OPEN ACCESS

Saudi Journal of Engineering and Technology

Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Operational Risk Indicators Derived from Customer Interaction Data in Digital Banking Platforms

Md Imran Hossain Bhuiyan[1*], Tahamina Akter[2], Sadia Afroje[3], Rasel Chokder[4]

[1]MS in Business Analytics, University- Trine University - Detroit, MI, US
[2]MS in management (Major business analytics), University- St. Francis College, Brooklyn, New York, United States
[3]Master's in Management Information Systems Lamar University, Beaumont, Texas, United States
[4]Master's in Management Information Systems Lamar University, Beaumont, Texas, United States

DOI: https://doi.org/10.36348/sjet.2026.v11i04.011 | **Received:** 13.02.2026 | **Accepted:** 07.04.2026 | **Published:** 11.04.2026

***Corresponding author:** Md Imran Hossain Bhuiyan
MS in Business Analytics, University- Trine University - Detroit, MI, US

Abstract

Digital banking platforms generate large volumes of operational information through transaction processing systems, system logs, and customer communication channels. Many studies examine transaction monitoring, fraud detection, and cybersecurity events. Customer interaction records receive less attention as a source of operational risk information. This study investigates the use of customer interaction data as indicators of operational conditions in digital banking platforms. The research examines interaction records collected from support tickets, complaint submissions, chat conversations, and service request logs. These records are analyzed together with Management Information System (MIS) event logs in order to identify recurring service issues and operational patterns. The proposed analytical framework organizes interaction data through several stages that include data collection, preprocessing, interaction pattern detection, and operational risk indicator generation. Repeated reports related to transaction delays, authentication failures, and application performance problems appear within the interaction dataset. These patterns correspond to operational events recorded in system activity logs. The study also introduces a quantitative operational risk score calculated from the frequency and severity of interaction categories. The results indicate that customer interaction datasets contain measurable signals related to operational disruptions within digital banking platforms. The analytical framework demonstrates that interaction records provide an additional information source for operational monitoring and risk analysis in digital financial services.

Keywords: Banking analytics, Complaint monitoring, financial risk indicators, Digital banking systems, Operational analytics.

I. INTRODUCTION

Digital banking platforms play a central role in the delivery of modern financial services. Customers conduct transactions, manage accounts, and communicate with financial institutions through mobile and web applications. These platforms operate through interconnected systems that include transaction processing engines, authentication services, application interfaces, and data management infrastructures. Continuous operation of these components is necessary for reliable banking services. Any disruption in these systems may affect financial transactions and customer service performance. Digital banking environments generate large volumes of operational data. Transaction records, authentication logs, and system activity reports provide detailed information about platform behavior. Financial institutions analyze these datasets in order to observe operational conditions and identify irregular system activity. Data-driven analytics integrated with Management Information Systems (MIS) supports financial reporting and operational monitoring across enterprise environments [1]. Secure data management architectures also support digital transformation within financial and IT systems that handle large volumes of operational information [2]. Research on financial analytics frequently examines operational data in order to evaluate financial performance and detect system anomalies. Machine learning models have been applied to financial datasets to estimate key performance indicators and operational metrics in enterprise environments [7]. Analytical systems also examine MIS event logs to identify irregular operational patterns and

internal control issues within financial organizations [3]. In addition, data governance frameworks address privacy protection and structured data management in digital enterprise environments [12]. These analytical approaches demonstrate how system records support monitoring of operational activity within financial systems. Modern digital banking platforms also rely on large-scale computing infrastructure and distributed service environments. Cloud-based financial platforms process financial transactions and service interactions across distributed networks [11]. Infrastructure monitoring tools and automated administration systems provide operational information regarding system performance, resource usage, and service activity within these environments [16,18]. Security monitoring systems examine system access activity and network behavior to identify abnormal operational conditions in digital service platforms [9,21]. These monitoring tools focus primarily on technical system activity recorded in infrastructure logs. Although these studies provide valuable insight into operational monitoring within financial systems, most research emphasizes transaction monitoring, infrastructure analytics, and cybersecurity observation. Analytical models frequently rely on transaction records, system logs, and network activity reports. These datasets describe system-level events within digital banking environments.

Digital banking platforms also generate extensive customer interaction records that describe user experiences during financial service activities. Customers communicate with financial institutions through support tickets, complaint submissions, chat conversations, and feedback channels. These communication records often contain descriptions of operational issues encountered during banking activities. Customers report transaction delays, login problems, service interruptions, and application errors through these interaction channels. Interaction datasets therefore contain information related to operational conditions experienced during financial service usage. Despite the availability of these records, customer interaction data receives limited attention in operational risk analysis for digital banking systems. Most monitoring frameworks rely primarily on system logs and infrastructure metrics. Interaction records provide direct descriptions of operational problems encountered during service usage. Examination of these records may therefore reveal operational conditions that influence both system performance and customer experience. This study presents an analytical framework that examines customer interaction records together with MIS event logs in order to derive operational risk indicators for digital banking platforms. The proposed framework analyzes recurring interaction patterns that correspond to service disruptions and operational irregularities. These patterns are translated into measurable indicators representing operational conditions such as transaction processing delays, authentication instability, and digital platform performance issues. The study also introduces an analytical workflow that integrates interaction datasets with system activity records for operational monitoring in digital financial services.

