Secure Data Transmission Framework for Distributed Semiconductor Process Monitoring

Takeshi Yamamoto

Japan

Abstract

This study proposes a secure data transmission framework for distributed semiconductor process monitoring systems, focusing on protecting manufacturing information while maintaining communication reliability and operational efficiency. The proposed architecture integrates lightweight encryption, mutual authentication, and secure communication protocols to safeguard sensor measurements, equipment status information, and process metrology data exchanged across interconnected fabrication facilities. A distributed edge-cloud communication model is developed to support real-time data acquisition, secure transmission, and centralized process analysis. Cryptographic key management and role-based access control mechanisms are incorporated to prevent unauthorized access, data manipulation, and communication interception. The framework employs integrity verification and adaptive security policies to maintain data confidentiality and authenticity under varying network conditions. Performance evaluation considers encryption overhead, transmission latency, packet delivery reliability, computational resource utilization, and resistance to simulated cyberattacks. The proposed approach supports trustworthy semiconductor process monitoring, secure industrial connectivity, and reliable information exchange in advanced manufacturing environments.

Keywords: Secure Data Transmission; Semiconductor Process Monitoring; Industrial Cybersecurity; Edge-Cloud Computing; Data Encryption.

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. Ma, R., Zhang, L., Wu, Q., Mu, Y., & Rezaeibagha, F. (2023). Be-trdss: Blockchain-enabled secure and efficient traceable-revocable data-sharing scheme in industrial internet of things. *IEEE transactions on industrial informatics*, *19*(11), 10821-10830.
2. Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2022). A secure and trusted mechanism for industrial IoT network using blockchain. *IEEE Transactions on Industrial Informatics*, *19*(2), 1894-1902.
3. rao Gondi, S. (2023). Data-Driven Process Analytics for Early Defect Detection in High-Volume Semiconductor Fabrication. Cross-Disciplinary Knowledge Systems, 10, 37-42.
4. Nie, Z., Long, Y., Zhang, S., & Lu, Y. (2022). A controllable privacy data transmission mechanism for internet of things system based on blockchain. *International Journal of Distributed Sensor Networks*, *18*(3), 15501329221088450.
5. Bojič Burgos, J., & Pustišek, M. (2024). Decentralized IoT data authentication with signature aggregation. *Sensors*, *24*(3), 1037.
6. Hewa, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2022). Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing. *IEEE transactions on industrial informatics*, *18*(10), 7174-7185.
7. Shahjalal, M., Islam, M. M., Alam, M. M., & Jang, Y. M. (2022). Implementation of a secure LoRaWAN system for industrial internet of things integrated with IPFS and blockchain. *IEEE Systems Journal*, *16*(4), 5455-5464.

8. Shang, S., Li, X., Gu, K., Li, L., Zhang, X., & Pandi, V. (2023). A robust privacy-preserving data aggregation scheme for edge-supported IIoT. *IEEE Transactions on Industrial Informatics*, *20*(3), 4305-4316.
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. Huang, K., Wang, Q., Chen, Z., Yang, C., & Gui, W. (2025). Secure cloud-edge collaborative method for dynamic industrial process monitoring using self-updating dictionary learning. *IEEE Transactions on Automation Science and Engineering*, *22*, 14170-14182.