Zero-Trust Access Control Architecture for Secure Industrial Internet of Things Networks

Ravi Krishnan

Singapore

Abstract

This study proposes a Zero-Trust access control architecture for securing Industrial Internet of Things (IIoT) networks against unauthorized access, cyberattacks, and lateral threat propagation. The proposed framework integrates continuous identity verification, device authentication, context-aware authorization, and network microsegmentation to protect interconnected industrial devices and communication infrastructures. A risk-adaptive access control mechanism evaluates device integrity, user privileges, network behavior, and operational context before granting access to critical industrial resources. Attribute-Based Access Control and lightweight cryptographic authentication are incorporated to support granular security enforcement across resource-constrained IIoT environments. The architecture employs continuous monitoring and dynamic policy updates to identify suspicious activities and restrict compromised devices without disrupting essential industrial operations. Performance evaluation considers authentication latency, access decision accuracy, computational overhead, network scalability, and resilience against simulated security threats. The proposed approach establishes a systematic foundation for secure industrial connectivity, improved cyber resilience, and reliable access management in Industry 4.0 environments.

Keywords: Zero-Trust Architecture; Industrial Internet of Things; Access Control; Device Authentication; Cybersecurity.

1. Introduction

Enterprise applications depend on reliable diagnostics to detect runtime errors, failed workflows, API issues, slow transactions, and integration faults [1]. Logs are the main evidence source for understanding what happened before, during, and after an incident. Effective application diagnostics require structured logging, traceability, contextual metadata, error classification, and operational visibility [2]. However, fixed logging strategies often create two problems. Low-detail logs may miss important causes, while high-detail logs may generate excessive storage cost and alert noise [3].

The main challenge is that diagnostic needs change during runtime. A normal transaction may require only basic logs, but a failing workflow, repeated exception, or security-sensitive event may need deeper traces [4]. Adaptive logging improves this process by changing log depth according to system condition, transaction risk, and error behavior [5]. AI-assisted monitoring can identify when additional diagnostic detail is needed and when logging can return to normal levels. This article proposes an adaptive logging framework for enterprise application diagnostics.

2. Methodology

The proposed framework captures log metadata from application servers, API gateways, databases, background jobs, authentication modules, and integration services [6]. It records event type, severity, timestamp, user role, transaction ID, request path, error frequency, response time, affected component, and workflow state. These features are converted into diagnostic context profiles. Adaptive logging requires context because the same event may be low-risk in one workflow but critical in another [7].

The logging controller classifies runtime states as normal, warning, error-prone, performance-risk, security-sensitive, workflow-critical, or incident-active [8]. Based on this classification, it adjusts log level, trace depth, parameter capture, correlation ID tracking, and diagnostic enrichment. Lightweight scoring and policy rules are used so logging decisions remain fast and explainable. Sensitive fields are masked before storage [9], and transaction-critical events are linked with workflow and database identifiers for easier diagnosis.

The framework is evaluated using simulated enterprise applications involving APIs, database workflows, authentication events, scheduled jobs, and service integrations. Static logging is compared with adaptive logging under repeated exceptions, slow requests, failed jobs, API timeout, suspicious login, and workflow interruption scenarios [10]. Evaluation metrics include diagnosis time, log volume reduction, root-cause evidence quality, missed-event rate, storage overhead, alert usefulness, and administrator acceptance rate. Feedback from resolved incidents, ignored logs, and administrator notes is used to refine logging policies over time.

3. Results and Discussion

The results show that adaptive logging improves diagnostics by capturing richer evidence only when runtime risk increases. In the baseline condition, static logs either lack enough detail or produce large volumes of low-value records. With the proposed framework, detailed traces are activated for high-risk events and reduced during normal execution. The strongest improvement appears in intermittent failures, where deeper logs are needed only around the failure window.

The discussion shows that adaptive logging must balance diagnostic depth with privacy and storage cost. Excessive logging can expose sensitive data or overload monitoring systems, while weak logging may hide failure causes. The main limitation is that log-level decisions depend on accurate runtime classification. Regular policy review and masking controls are necessary for safe long-term use.

4. Conclusion

This article presented an adaptive logging framework for enterprise application diagnostics. The framework adjusts log detail using runtime context, risk scoring, workflow state, and error behavior. It improves troubleshooting by increasing diagnostic evidence during abnormal conditions while reducing unnecessary log noise during normal operation. The study shows that adaptive logging can strengthen enterprise diagnostics when combined with structured metadata, privacy controls, and continuous incident feedback.

References

1. Federici, F., Martintoni, D., & Senni, V. (2023). A zero-trust architecture for remote access in industrial IoT infrastructures. *Electronics*, *12*(3), 566.
2. Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, *156*, 103414.
3. Gondi, S. R. (2023). AI-Assisted Fault Localization in Semiconductor Wafer Testing and Manufacturing Operations. Perception, Navigation and Intelligent Devices, 10, 1-8.
4. Ameer, S., Praharaj, L., Sandhu, R., Bhatt, S., & Gupta, M. (2024). Zta-iot: A novel architecture for zero-trust in iot systems and an ensuing usage control model. *ACM Transactions on Privacy and Security*, *27*(3), 1-36.
5. Abuhasel, K. A. (2023). A zero-trust network-based access control scheme for sustainable and resilient industry 5.0. *IEEE Access*, *11*, 116398-116409.
6. Nie, Y. (2024). Analysis and research on secure access control technology of industrial internet of things based on ztm model. *Journal of Cyber Security and Mobility*, *13*(4), 585-604.
7. Ferretti, L., Longo, F., Merlino, G., Colajanni, M., Puliafito, A., & Tapas, N. (2021). Verifiable and auditable authorizations for smart industries and industrial Internet-of-Things. *Journal of Information Security and Applications*, *59*, 102848.
8. Wang, B., Peng, J., & Cui, M. (2024). Secure access technology for industrial internet of things. *Concurrency and Computation: Practice and Experience*, *36*(25), e8231.
9. rao Gondi, S. (2025). Multi-Modal AI-Driven Electrical and Optical Characterization Framework for Sub-5 nm Semiconductor Defect Localization. Research Briefs on Information and Communication Technology Evolution, 11, 188-198.

10. Son, S., Kwon, D., Lee, S., Kwon, H., & Park, Y. (2024). A zero-trust authentication scheme with access control for 6g-enabled iot environments. *IEEE Access*, *12*, 154066-154079.