This study examines how customer interaction data can support operational risk monitoring in digital banking platforms. The research focuses on identifying recurring service issue patterns within customer interaction records such as support tickets, complaints, and chat conversations. It also integrates customer interaction data with MIS event logs to analyze operational conditions within digital banking systems. Another objective involves developing a framework that converts interaction patterns into measurable operational risk indicators representing issues such as transaction delays, authentication problems, and platform performance concerns. The study further presents an analytical workflow for interaction-based operational monitoring and evaluates the relationship between customer interaction patterns and operational disruptions within digital banking services.

II. Related Work

A. Financial Data Analytics and Digital Banking Risk Management

Research on financial information systems examines how analytical tools support risk monitoring in digital financial services. Data-driven financial analytics integrated with Management Information Systems (MIS) provide structured access to financial records and transaction datasets that support operational analysis [1]. Studies on digital finance infrastructures also address scalable storage and processing methods for financial data used in enterprise platforms [2]. Fraud detection and financial threat monitoring have received significant attention in recent work. Real-time analytics platforms apply machine learning models to detect suspicious transactions and abnormal behavioral patterns in financial systems [10]. Other research introduces financial risk management models that combine privacy-preserving analytics and federated learning to support collaborative data analysis among organizations while protecting sensitive information [6]. These studies show that financial analytics platforms and secure data environments support operational monitoring in digital financial systems.

B. MIS Event Logs and Enterprise Analytics for Operational Monitoring

Enterprise information systems record operational activities through MIS event logs, which provide structured records of system events and user interactions. Internal control models analyze these event logs to detect irregular operational patterns and compliance issues in organizational processes [3]. Service-oriented analytics frameworks also examine workforce data and operational records to evaluate service performance and organizational activity [4]. Machine learning models contribute to this area through predictive analytics for financial indicators and

operational performance metrics [7]. Enterprise dashboards and SQL-based data quality frameworks support analytics across multiple data sources and support consistent reporting within enterprise systems [8]. Together, these studies demonstrate how enterprise analytics platforms extract operational indicators from large volumes of system interaction data.

C. Cloud and Data Infrastructure for Digital Service Platforms

Digital financial services depend on distributed computing platforms that process large transaction datasets and user interaction records. Cloud-native fintech analytics platforms support transaction monitoring and digital service analytics across distributed financial networks [11]. Research on enterprise data governance also examines ethical AI policies and data management structures that guide the use of analytics in enterprise systems [12]. Conversational analytics platforms process user feedback and interaction data from digital service interfaces to support decision support systems and service management processes [13]. Infrastructure research also addresses hybrid cloud architecture, system monitoring frameworks, and data center administration models used in enterprise computing environments [16,19,20]. These infrastructures support data processing tasks required for large-scale digital financial platforms.

D. Cybersecurity, Monitoring Systems, and Operational Intelligence

Operational monitoring in digital platforms also includes security analysis and infrastructure monitoring. Identity and access management research examines anomaly detection methods used to identify abnormal system activities and unauthorized access attempts [9]. Network monitoring dashboards support continuous observation of system performance and digital infrastructure activities [22]. Automated threat detection models identify cyber incidents and abnormal network behavior in enterprise environments [23]. Incident response frameworks analyze system vulnerabilities and support threat mitigation procedures in corporate networks [21]. Additional studies discuss AI-supported monitoring platforms and infrastructure automation systems that analyze operational data within enterprise technology environments [24]. These works indicate that monitoring systems and cybersecurity analytics support the identification of operational risk indicators in digital service platforms.

III. METHODOLOGY

This study presents a methodological framework that derives operational risk indicators from customer interaction records generated within digital banking platforms. Digital banking services produce large volumes of interaction data through customer communications, support requests, complaints, and service logs. These records contain descriptions of operational issues experienced during banking activities. Careful examination of such records reveals observable conditions related to service reliability, transaction processing, and platform performance. The methodology integrates customer interaction data with Management Information System (MIS) event logs in order to identify patterns associated with operational disruptions. Interaction records pass through several analytical stages that transform raw communication data into structured operational indicators. These indicators support observation of operational conditions such as service delays, authentication instability, and platform performance variation.

A. Proposed Analytical Framework

The analytical framework treats customer interaction records as signals that reflect operational conditions within digital banking systems. Customers communicate with banking services through several digital channels, including support portals, complaint systems, chat interfaces, and feedback forms. Each interaction produces a record describing the circumstances experienced during a banking activity. The framework organizes these records through a structured analytical sequence. Interaction data collected from service channels combines with MIS event logs that record system activities such as transaction processing and authentication events. The resulting dataset contains both user-reported issues and system activity records.

