the IIoT has become an urgent problem to be solved. But at the same time, it also provides a broad space for the development of innovative security solutions. In the integration of the IIoT and access control, the ZTM, as an emerging network security concept, is increasingly attracting attention. ZTM is based on any component in the network. This new trust mechanism provides a more flexible and intelligent access control mode for the industrial IoT environment.

4 Design and Implementation of Secure Access Control Technology for IIoT Based on ZTM Model

4.1 Application Analysis of ZTM Model in IIoT

In the context of the IIoT, the challenges of network security have become particularly complex, so adopting advanced security models is particularly important [28, 29]. As an advanced network security concept, the ZTM shows its unique applicability in the IIoT.

When considering the applicability of ZTM in the IIoT, you can focus on the behaviour of devices in the IIoT network and calculate their trust score, as shown in Equation (4).

$$Trust\ Score_{Device} = \sum_{k=1}^{p} (Behavior_k \times Weight_k) \tag{4}$$

The complexity of the industrial IoT requires a highly cautious attitude towards each component in the network. The core concept of ZTM is to "do not trust any components", which fits with the characteristics of the large, heterogeneous device network in the IIoT. By implementing strict authentication and authorization in the network, the ZTM model helps to ensure that every device, user, or application is validated, reducing the potential threat of network intrusion. The real-time validation and authorization mechanism of the ZTM model is consistent with the requirement of the real-time data. In an industrial production environment, the timely response to potential threats is crucial. By emphasizing the requirements of real-time performance, ZTM ensures that all components in the network are constantly being verified and authorized, thus effectively guarding against real-time network attacks.

The abnormal detection score is shown in formula (5):

$$ADS = \frac{Number\ of\ Anomalous\ Events}{Total\ Events} \times 100\% \tag{5}$$

The abnormal detection score (ADS) represents the percentage of events that deviate from the expected behaviour and facilitates abnormality detection within the system.

$$REAC = -\sum_{i=1}^{n} P_i \times \log_2(P_i) \tag{6}$$

The resource entropy of access control is shown in formula (6), where P_i represents the proportion of access events related to the resource, and n is the total number of resources. REAC calculates the resource distribution entropy of access control, providing a measure of the diversity and dispersion of resource access.

$$SCS = \frac{Number\ of\ Security\text{-}Compliant\ Events}{Total\ Compliance\ Checks} \times 100\% \tag{7}$$

The security compliance score is shown in formula (7), and the security compliance score SCS reflects the percentage of events that comply with predefined security policies, providing a measure of the overall security status of the system.

$$TI = \alpha \times TS + \beta \times (1 - PE) \tag{8}$$

The reliability index is shown in formula (8), where the reliability index *TI* combines the reliability score *TS* and the available equipment ratio *PE*,

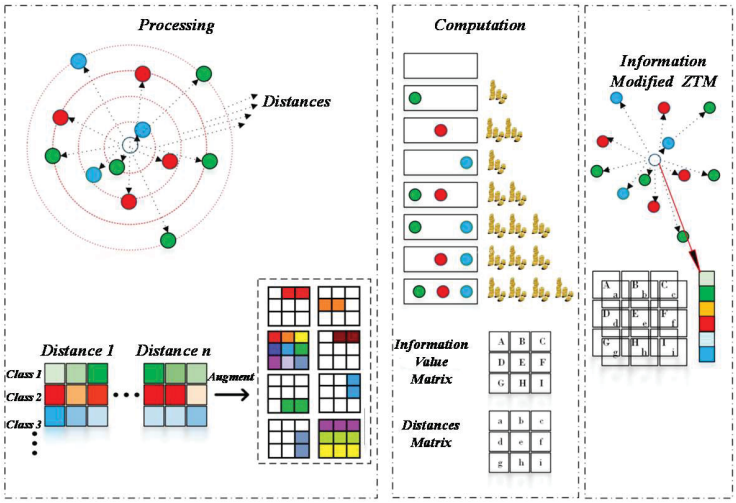

Figure 3 Modified ZTM framework.

where α and β are weight coefficients. This formula aims to evaluate the overall credibility of the system by considering device reliability and potential vulnerabilities.

Figure 3 shows the Modified ZTM framework. The policy-based dynamic access control of the Modified ZTM framework makes it more adaptable to the changing features of devices and users in the industrial IoT. With the continuous update and replacement of equipment in industrial production, the traditional static access control is difficult to adapt to this change. By dynamically adjusting the access policy, we ensure that the changes in devices and users do not affect the security of the overall network.

