Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

EDGE COMPUTING–ENABLED INTELLIGENT FINANCIAL AUDITING: AN ADVANCED REAL-TIME FRAMEWORK FOR AUTOMATED FRAUD DETECTION, PREDICTIVE ACCOUNTING ANALYTICS, AND FINANCIAL RISK ASSESSMENT

Muhammad Adil [1], Shahzeb Iqbal [2], Farah Arzu [3], Ashraf Zia [4], Muhammad Essa Siddique [5]

DOI: https://doi.org/10.63544/jbii.v5i5.194

Affiliations:

[1] Department of Commerce, University of the Punjab, Gujranwala Campus, Punjab, Pakistan
Email: adilmuhammadkhann@gmail.com

[2] Department of Computer Science, University of Mianwali, Mianwali, Pakistan
Email: shahzebiqbal749@gmail.com

[3] Tun Razaq Graduate School of Business, Universiti Tun Abdul Razak, Kuala Lumpur, Malaysia
Email: arzu.farah@ur.unirazak.edu.my

[4] Department of Computer Science, Abdul Wali Khan University Mardan, Mardan, Khyber Pakhtunkhwa, Pakistan
Email: ashrafzia@awkum.edu.pk

[5] Department of Computer Science & IT, University of Balochistan, Kharan Campus, Balochistan, Pakistan
Email: essasiddique@live.com

Corresponding Author's Email:

[1] ashrafzia@awkum.edu.pk
[2] shahzebiqbal749@gmail.com

Article History:
Received: 18.04.2026
Accepted: 15.05.2026
Published: 25.05.2026

Abstract

Purpose: *The increasing volume, velocity, and complexity of digital financial transactions have reduced the effectiveness of conventional auditing systems that depend on centralized processing, periodic examination, and static rule-based controls. This study develops an edge computing–enabled intelligent financial auditing framework for real-time fraud detection, predictive accounting analytics, and dynamic financial risk assessment.*

Design/Methodology/Approach. *The framework integrates distributed edge nodes, secure financial gateways, machine learning, attention-based deep learning, explainable artificial intelligence, and human-in-the-loop audit validation. A multi-institutional dataset comprising 285,000 anonymized transactions from 18,750 individual and corporate accounts collected over three years was used for framework evaluation. Following missing-value treatment, normalization, feature selection, class balancing, and temporal segmentation, the data were divided into training, validation, and testing subsets using a 70:15:15 ratio.*

Findings. *The proposed edge-enabled attention-based model achieved 97.4% accuracy, 96.8% precision, 97.1% recall, a 96.9% F1-score, and a 0.991 ROC–AUC, exceeding the best-performing benchmark, XGBoost, which produced 94.6% accuracy and a 0.967 ROC–AUC. Edge-based processing reduced average fraud-detection latency from 2.84 seconds to 0.41 seconds, lowered financial-data transmission requirements by 38.7%, and increased high-risk account identification by 21.6% compared with centralized auditing. Predictive analytics achieved a mean absolute percentage error of 6.8% for cash-flow forecasting and identified 93.5% of emerging financial-risk events before critical thresholds were reached.*

Research Limitations. *The dataset, while multi-institutional, may not fully represent all geographic regions or financial sectors. Future studies should incorporate cross-border payments, digital wallets, and cryptocurrency transactions.*

Practical Implications. *The framework offers a scalable and privacy-aware foundation for banks, accounting organizations, and audit firms pursuing secure real-time digital transformation. It can strengthen continuous assurance, accelerate fraud intervention, improve accounting forecasts, reduce audit workload, and support proactive financial governance.*

Keywords: Edge Computing; Intelligent Financial Auditing; Real-Time Fraud Detection; Predictive Accounting Analytics; Financial Risk Assessment; Explainable Artificial Intelligence; Machine Learning; Continuous Auditing

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

1. Introduction.

1.1 Background of the Study

The rapid digitalization of banking, accounting, and financial services has transformed the scale and structure of modern financial transactions. Organizations now process large volumes of payments, transfers, credit activities, digital invoices, account updates, authentication events, and cross-platform financial records in real time. Although this transformation has improved operational efficiency and service accessibility, it has simultaneously increased the complexity of financial auditing and risk monitoring. Conventional audit systems, which commonly rely on centralized data processing, periodic inspection, manual sampling, and predefined rule-based controls, are increasingly challenged by the volume, velocity, heterogeneity, and continuous nature of contemporary financial data (Amirineni & Abhilash, 2025). As fraudulent activities become more dynamic and technologically sophisticated, delays between transaction execution, audit inspection, risk identification, and corrective intervention can create substantial financial and regulatory exposure.

1.2 Problem Statement

Traditional financial auditing is largely retrospective. Auditors typically evaluate historical records, transaction samples, control procedures, and financial statements after accounting events have already occurred. This approach remains important for assurance and compliance; however, it is less effective for environments in which financial threats can develop within seconds or minutes. Fraudulent transactions, unauthorized account access, unusual beneficiary activity, abnormal cash-flow movements, identity manipulation, device inconsistency, and rapidly changing credit-risk conditions require more immediate detection capabilities. The transition from periodic auditing toward continuous and intelligent auditing therefore represents an important development in modern financial governance.