Preprocessing procedures organize the combined dataset into standardized categories. Categorization allows the dataset to represent recurring service issues in a consistent form. Interaction records then undergo analytical examination to detect repeated patterns associated with operational disruptions. Recurring interaction patterns indicate potential operational conditions within the banking platform. The analytical framework converts these patterns into operational risk indicators that represent service interruptions, authentication problems, and system performance issues. Figure 1 presents the conceptual structure of the proposed framework.

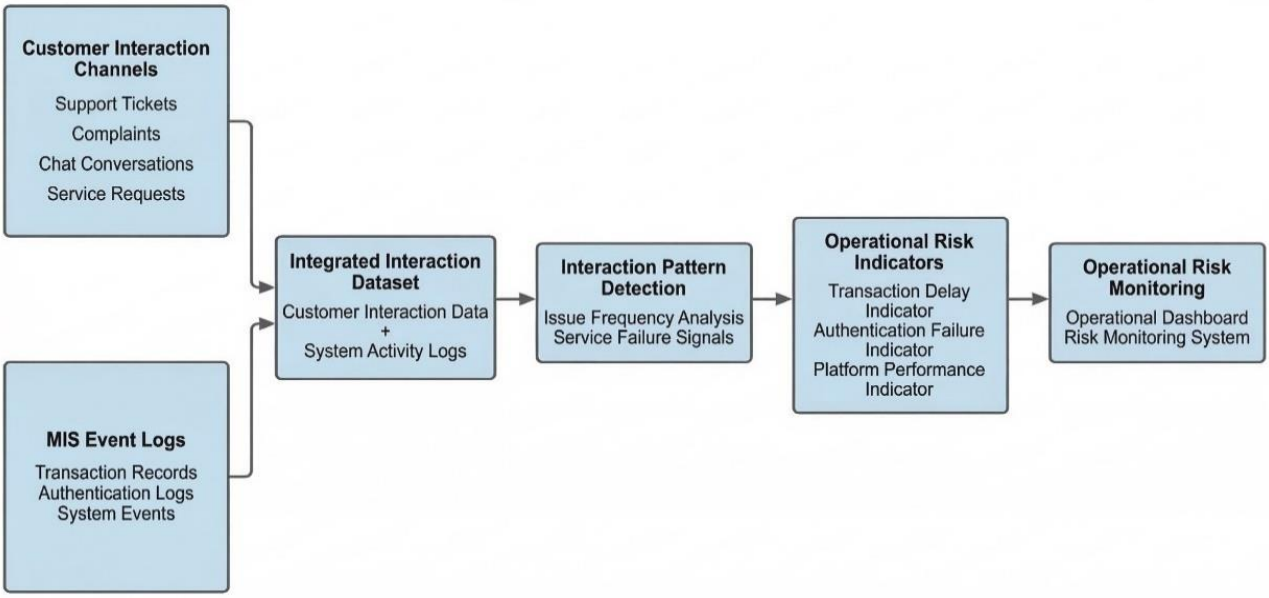

Figure 1: Conceptual framework for deriving operational risk indicators from customer interaction data in digital banking platforms

The diagram can be represented as a sequence diagram with six components placed in sequence from left to right. The first component is for Customer Interaction Channels, which includes support tickets, complaint submission, chat conversations, and requests for service. The second component represents MIS Event Logs, which record system activities such as transaction execution and authentication events. Both components connect to the third stage, Integrated Interaction Dataset, where interaction records and system logs form a unified dataset. The fourth component represents Interaction Pattern Detection, where recurring service issues and interaction trends appear through analytical examination. The fifth component represents Operational Risk Indicators, which summarize the detected patterns. The final component represents Operational Risk Monitoring, where these indicators support observation of operational conditions within the digital banking platform.

B. Customer Interaction Data Collection

Customer interaction data originates from several digital communication channels used in online banking services. These channels include customer support portals, complaint management platforms, live chat services, and digital feedback systems. Each channel produces records that describe user experiences during banking activities. Customer support tickets represent structured service requests submitted through digital banking platforms. These records often contain descriptions of transaction failures, delayed transfers, account access problems, or system errors. Complaint management systems record formal complaints submitted after service disruptions remain unresolved. Such complaints frequently contain detailed explanations of operational difficulties encountered during financial transactions. Live chat systems generate conversational records between customers and service agents. These conversations often include immediate descriptions of service problems that occur during online banking sessions. Service request logs capture additional operational attributes such as interaction timestamps, issue categories, and resolution outcomes. These records allow observation of service activity trends across time. The dataset also includes MIS event logs generated within the banking infrastructure. These logs record transaction execution events, authentication attempts, and service processing activities. Integration of interaction records with MIS event logs allows examination of relationships between customer reports and system activity within the digital banking environment.