4.2 Design of Secure Access Control Framework

In the IIoT environment based on the ZTM model, it is crucial to ensure the design and implementation of secure access control technology. This framework aims to leverage the concept of ZTM model to achieve comprehensive, dynamic and sustainable secure access management [30]. The core design point of the framework is to build a powerful and flexible authentication system, covering multi-factor authentication, including biometrics, smart cards, etc. Based on the ZTM trust level of users and devices, fine authorization mechanisms are implemented to ensure that each entity can only access resources within its reasonable range. Flexible dynamic access

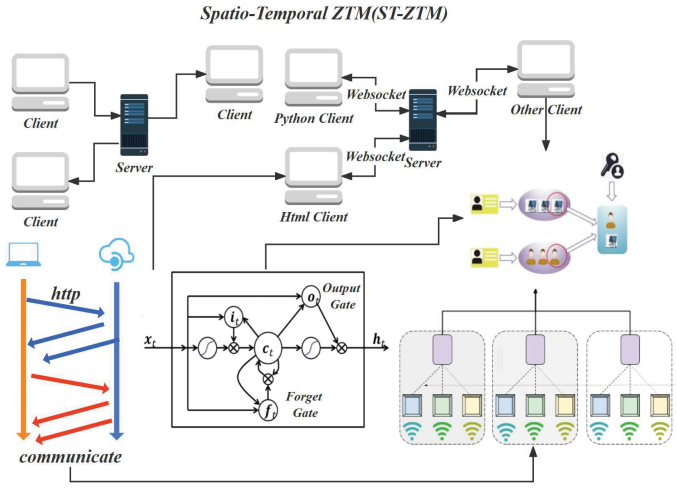

Figure 4 ST-ZTM framework.

control strategy is designed, relying on the real-time perception mechanism of ZTM model, enabling the system to intelligently adjust the access rights according to the real-time status, network topology and environment changes of devices and users. This helps to adapt to the complex industrial IoT environment.

Figure 4 shows the ST-ZTM framework, ST-ZTM implements the real-time audit and monitoring system. The audit log should include details such as timestamp, visitor identity, access resources, etc. In addition, real-time monitoring mechanisms are introduced to enable the system to respond to potential security threats in a timely manner. Introduce intelligent abnormal detection and response mechanism, through machine learning and other technologies, establish a benchmark of normal behaviour, and timely detect and respond to abnormal activities. When the system detects abnormalities, automatic or manual response measures can be taken to ensure that the security of the system is not threatened. In order to ensure the confidentiality and integrity of the data during transmission, ST-ZTM adopts a powerful encryption algorithm. Ensure that communication between devices is encrypted, and establish a secure tunnel to guard against middleman attacks and improve the credibility of data transmission. ST-ZTM regularly upgrades system components and fiknown vulnerabilities by designing secure update and maintenance mechanisms. Establish regular maintenance plans to ensure continuously improved system availability and safety.

4.3 Experimental Design and Result Analysis

To verify the design and implementation of the industrial IOT secure access control technology based on the ZTM model, this paper adopts a comprehensive experimental design. First, this paper constructs a real industrial IoT-based scenario, including devices, sensors, and control nodes, to simulate a typical industrial production environment. Next, in this paper, the secure access control technology based on the ZTM model is deployed to the system to ensure that the system can adjust the access rights according to the real-time situation.

For the secure access control technology based on ZTM model, consider the following formulas concerning the concepts of access control, security and trust:

$$ZTS = \frac{Number\ of\ Security\ Incidents}{Total\ Access\ Events} \times 100\% \tag{9}$$

The formula for zero trust is shown in formula (9), where ZTS represents the zero trust score.

$$CRA = \alpha \times AC + \beta \times (1 - T) \tag{10}$$

The comprehensive risk assessment formula is shown in formula (10), where *CRA* represents the comprehensive risk assessment value, *AC* is the access control score, and T is the trust score. α and β are weight coefficients used to adjust the relative importance of access control and trust in comprehensive risk assessment.

$$AC = \frac{Number\ of\ Compliant\ Access\ Events}{Total\ Access\ Events} \times 100\% \tag{11}$$

The access control score formula is shown in formula (11), and the access control score *AC* represents the percentage of access through the compliance path.

$$T = \frac{Number\ of\ Trusted\ Devices}{Total\ Number\ of\ Devices} \times 100\% \tag{12}$$

The trust score formula is shown in formula (12), and the trust score *T* represents the proportion of trusted devices in the system. During the experiment, this paper conducts attack simulation, simulating various network attacks, such as denial-of-service attacks and middle-man attacks, to evaluate the resistance of the system in the face of malicious behavior. The results show that the system shows strong anti-attack performance, successfully