Artificial intelligence and machine-learning techniques have increasingly been adopted to enhance fraud detection and financial-risk analytics. Logistic regression, support vector machines, random forests, artificial neural networks, gradient-boosting approaches, and deep-learning models have demonstrated considerable potential in identifying nonlinear and high-dimensional patterns that may be difficult to detect using conventional auditing procedures. Nevertheless, many existing AI-enabled financial auditing solutions continue to depend heavily on centralized cloud infrastructures. Financial data are transmitted from operational systems to remote servers for processing, which can introduce communication latency, increase bandwidth consumption, create data-privacy concerns, and reduce responsiveness in time-sensitive fraud-detection environments.

1.3 Gap Analysis

Existing studies have investigated machine learning for fraud detection, cloud-based financial analytics, continuous auditing, predictive risk modelling, and explainable AI independently. However, comparatively limited research has integrated these capabilities within a unified edge computing–enabled financial auditing architecture that simultaneously addresses real-time fraud detection, predictive accounting analytics, dynamic financial risk assessment, explainability, communication efficiency, and auditor validation. Furthermore, many prior approaches evaluate predictive accuracy without examining operational indicators such as detection latency, data-transmission requirements, early risk-event identification, and the practical integration of automated models into continuous auditing workflows. These limitations indicate a need for a more comprehensive framework capable of combining predictive performance with computational efficiency, privacy awareness, and audit usability.

2. Literature Review

2.1 Theoretical Foundations

2.1.1 Resource-Based View (RBV) Theory. The Resource-Based View (RBV) perspective, as developed by Barney (1991), suggests that sustained competitive advantage is attained by firms through valuable, rare, inimitable, and non-substitutable (VRIN) resources. In the context of intelligent financial auditing, edge computing infrastructure, advanced analytical capabilities, and AI-driven decision support systems represent strategic resources that can provide organizations with superior fraud detection and risk

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

assessment capabilities (Ahmad et al., 2025). The integration of edge computing and AI capabilities enables organizations to develop unique competencies in real-time transaction monitoring and risk identification.

2.1.2 Dynamic Capabilities Framework. The Dynamic Capabilities framework, proposed by Teece et al. (1997), emphasizes the ability of organizations to sense, seize, and reconfigure resources in response to environmental changes. In financial auditing, dynamic capabilities are demonstrated through the ability to continuously adapt fraud-detection models, update risk assessments, and reconfigure analytical processes in response to emerging threats (Ahmad et al., 2026). Edge computing enables faster sensing and response capabilities, while machine learning facilitates continuous learning and adaptation to evolving fraud patterns.

2.1.3 Stakeholder Theory. Stakeholder theory (Freeman, 1984) states that organizations should balance the interests of various stakeholders, including shareholders, customers, regulators, employees, and the broader public. In the context of financial auditing, this perspective highlights the importance of transparent, accountable, and privacy-aware auditing practices. An intelligent auditing framework must therefore protect stakeholder interests by ensuring data privacy, regulatory compliance, and decision transparency (Moreau, 2025). The integration of explainable AI and privacy-preserving processing directly supports stakeholder trust and accountability.

2.2 Key Constructs and Prior Research

2.2.1 Edge Computing in Financial Systems. Edge computing offers a potential solution to the limitations of centralized processing by relocating selected computational and analytical processes closer to the sources where financial data are generated (Timileyin, 2026). In an edge-enabled financial architecture, transaction screening, anomaly detection, feature extraction, risk scoring, and preliminary model inference can be performed through local or distributed edge nodes before information is transmitted to centralized cloud or enterprise audit systems. Such an approach can reduce the volume of raw financial data transferred across networks, decrease processing delays, improve operational resilience, and strengthen privacy by limiting unnecessary exposure of sensitive information.

Lambropoulos et al. (2026) examined emerging technologies in financial services, highlighting the transition from virtualization and cloud infrastructures to edge computing applications. Their research demonstrated that edge-enabled architectures can significantly improve responsiveness and data privacy in financial monitoring systems. Similarly, Akinsanya et al. (2023) provided a comprehensive review of edge computing approaches for secure and efficient data processing, emphasizing the importance of distributed intelligence for real-time anomaly detection.

2.2.2 Machine Learning for Fraud Detection. Artificial intelligence and machine-learning techniques have been widely adopted to enhance fraud detection and financial-risk analytics. Logistic regression, support vector machines, random forests, artificial neural networks, gradient-boosting approaches, and deep-learning models have demonstrated considerable potential in identifying nonlinear and high-dimensional patterns that may be difficult to detect using conventional auditing procedures (Zakaria et al., 2025). These models can analyze transactional behavior, account histories, device characteristics, authentication patterns, payment velocity, beneficiary relationships, and other indicators to estimate the probability of fraudulent or high-risk activity.