C. Data Processing and Interaction Log Analysis

Customer interaction datasets contain structured attributes as well as textual descriptions. Analytical examination requires preprocessing procedures that convert these records into a consistent dataset suitable for analysis. Data cleaning removes incomplete entries and duplicate records. The resulting dataset undergoes categorization according to standardized interaction types. Similar service issues appear under consistent labels such as transaction errors, authentication problems, service delays, or application performance issues. Text descriptions contained in interaction records provide additional information regarding service problems. Keyword identification techniques extract recurring issue terms from customer communications. These terms assist the classification of interaction records according to operational themes. Interaction records are then matched with MIS event logs that record system activities during corresponding operational periods. Temporal comparison reveals relationships between customer reports and operational

events recorded in system logs. For example, a concentration of customer complaints related to payment failures may correspond to system events indicating transaction processing delays. This integrated dataset supports interaction log analysis that identifies patterns reflecting operational behavior within the digital banking platform.

D. Operational Risk Indicator Identification

Operational risk indicators originate from recurring patterns detected within interaction records. Repeated descriptions of similar service problems often correspond to operational conditions within the banking platform. Interaction analysis examines how frequently particular service issues appear across customer records. Numerous reports of delayed transactions may indicate congestion within transaction processing systems. Frequent login complaints may correspond to authentication instability. Reports describing application errors may signal performance limitations within the digital platform. These recurring patterns translate into operational risk indicators that represent observable operational conditions. Table 1 summarizes examples of interaction sources and the operational indicators derived from them.

Table 1: Customer interaction data and derived operational risk indicators

Customer Interaction Source	Observed Interaction Pattern	Operational Risk Indicator
Customer support tickets	Frequent reports of failed transactions	Transaction processing instability
Complaint submissions	Repeated reports of delayed payments	Transaction delay risk
Live chat conversations	High number of authentication issues	Authentication reliability risk
Service request logs	Increased verification requests	Identity verification system pressure
Customer feedback records	Reports of application performance problems	Digital platform performance risk

The indicators shown in Table 1 summarize operational issues reflected in customer communication records.

E. Operational Risk Monitoring Model

The final stage integrates the extracted indicators into a monitoring model for digital banking systems. This model evaluates interaction trends and translates them into signals representing operational conditions within the banking platform. The monitoring process begins with continuous collection of interaction records and system activity logs. Preprocessing procedures organize and categorize these records into a structured dataset. Feature extraction identifies attributes such as interaction type, issue category, and occurrence frequency. Interaction pattern analysis evaluates the frequency of operational issues across time intervals. Concentrated occurrences within short periods may indicate operational stress within the banking platform. The resulting indicators provide signals that support operational monitoring systems used within digital banking services. Figure 2 illustrates the analytical workflow applied in the methodology.

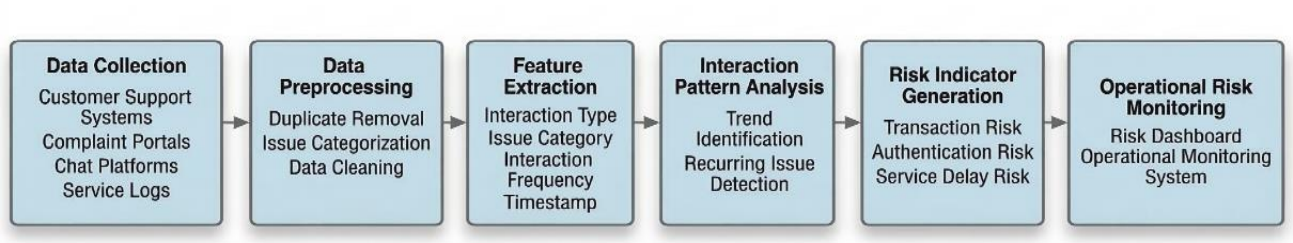

Figure 2: Analytical workflow for deriving operational risk indicators from customer interaction records

The diagram consists of six sequential stages arranged from left to right. The first stage represents Data Collection, which gathers interaction records and MIS event logs from digital banking systems. The second stage represents Data Preprocessing, where records undergo cleaning and categorization. The third stage represents Feature Extraction, which identifies attributes such as issue category and interaction frequency. The fourth stage represents Interaction Pattern Analysis, which examines recurring service issues and operational trends. The fifth stage represents Risk Indicator Generation, where interaction patterns convert into operational indicators. The final stage represents Operational Risk Monitoring, where these indicators support observation of operational conditions within the digital banking platform.

Research Gap

Previous research on operational risk within financial systems concentrates on transaction fraud detection, cybersecurity monitoring, and infrastructure analytics derived from system logs or network activity. These approaches address security incidents and system performance conditions. Customer interaction data receives limited attention as a source of operational risk analysis in digital banking platforms. Customer communications often contain direct descriptions of service disruptions experienced during banking activities. The methodology presented in this study

addresses this gap through systematic analysis of customer interaction records combined with MIS event logs in order to derive operational risk indicators for digital banking systems.