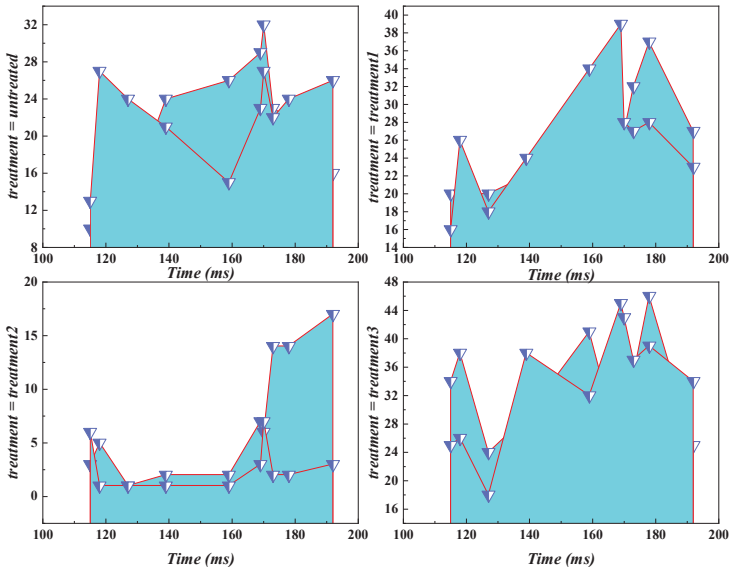

Figure 5 ZTM framework and other methods.

prevents a variety of network attacks, and ensures the stability and security of the IIoT system.

Figure 5 provides a visual representation of the comparative analysis between the ZTM framework and alternative methods. In this study, performance monitoring tools were used to dynamically observe and evaluate the real-time operating parameters of the system. The results showed that the response time was only 1.1 seconds and the system resource utilization rate was as high as 98.23%, indicating the overall efficiency and effectiveness of the access control technology based on the ZTM model. The ZTM model effectively manages access control while maintaining optimal system responsiveness and data transfer rates. Meanwhile, monitoring the utilization of system resources ensures that ZTM based methods achieve these security goals without burdening the underlying infrastructure.

Figure 6 provides a granular view of the ZTM framework at each stage, offering detailed insights into its performance and functionality. Notably, the audit of access logs emerges as a key feature, demonstrating the system's capability to comprehensively record user and device access activities. This logging mechanism serves as a robust foundation for conducting post-hoc security analyses, enabling a thorough examination of historical access events. By recording and archiving access activities, the system establishes

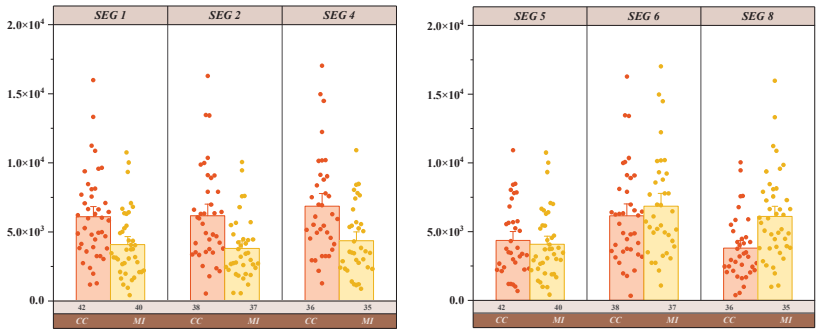

Figure 6 Data diagram of each stage of ZTM framework.

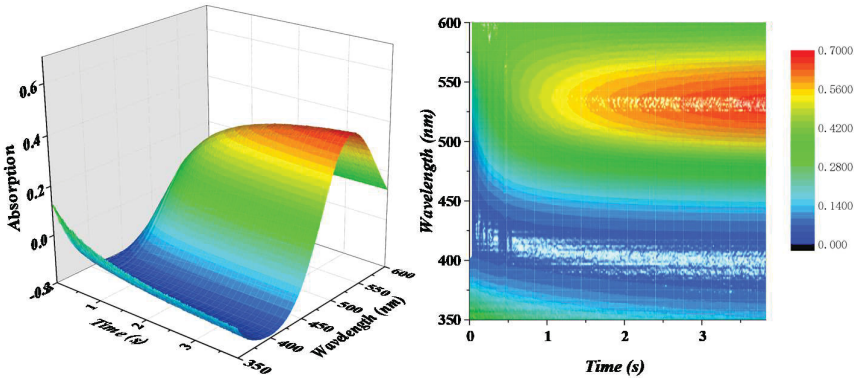

Figure 7 Experimental visualization results of ZTM framework.

