Machine Learning-Based Intrusion Detection for Cloud-Connected Electronic Manufacturing Systems

Jonathan Reed

United States

Abstract

This study proposes a machine learning-based intrusion detection framework for cloud-connected electronic manufacturing systems, focusing on improving cybersecurity, network reliability, and operational resilience. The proposed methodology integrates network traffic monitoring, industrial communication logs, and cloud access records to identify malicious activities affecting interconnected manufacturing environments. Advanced data preprocessing and feature selection techniques are employed to extract relevant traffic characteristics, including packet frequency, connection duration, protocol behavior, and abnormal access patterns. Supervised learning algorithms, including Random Forest, Support Vector Machines, and Gradient Boosting, are investigated for detecting and classifying network intrusions. An adaptive anomaly detection mechanism is incorporated to identify previously unseen attack patterns and reduce dependence on predefined threat signatures. Performance evaluation considers detection accuracy, precision, recall, F1-score, false positive rate, and computational latency. The proposed framework supports early cyberattack identification, secure cloud integration, and reliable industrial operations through intelligent threat monitoring and automated security decision support.

Keywords: Intrusion Detection; Machine Learning; Cloud-Connected Manufacturing; Industrial Cybersecurity; Network Anomaly Detection.

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, 5]. Adaptive logging improves this process by changing log depth according to system condition, transaction risk, and error behavior [6]. 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 [7]. 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 [8, 9].

The logging controller classifies runtime states as normal, warning, error-prone, performance-risk, security-sensitive, workflow-critical, or incident-active [10]. 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 [11], 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 [12]. 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. rao Gondi, S. (2021). Big Data Analytics Framework for Process Optimization and Yield Improvement in Semiconductor Production. Journal of Privacy-Aware Computing Systems, 8, 52-57.
2. Friha, O., Ferrag, M. A., Benbouzid, M., Berghout, T., Kantarci, B., & Choo, K. K. R. (2023). 2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT. *Computers & Security*, *127*, 103097.
3. Ponniah, K. K., & Retnaswamy, B. (2023). A novel deep learning based intrusion detection system for the IoT-Cloud platform with blockchain and data encryption mechanisms. *Journal of Intelligent & Fuzzy Systems*, *45*(6), 11707-11724.
4. Ruiz-Villafranca, S., Roldán-Gómez, J., Gómez, J. M. C., Carrillo-Mondéjar, J., & Martinez, J. L. (2024). A TabPFN-based intrusion detection system for the industrial internet of things: S. Ruiz-Villafranca et al. *The Journal of Supercomputing*, *80*(14), 20080-20117.
5. Gondi, S. R. (2025). Manufacturing Variation Modeling and Yield Optimization in Sub-5 nm Semiconductor Technologies. Journal of Privacy-Aware Computing Systems, 12, 1-8.
6. Hassini, K., Khalis, S., Habibi, O., Chemmakha, M., & Lazaar, M. (2024). An end-to-end learning approach for enhancing intrusion detection in Industrial-Internet of Things. *Knowledge-Based Systems*, *294*, 111785.
7. Nandanwar, H., & Katarya, R. (2024). Deep learning enabled intrusion detection system for Industrial IOT environment. *Expert Systems with Applications*, *249*, 123808.

8. Sinha, R., Thakur, P., Gupta, S., & Shukla, A. (2024). Development of lightweight intrusion model in Industrial Internet of Things using deep learning technique. *Discover Applied Sciences*, *6*(7), 346.
9. Chaurasia, N., Ram, M., Verma, P., Mehta, N., & Bharot, N. (2024). A federated learning approach to network intrusion detection using residual networks in industrial IoT networks: N. Chaurasia et al. The Journal of Supercomputing, 80(13), 18325-18346.
10. Anwer, R. W., Abrar, M., Ullah, M., Salam, A., & Ullah, F. (2025). Advanced intrusion detection in the industrial Internet of Things using federated learning and LSTM models. *Ad Hoc Networks*, 103991.
11. Ahmad, J., Latif, S., Khan, I. U., Alshehri, M. S., Khan, M. S., Alasbali, N., & Jiang, W. (2025). An interpretable deep learning framework for intrusion detection in industrial Internet of Things. *Internet of Things*, *33*, 101681.
12. Gondi, S. R. (2024). Data-Centric Yield Engineering Frameworks for Next-Generation Semiconductor Production Systems. Transactions on Smart Electrical and Computational Systems, 11, 37-44.