IV. DISCUSSION AND RESULTS

This section presents the analytical results obtained from the methodological framework described earlier. The analysis examines customer interaction records collected from digital banking service channels and relates these records to operational conditions observed in system activity logs. Interaction data provides descriptions of service problems encountered during banking activities. These descriptions include transaction delays, authentication errors, and application performance problems. Systematic examination of interaction records reveals patterns associated with operational conditions within the banking platform. Repeated issue reports appear across several interaction channels. When these reports occur within short time intervals, they often correspond to operational events recorded in MIS system logs. The combined analysis of interaction records and system activity data produces indicators that represent operational conditions in digital banking services.

A. Interaction Pattern Analysis in Digital Banking Platforms

Customer interaction datasets contain records from multiple service channels. The dataset examined in this study includes support tickets, complaint submissions, chat conversations, service requests, and feedback messages. Each interaction record provides information related to a service issue experienced during a banking transaction. Interaction analysis identifies several recurring issue categories. Transaction processing delays appear frequently in support tickets and complaint records. Authentication issues appear often in chat conversations and login assistance requests. Platform performance issues occur in feedback messages related to mobile or web banking applications. Temporal patterns also appear in the interaction dataset. Several interaction reports occur within short time periods during operational disturbances. These clusters often correspond to system events recorded in MIS logs that indicate transaction processing delays or authentication failures. Figure 3 illustrates the distribution of interaction categories observed during the analysis.

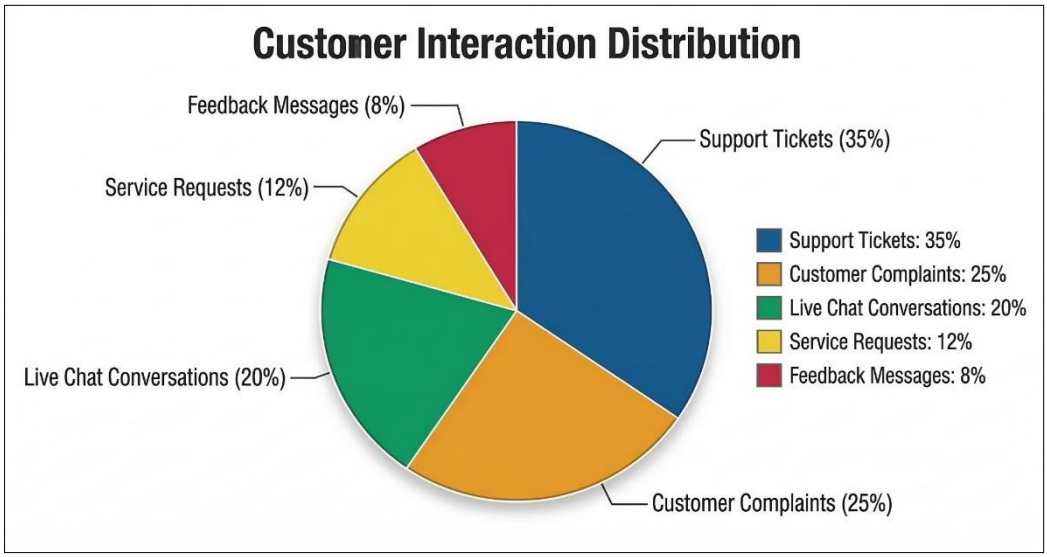

Figure 3: Distribution of customer interaction categories used in operational risk analysis.

The figure indicates that support tickets and complaint submissions form the largest portion of interaction records. These categories often contain descriptions of transaction delays, payment errors, and account access problems. Chat conversations also provide important operational information because customers frequently report issues during real-time support sessions.

B. Derivation of Operational Risk Indicators

Recurring interaction patterns indicate operational conditions within the banking platform. Interaction analysis evaluates the frequency and distribution of issue categories reported in customer communications. When similar issues appear repeatedly in interaction records, the pattern signals a potential operational problem within the digital banking system. Several operational indicators appear from the interaction analysis. Transaction processing instability corresponds to frequent reports of failed or incomplete financial transactions. Payment delay risk appears in repeated complaints related to delayed transfers or payment confirmation problems. Authentication reliability risk corresponds to login failures and password verification issues. Platform performance risk appears in feedback messages describing application errors or slow system response. Table 2 summarizes operational indicators derived from interaction records.

Table 2: Operational risk indicators derived from customer interaction data

Interaction Category	Observed Issue Pattern	Derived Operational Indicator
Support tickets	Failed or incomplete transactions	Transaction processing instability
Complaint submissions	Delayed transfers or payments	Payment processing delay risk
Chat conversations	Login and authentication problems	Authentication reliability risk
Service requests	Repeated verification requests	Identity verification pressure
Feedback messages	Application errors or slow response	Platform performance risk

The indicators listed in Table 2 represent operational conditions observed through customer communication records. Each indicator corresponds to a service disruption category within the digital banking system.

C. Quantitative Operational Risk Scoring

Interaction patterns detected in the analysis allow construction of a quantitative operational risk score. The score represents the aggregated influence of interaction indicators within a given time period.

