Adaptive Authentication and Access Management in Cloud-Based Industrial Control Platforms

Elena García

Spain

Abstract

This study proposes an adaptive authentication and access management framework for cloud-based industrial control platforms, focusing on strengthening cybersecurity while maintaining operational efficiency and system availability. The proposed architecture integrates risk-based authentication, continuous identity verification, and context-aware access control to protect industrial applications, connected devices, and sensitive operational data. A dynamic risk assessment model evaluates user behavior, device integrity, access location, authentication history, and network conditions to determine appropriate security requirements. Attribute-Based Access Control and multifactor authentication are incorporated to enforce granular authorization policies and prevent unauthorized system access. Machine learning-based anomaly detection supports identification of suspicious authentication activities and adaptive responses to emerging security threats. The framework considers industrial communication constraints and time-sensitive control operations to minimize authentication delays and computational overhead. Performance evaluation examines authentication accuracy, access latency, false rejection rates, scalability, and resistance to simulated attacks, supporting secure and reliable industrial cloud operations.

Keywords: Adaptive Authentication; Cloud-Based Industrial Control; Access Management; Risk-Based Security; Industrial 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. 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. Gupta, B. B., & Quamara, M. (2020). Attribute-based access control and authentication mechanism using smart cards for cloud-based IoT applications. *International Journal of Embedded Systems*, *13*(1), 40-49.
3. Wang, J., Wang, H., & Zhang, H. (2020). A trust and attribute-based access control framework in internet of things. *International Journal of Embedded Systems*, *12*(1), 116-124.
4. rao Gondi, S. (2019). Predictive Modeling of Wafer Acceptance Test Parameters for Semiconductor Yield Enhancement. Emerging Digital Systems, 6, 33-38.
5. Sifou, F., AlShahwan, F., Hammoud, A., Marwan, M., & Hammouch, A. (2020). Implementing Policy Rules in Attributes Based Access Control with XACML within Cloud-Enabled IoT Environment. *J. Commun.*, *15*(1), 107-112.
6. Cui, H., Deng, R. H., Liu, J. K., Yi, X., & Li, Y. (2018). Server-aided attribute-based signature with revocation for resource-constrained industrial-internet-of-things devices. *IEEE Transactions on Industrial Informatics*, *14*(8), 3724-3732.
7. Bernieri, G., Cecconello, S., Conti, M., & Lain, G. (2020). TAMBUS: A novel authentication method through covert channels for securing industrial networks. *Computer Networks*, *183*, 107583.

8. rao Gondi, S. (2020). Intelligent Fault Detection and Classification in Semiconductor Manufacturing Using Statistical Learning Techniques. Transactions on Smart Electrical and Computational Systems, 7, 26-31.
9. Lupascu, C., Lupascu, A., & Bica, I. (2020). DLT based authentication framework for industrial IoT devices. *Sensors*, *20*(9), 2621.
10. Veloudis, S., Paraskakis, I., Petsos, C., Verginadis, Y., Patiniotakis, I., Gouvas, P., & Mentzas, G. (2019). Achieving security-by-design through ontology-driven attribute-based access control in cloud environments. *Future Generation Computer Systems*, *93*, 373-391.