a comprehensive audit trail, empowering administrators and security personnel to conduct in-depth investigations into any potential security incidents. This level of visibility is crucial for identifying and responding to security breaches, as well as for implementing proactive measures to enhance the overall security posture of the IIoT ecosystem. The accessibility of detailed access log data not only facilitates post-hoc security analysis but also contributes to compliance requirements and regulatory standards. The ability to demonstrate a meticulous record of access events aligns with best practices in cybersecurity and provides a tangible means of ensuring adherence to industry-specific regulations. The real-world environment in which these experiments were conducted adds credibility to the findings, emphasizing the adaptability and effectiveness of the ZTM framework in addressing the unique challenges posed by industrial IoT scenarios.

In Figure 7, the experimental visualization results underscore the outstanding performance of the ZTM framework. The design of the ZTM framework emerges as a pivotal factor in delivering a robust and efficient secure access management solution for IIoT systems. These results not only validate the effectiveness of the ZTM framework but also highlight its significant contributions to enhancing both the security and performance aspects of the system. The comprehensive nature of the framework's design becomes evident as it successfully manages and mitigates potential security threats, ensuring the integrity and confidentiality of sensitive data within the IIoT system. The efficiency demonstrated by the ZTM framework in the experimental results is indicative of its ability to facilitate seamless and secure communication within the IIoT ecosystem. This efficiency is particularly crucial for maintaining optimal performance levels, a factor that is paramount in industrial settings where real-time responsiveness and reliability are of utmost importance.

5 Conclusions

Based on the ZTM model, a secure access control technology has been designed and implemented. By constructing practical IIoT scenarios, this article successfully introduces the ZTM model into access control systems, achieving context based intelligent access management. In the experiment, its resistance to attacks, real-time performance, and auditing ability were verified. This article demonstrates the robustness of the system in responding to various network attacks. By simulating common attacks such as denial of service attacks and man in the middle attacks, the system demonstrates strong resistance and effectively ensures the stable operation of the IIoT system. The access control technology based on the ZTM model has certain advantages in real-time performance. The system can adjust access permissions based on real-time contextual information, ensuring sensitivity to dynamic environmental changes and providing users with more intelligent and flexible access control services. By monitoring performance parameters and recording audit logs, it is proven that the system will not have a significant impact on system performance while ensuring security. The system can efficiently handle large-scale access requests and provide complete audit records, providing strong support for system management and maintenance.

The design and implementation of IIoT security access control technology based on the ZTM model have achieved significant results in practical applications. This technology provides a comprehensive and efficient security

management tool for IIoT systems, significantly improving the reliability, intelligence, and maintainability of the system. The optimized security access control technology improves security performance by 28%, with a low detection rate of 3.2%. Future research directions can further optimize algorithm performance, expand the application scope of the system, and better meet the security needs of the IIoT field.

References

[1] Qiu, R., Zhang, J. F., Chen, L., Li, W., and Lin, N. (2022). Internet of things terminal access security based on zero trust. 2022 6th International Symposium on Computer Science and Intelligent Control (ISCSIC), 7–11.

[2] Chen, Z., Yan, L., Zitong Lü, Zhang, Y., Guo, Y., and Liu, W., et al. (2021). Research on zero-trust security protection technology of power iot based on blockchain. Journal of Physics: Conference Series, 1769(1), 012039 (8pp).

[3] Song, L., Ju, X., Zhu, Z., and Li, M. (2021). An access control model for the internet of things based on zero-knowledge token and blockchain. EURASIP Journal on Wireless Communications and Networking, 2021(1), 1–20.

[4] Yang, D. (2021). Research on traffic detection method of secure transmission industrial internet of things based on computer vision. Scientific programming (Pt.13), 2021.

[5] Yanli, W. (2018). Research on smart home security access control technology based on internet of things and cloud computing. Video Engineering.

[6] Zheng, F., and Zheng, B. (2021). Research on the optimization and application of intelligent data acquisition and alarm system based on internet of things. Journal of Physics: Conference Series, 1992(2), 022083–.

[7] Zhang, J., Liu, Y., and Zhang, Z. (2019). Research on Cross-Chain Technology Architecture System Based on Blockchain. International Conference on Communications, Signal Processing, and Systems.

[8] Mitani, S., Singh, T., Ghate, N., and Ueda, H. (2021). Attribute-based low-complexity network access control policy with optimal grouping algorithm. IEICE Communications Express, 10(11), 846–851.