Let:

- fi denote the frequency of issue category i
- wi denote the severity weight assigned to issue category i

The operational risk score is defined as

$$ORS = \sum_{i=1}^{n} w_i f_i$$

where:

- ORS represents the operational risk score
- n represents the number of interaction categories

The severity weight reflects the operational impact associated with each issue category. For instance, transaction failures receive a higher weight than minor interface delays because transaction disruptions affect financial operations directly.

A normalized operational risk score allows comparison across time intervals:

$$NORS = \frac{ORS}{\sum_{i=1}^{n} f_i}$$

The normalized score provides a proportional representation of operational pressure within the banking system. Higher values correspond to periods where interaction records indicate increased operational disturbances.

D. Integration of Interaction Data and System Logs

Customer interaction data provides information about user experiences during digital banking activities. System activity logs provide records related to internal system operations such as transaction execution, authentication attempts, and service response times. Joint examination of these datasets reveals relationships between user-reported issues and operational events recorded in system logs. For example, a sudden increase in transaction failure reports may coincide with system records indicating processing delays. Similarly, multiple login complaints may correspond to authentication system errors recorded in MIS logs. Figure 4 illustrates the analytical workflow that combines interaction records with system activity logs to generate operational indicators.

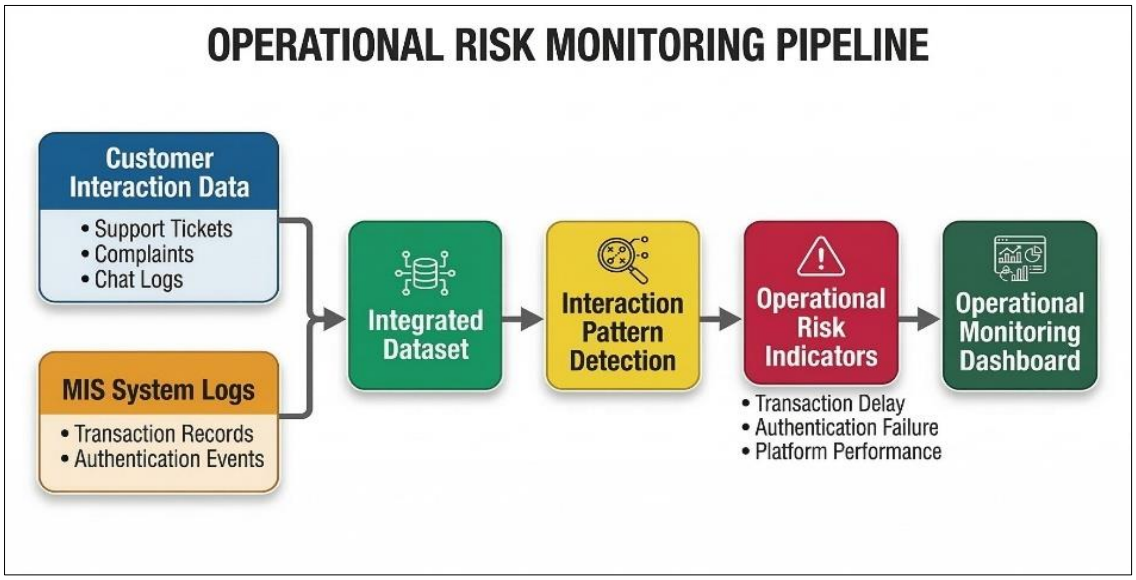

Figure 4: Analytical workflow for interaction-based operational risk monitoring

The workflow illustrates the sequence of analytical steps that convert interaction records into operational indicators. Interaction data and system logs form a unified dataset. Pattern detection identifies recurring service issues. These patterns translate into indicators that represent operational conditions.

E. Interpretation of Results

The results indicate that customer interaction records provide valuable information regarding operational conditions within digital banking systems. Customer communications often contain immediate descriptions of service problems encountered during financial transactions. These descriptions appear in interaction logs soon after service disruptions occur. Interaction analysis also reveals several patterns related to service reliability. Frequent reports of transaction delays correspond to operational pressure within transaction processing systems. Authentication problems appear during periods of system login failure. Application performance complaints appear during high system activity periods. Combined analysis of interaction records and system logs produces a comprehensive representation of operational conditions within digital banking services. System logs record internal system events, while interaction records capture customer experiences during service usage. When these data sources appear together in the analytical framework, the resulting indicators represent operational conditions that affect both system performance and customer service quality.

F. Implications for Operational Risk Monitoring

The analytical results show that customer interaction data can function as an additional source of information for operational monitoring in digital banking systems. Interaction indicators complement existing monitoring methods that rely mainly on system logs or infrastructure metrics. Operational monitoring systems can incorporate interaction indicators into dashboards used by banking administrators. These indicators provide signals related to service disruptions and system instability. Monitoring platforms can track interaction trends across time and identify operational disturbances within the banking system. The analytical framework presented in this study demonstrates that customer communication records provide useful information for operational risk monitoring. Interaction analysis, combined with system activity records, produces indicators that represent operational conditions in digital banking platforms.

