

CARDIOLOGY SOFTWARE SYSTEMS FOR ECG ANALYSIS, HEART RISK PREDICTION, AND CONTINUOUS PATIENT MONITORING

Valentina Romano
Italy

ABSTRACT

Cardiology software systems support ECG analysis, heart risk prediction, and continuous patient monitoring through integrated digital tools. The system can analyze heart rhythm, detect abnormal patterns, and identify possible signs of arrhythmia, ischemia, or other cardiac conditions. Predictive models use clinical history, vital signs, laboratory results, and lifestyle factors to estimate future cardiovascular risk. Data from wearable devices and bedside monitors can be transmitted in real time for medical review. Automated alerts help clinicians respond quickly to abnormal heart rate, blood pressure, oxygen levels, or ECG changes. Integration with electronic medical records improves care coordination and follow-up planning. Overall, cardiology software can support earlier diagnosis, continuous monitoring, timely intervention, and more accurate management of patients with heart-related conditions.

keywords: Cardiology Software; ECG Analysis; Heart Risk Prediction; Continuous Patient Monitoring; Cardiovascular Care.

1. Introduction

Enterprise applications depend on reliable diagnostics to detect runtime errors, failed workflows, API issues, slow transactions, and integration faults. Logs are the main evidence source for understanding what happened before, during, and after an incident [1]. 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.

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. Adaptive logging improves this process by changing log depth according to system condition, transaction risk, and error behavior [3]. AI-assisted monitoring can identify when additional diagnostic detail is needed and when logging can return to normal levels [4]. 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. 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 [5].

The logging controller classifies runtime states as normal, warning, error-prone, performance-risk, security-sensitive, workflow-critical, or incident-active. 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 [6]. Sensitive fields are masked before storage [7], 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 [8]. 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. Kavuluri, H. V. R. (2021). Text Classification of Software Requirement Documents with TFIDF Models. *Emerging Digital Systems*, 8, 1-6.
2. Kavuluri, V. V. R., Bandla, S., Gorumutchu, M. R., Mandapatti, J. K., & Jagadhabhi, N. (2022). Execution Trace Forensics in Low-Code Platforms for Critical Workflows. *Journal of Grid, Machines and Drives*, 9, 1-8.
3. Kavuluri, H. V. R. (2020). Clustering Analysis of User Behavior in Web-Based Software Applications. *Cross-Disciplinary Knowledge Systems*, 7, 7-12.
4. Gorumutchu, M. R., Jagadhabhi, N., Mandapatti, J. K., Bandla, S., & Kavuluri, V. V. R. (2021). Concurrency Anomalies in AI-Mediated Transaction Routing Layers. *Journal of Grid, Machines and Drives*, 8, 20-26.
5. Kavuluri, H. V. R. (2019). Bug Severity Classification in Issue Tracking Systems with Support Vector Machines. *High-Performance Distributed Computing Review*, 6, 7-12.
6. Kavuluri, H. V. R. (2020). Feature Selection for Machine Learning Fault Prediction in Software Modules. *Journal of Privacy-Aware Computing Systems*, 7, 7-12.

7. Kavuluri, H. V. R., & Keshireddy, S. R. (2019). Migrating Sensitive Government Databases to AWS RDS: Security, Compliance, and Risk Mitigation. *Emerging Digital Systems*, 6, 26-32.
8. Keshireddy, S. R. (2019). Spreadsheet-Based Record Migration to Oracle APEX Database Applications. *Transactions on Smart Electrical and Computational Systems*, 6, 1-5.