[9] Chandramouli, R. (2023). A zero trust architecture model for access control in cloud native applications in multi-cloud environments.

[10] Kumar, N., Kasbekar, G. S., and Manjunath, D. (2022). Application of data collected by endpoint detection and response systems for implementation of a network security system based on zero trust principles and the eigentrust algorithm.
[11] Zhang, J., Zheng, J., Zhang, Z., Chen, T., Qiu, K., and Zhang, Q., et al. (2022). Hybrid isolation model for device application sandboxing deployment in zero trust architecture. International journal of intelligent systems.
[12] Ahmed, I., Nahar, T., Urmi, S. S., and Taher, K. A. (2020). Protection of Sensitive Data in Zero Trust Model. ICCA 2020: International Conference on Computing Advancements.
[13] Jiang, C., Xu, H., Huang, C., and Huang, Q. (2022). An adaptive information security system for 5g-enabled smart grid based on artificial neural network and case-based learning algorithms. Frontiers in computational neuroscience, 16, 872978.
[14] Ferretti, L., Magnanini, F., Andreolini, M., and Colajanni, M. (2021). Survivable zero trust for cloud computing environments. Computers & Security, 110, 102419.
[15] Collier, Z. A., and Sarkis, J. (2021). The zero trust supply chain: managing supply chain risk in the absence of trust. International Journal of Production Research(1), 1-16.
[16] Pularikkal, G. B., Patil, S. R., Brinckman, B., and Nanjanagud, M. (2020). Machine learning-based application posture for zero trust networking.
[17] Cheng, Y., Meng, H., Yuan, L., and Lei, Y. (2021). Research on edge computing technology of Internet of Things based on intelligent and environmental protection. 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE). IEEE.
[18] Chen, G., Zhang, X., Wang, C., and Hao, S. (2021). Research on flexible control strategy of controllable large industrial loads based on multi-source data fusion of internet of things. IEEE Access.
[19] Yue, J. (2020). Research on the development trend of industrial automation control technology based on big data analysis. Journal of Physics: Conference Series, 1648, 022116–.
[20] Di, C., Li, M., and Zhao, Z. (2020). Research on Interconnection and Mutual Control Technology of Power Transmission and Transformation Equipment Based on Internet of Things. International Conference on Dependable Systems and Their Applications. IEEE.

[21] Lin, B. (2021). Research on data release and location monitoring technology of sensor network based on internet of things. Journal of web engineering(3), 20.

[22] Zhang, P., Tian, C., Shang, T., Liu, L., Li, L., and Wang, W., et al. (2021). Dynamic access control technology based on zero-trust light verification network model. International Conference on Communications, Information System and Computer Engineering. IEEE.

[23] Shi, C., Fei, J., Zhang, X., Yao, Q., and Fan, J. (2020). Continuous trust evaluation of power equipment and users based on risk measurement. Scientific Programming.

[24] Chen, L., Dai, Z., Chen, M., and Li, N. (2021). Research on the security protection framework of power mobile internet services based on zero trust.

[25] Tao, Y., Lei, Z., and Ruxiang, P. (2018). Fine-Grained Big Data Security Method Based on Zero Trust Model. 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). IEEE.

[26] Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., and Lyu, M., et al. (2021). A security awareness and protection system for 5g smart healthcare based on zero-trust architecture. IEEE internet of things journal (8–13).

[27] Xiaojian, Z., Liandong, C., Jie, F., Xiangqun, W., and Qi, W. (2021). Power IoT security protection architecture based on zero trust framework. 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP). IEEE.

[28] Jian-Wei, L., Feng, G., Xiong-Lin, L., and Automation, D. O. (2019). Survey of deep reinforcement learning based on value function and policy gradient. Chinese Journal of Computers.

[29] Wang, W., Chen, X., Gan, W., Yang, Y., Zhang, W., and Zhang, X., et al. (2022). Research on Network Security Situation Assessment Model Based on Double AHP. International Conference on Artificial Intelligence and Security. Springer, Cham.

[30] Surantha, N., and Ivan, F. (2019). Secure Kubernetes Networking Design Based on Zero Trust Model: A Case Study of Financial Service Enterprise in Indonesia. International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Springer, Cham.

Biography

Yanliu Nie was born in Jiaozuo, Henan in 1987, obtained a master's degree from Chongqing University of Posts and Telecommunications. Currently, she works at the School of Information Engineering and Big Data at Zhengzhou Technical College, with main research directions in computer networks, network security, system development, etc.