G. Limitations of the Study

Several limitations affect the interpretation of the results presented in this study. The analysis relies mainly on customer interaction records collected from support tickets, complaint submissions, chat conversations, and feedback messages. These records capture issues reported through digital service channels; operational problems that occur without customer reports may remain outside the dataset. Interaction data also contains subjective descriptions of service issues, and different users may describe similar problems in different ways. Such variation can influence issue categorization during interaction analysis. The study examines interaction records together with MIS event logs from a particular digital banking environment. Banking platforms often differ in system architecture, service design, and operational procedures. These differences may influence interaction patterns observed in other systems. Future research may include additional operational datasets, such as infrastructure monitoring records and transaction performance metrics, to obtain a broader view of operational conditions.

V. CONCLUSION

This study presented an analytical framework for deriving operational risk indicators from customer interaction data in digital banking platforms. The proposed approach examined interaction records such as support tickets, complaint submissions, chat conversations, and service logs together with MIS event data in order to identify recurring service issue patterns. The analysis shows that customer interaction records contain information related to operational conditions within digital banking systems. Interaction logs frequently reflect transaction delays, authentication failures, and platform performance problems experienced during financial service usage. These observations indicate that interaction-based indicators can complement monitoring approaches that rely on system logs and infrastructure metrics. The framework introduced in this research therefore provides an additional analytical perspective for operational monitoring in digital financial services through systematic examination of customer interaction data.

Future research may extend this framework through the use of larger datasets collected from multiple digital banking platforms. Additional data sources such as transaction monitoring records, infrastructure performance metrics, and network activity logs may provide a broader view of operational behavior in financial systems. Machine learning models may also support pattern detection within interaction datasets and assist in identifying early signals of operational disruption. Further investigation may examine the integration of interaction-based indicators into real-time monitoring systems used in digital banking operations. These directions may contribute to more comprehensive approaches for operational risk monitoring in digital financial platforms.

REFERENCES

1. Tabassum, M., Rokibuzzaman, M., Islam, M. I., & Bristy, I. J. (2025, September). Data-driven financial analytics through MIS platforms in emerging economies. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 440–446. https://doi.org/10.36348/sjet.2025.v10i09.007

2. Hasan, E. (2025). Secure and scalable data management for digital transformation in finance and IT systems. *Zenodo*. https://doi.org/10.5281/zenodo.17202282
3. Akhter, T. (2025, October 6). Algorithmic internal controls for SMEs using MIS event logs. *TechRxiv*. https://doi.org/10.36227/techrxiv.175978941.15848264.v1
4. Akhter, T. (2025, October 6). MIS-enabled workforce analytics for service quality & retention. *TechRxiv*. https://doi.org/10.36227/techrxiv.175978943.38544757.v1
5. Al Sany, S. M. A. (2025). The role of data analytics in optimizing budget allocation and financial efficiency in startups. *IJSRED – International Journal of Scientific Research and Engineering Development,* *8*(5), 2287–2297. https://doi.org/10.5281/zenodo.17536325
6. Rahman, M. (2025). Design and implementation of a data-driven financial risk management system for
7. U.S. SMEs using federated learning and privacy-preserving AI techniques. *IJSRED – International Journal of Scientific Research and Engineering Development,* *8*(6), 1041–1052. https://doi.org/10.5281/zenodo.17769869
8. Hasan, E. (2025). Machine learning-based KPI forecasting for finance and operations teams. *IJSRED – International Journal of Scientific Research and Engineering Development,* *8*(6), 2139–2149. https://doi.org/10.5281/zenodo.17926746
9. Hasan, E. (2025). SQL-driven data quality optimization in multi-source enterprise dashboards. *IJSRED – International Journal of Scientific Research and Engineering Development,* *8*(6), 2150–2160. https://doi.org/10.5281/zenodo.17926758
10. Zaman, S. U. (2025). Enhancing security in cloud-based IAM systems using real-time anomaly detection. *IJSRED – International Journal of Scientific Research and Engineering Development,* *8*(6), 2292–2304. https://doi.org/10.5281/zenodo.17926883
11. Rahman, T. (2026). Financial risk intelligence: Real-time fraud detection and threat monitoring. *Zenodo*. https://doi.org/10.5281/zenodo.18176490
12. Sharan, S. M. M. I., Fahim, M. A. I., & Farooq, H. (2026). Cloud native fintech analytics platform for IoT enabled retail networks. *World Journal of Advanced Engineering Technology and Sciences,* *18*(01), 089–104. https://doi.org/10.30574/wjaets.2026.18.1.1582
13. Nahar, S., Rahman, M., Alam, M. S., & Al Sany, S. M. A. (2026). Intelligent data governance and ethical AI framework for enterprise information systems. *Zenodo*. https://doi.org/10.5281/zenodo.18839122
14. Dukkipati, S. S. N. C. (2026, February 9). Design and implementation of scalable AI-driven conversational systems for enterprise-level feedback intelligence and decision support. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6263818
15. Rahman, M. A., Bristy, I. J., Islam, M. I., & Tabassum, M. (2025, September). Federated learning for secure inter-agency data collaboration in critical infrastructure. *Saudi Journal of Engineering and Technology*, *10*(9), 421–430. https://doi.org/10.36348/sjet.2025.v10i09.005
16. Rahman, M. A., Islam, M. I., Tabassum, M., & Bristy, I. J. (2025, September). Climate-aware decision intelligence: Integrating environmental risk into infrastructure and supply chain planning. *Saudi Journal of Engineering and Technology*, *10*(9), 431–439. https://doi.org/10.36348/sjet.2025.v10i09.006
17. Joarder, M. M. I. (2025). Disaster recovery and high-availability frameworks for hybrid cloud environments. *Zenodo*. https://doi.org/10.5281/zenodo.17100446
18. Joarder, M. M. I. (2025). Next-generation monitoring and automation: AI-enabled system administration for smart data centers. *TechRxiv*. https://doi.org/10.36227/techrxiv.175825633.33380552/v1
19. Joarder, M. M. I. (2025). Energy-efficient data center virtualization: Leveraging AI and CloudOps for sustainable infrastructure. *Zenodo*. https://doi.org/10.5281/zenodo.17113371
20. Farooq, H. (2025). Cross-platform backup and disaster recovery automation in hybrid clouds. *International Journal of Science and Innovation Engineering*, *2*(11), 220–242. https://doi.org/10.70849/IJSCI02112025025
21. Farooq, H. (2025). Resource utilization analytics dashboard for cloud infrastructure management. *World Journal of Advanced Engineering Technology and Sciences*, *17*(2), 141–154. https://doi.org/10.30574/wjaets.2025.17.2.1458
22. Zaman, S. U. (2025). Vulnerability management and automated incident response in corporate networks. *International Journal of Scientific Research and Engineering Development*, *8*(5), 2275–2286. https://doi.org/10.5281/zenodo.17536305
23. Afrin, S. (2025). Cloud-integrated network monitoring dashboards using IoT and edge analytics. *International Journal of Scientific Research and Engineering Development*, *8*(5), 2298–2307. https://doi.org/10.5281/zenodo.17536343
24. Afrin, S. (2025). Cyber-resilient infrastructure for public internet service providers using automated threat detection. *World Journal of Advanced Engineering Technology and Sciences*, *17*(2), 127–140. https://doi.org/10.30574/wjaets.2025.17.2.1475
25. Fahim, M. A. I., Sharan, S. M. M. I., & Farooq, H. (2025). AI-enabled cloud-IoT platform for predictive infrastructure automation. *World Journal*

