HEALTHCARE CHATBOT SOFTWARE FOR PATIENT QUERY HANDLING, SYMPTOM SCREENING, AND APPOINTMENT ASSISTANCE

Julien Moreau
France

ABSTRACT

Healthcare chatbot software supports patient query handling, symptom screening, and appointment assistance through automated digital communication. The system can answer common questions about hospital services, doctor availability, medications, diagnostic tests, and treatment instructions. Symptom-screening tools collect basic health information, identify possible risk levels, and guide patients toward suitable medical support without replacing professional diagnosis. The chatbot can also schedule, reschedule, or cancel appointments and send reminders for consultations and follow-up visits. Integration with hospital systems improves access to patient records, service information, and appointment calendars. Multilingual support, data encryption, user authentication, and clear escalation to healthcare professionals strengthen accessibility and safety. Overall, healthcare chatbots can reduce administrative workload, improve response speed, support patient engagement, and provide convenient access to basic healthcare services.

keywords: Healthcare Chatbot Software; Patient Query Handling; Symptom Screening; Appointment Assistance; Digital Patient Engagement.

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 [9]. 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. Keshireddy, S. R. (2022). Low-Latency Data Lake Ingestion Using Adaptive Partitioning and Query-Aware Layouts. Cross-Disciplinary Knowledge Systems, 9, 8-14.
2. Kande, R., Kotla, C., & kanth Thottempudi, K. (2022). Zero Trust Architecture with MLDriven Behavioral Analytics for Healthcare ERP on Microsoft Azure. Journal of Grid, Machines and Drives, 9, 29-36.
3. Keshireddy, S. R. (2021). Role-Based Access Control in Oracle APEX with Database Authentication. Emerging Digital Systems, 8, 7-12.
4. Kotla, C., kanth Thottempudi, K., & Kande, R. (2022). Software Supply Chain Security for Infrastructure-as-Code Pipelines with Vulnerability Detection and Remediation. Perception, Navigation and Intelligent Devices, 9, 29-36.
5. Keshireddy, S. R. (2019). Oracle APEX Integration with RESTful Services for Lightweight Enterprise Data Exchange. Journal of Grid, Machines and Drives, 6, 7-12.

6. Bandla, S., Jagadhabi, N., Gorumutchu, M. R., Kavuluri, V. V. R., & Mandapatti, J. K. (2022). Temporal Drift Accumulation in Machine-Learned Database Index Mechanisms. High-Performance Distributed Computing Review, 9, 25-31.
7. Kavuluri, H. V. R. (2021). Automating Oracle Database Performance Tuning Through AIBased Workload Analysis. Journal of Privacy-Aware Computing Systems, 8, 35-51.
8. Jagadhabi, N., Mandapatti, J. K., Bandla, S., Gorumutchu, M. R., & Kavuluri, V. V. R. (2022). Semantic Degradation in Long-Lived Machine-Learned Data Pipelines. Transactions on Smart Electrical and Computational Systems, 9, 33-40.
9. Gorumutchu, M. R., Kavuluri, V. V. R., Jagadhabi, N., Bandla, S., & Mandapatti, J. K. (2022). Latency Determinism Breakdown in AI-Optimized Distributed Systems. Cross-Disciplinary Knowledge Systems, 9, 1-7.