of Advanced Engineering Technology and Sciences, *17*(3), 431–446. https://doi.org/10.30574/wjaets.2025.17.3.1574

26. Rahman, F. (2025). Data science in power system risk assessment and management. *World Journal of Advanced Engineering Technology and Sciences*, *17*(3),295–311. https://doi.org/10.30574/wjaets.2025.17.3.1560
27. Haque, S. (2025). Effectiveness of managerial accounting in strategic decision making. *Preprints*. https://doi.org/10.20944/preprints202509.2466.v1
28. Haque, S. (2025). The impact of automation on accounting practices. *International Journal of Scientific Research and Engineering Development*, *8*(6), 2312–2323. https://doi.org/10.5281/zenodo.18074324
29. Rahman, M. (2025). Integrating IoT and MIS for last-mile connectivity in residential broadband services.
30. *TechRxiv*. https://doi.org/10.36227/techrxiv.176054689.95468219/v1
31. Rahman, F., Nahar, S., & Mim, M. A. (2026). Cloud-native enterprise resource management for multi-sector operations. *Global Journal of Engineering and Technology Advances*, *26*(1), 126–141. https://doi.org/10.30574/gjeta.2026.26.1.0012
32. Islam, R. (2026). AI-integrated management information systems for manufacturing and supply chain risk mitigation. *Zenodo*. https://doi.org/10.5281/zenodo.18349501
33. Haque, S., & Al Sany, S. M. A. (2025). Impact of consumer behavior analytics on telecom sales strategy. *International Journal of Science and Innovation Engineering*, *2*(10), 998–1018. https://doi.org/10.70849/IJSCI02102025114
34. Hasan, E. (2025). Big data-driven business process optimization: Enhancing decision-making through predictive analytics. *TechRxiv*. https://doi.org/10.36227/techrxiv.175987736.61988942/v1
35. Rahman, F. (2025). Advanced statistical models for forecasting energy prices. *Global Journal of Engineering and Technology Advances*, *25*(3), 168–182. https://doi.org/10.30574/gjeta.2025.25.3.0350
36. Nahar, S. (2025). Optimizing HR management in smart pharmaceutical manufacturing through IIoT and MIS integration. *World Journal of Advanced Engineering Technology and Sciences*, *17*(3), 240–252. https://doi.org/10.30574/wjaets.2025.17.3.1554