Khan et al. (2025) investigated real-time financial fraud detection using cognitive 6G networks and distributed AI for autonomous risk management. Their study demonstrated the potential of combining advanced communication networks with AI-driven analytics for enhanced fraud detection capabilities. Bello et al. (2023) examined AI-driven approaches for real-time fraud detection in US financial transactions, highlighting both the opportunities and challenges associated with implementing AI in financial monitoring systems.

2.2.3 Attention-Based Deep Learning. Deep-learning methods have become increasingly important in financial auditing because modern financial datasets contain complex, nonlinear, and time-dependent relationships that are often difficult to identify using conventional statistical techniques. Artificial neural networks, convolutional neural networks, recurrent neural networks, long short-term memory networks, and hybrid deep-learning architectures have been applied to fraud detection, credit-risk prediction, transaction

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

classification, financial forecasting, and anomaly identification. Despite their strong predictive capabilities, conventional deep-learning models may not always distinguish effectively between highly informative and less relevant financial indicators.

Attention mechanisms address this limitation by enabling the model to assign greater importance to features or observations that contribute more strongly to a particular prediction (Nawaz & Musah, 2025). In financial auditing, variables such as transaction amount, payment velocity, beneficiary novelty, failed-login frequency, device inconsistency, geographical deviation, cash-flow volatility, and credit exposure may contribute differently across transactions and accounts. An attention-based architecture can dynamically identify the most influential combinations of these indicators and prioritize them during fraud or risk classification.

Table 1

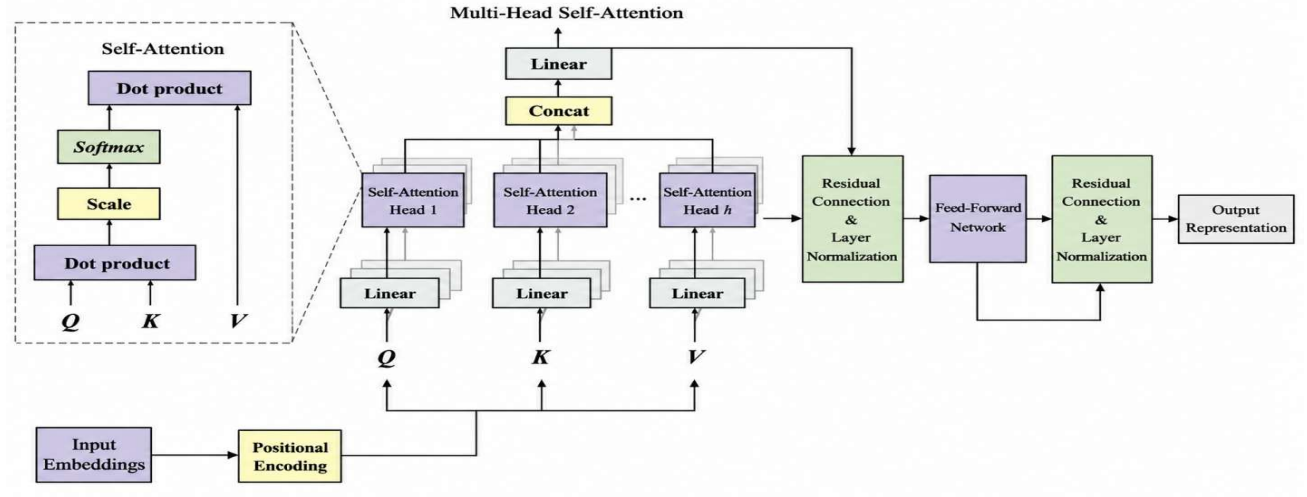
Comparative characteristics of deep-learning approaches for intelligent financial auditing

Deep-learning approach	Principal capability	Financial auditing application
Artificial Neural Network	Nonlinear feature learning	Fraud classification and credit-risk prediction
Convolutional Neural Network	Local pattern and feature-interaction extraction	Transaction-pattern recognition and anomaly detection
Recurrent Neural Network	Sequential information processing	Temporal transaction monitoring
Long Short-Term Memory	Long-term temporal dependency learning	Behavioral analysis and financial forecasting
Attention-Based Deep Learning	Dynamic weighting of important features and observations	Fraud detection, risk prioritization, and audit intelligence
Hybrid Attention Architecture	Integrated temporal, nonlinear, and selective feature learning	Real-time fraud and financial-risk assessment

The conceptual operation of an attention-based financial auditing model is illustrated in Figure 1. Financial information is initially collected from multiple sources and organized into transactional, accounting, behavioral, device, network, and credit-risk features. These features are processed through deep-learning layers to generate high-level representations of account and transaction behavior. The attention mechanism then identifies the most relevant risk-sensitive information and gives greater importance to indicators that are strongly associated with fraud or financial instability.

Figure 1

Multi-head self-attention architecture with residual connections and feed-forward processing



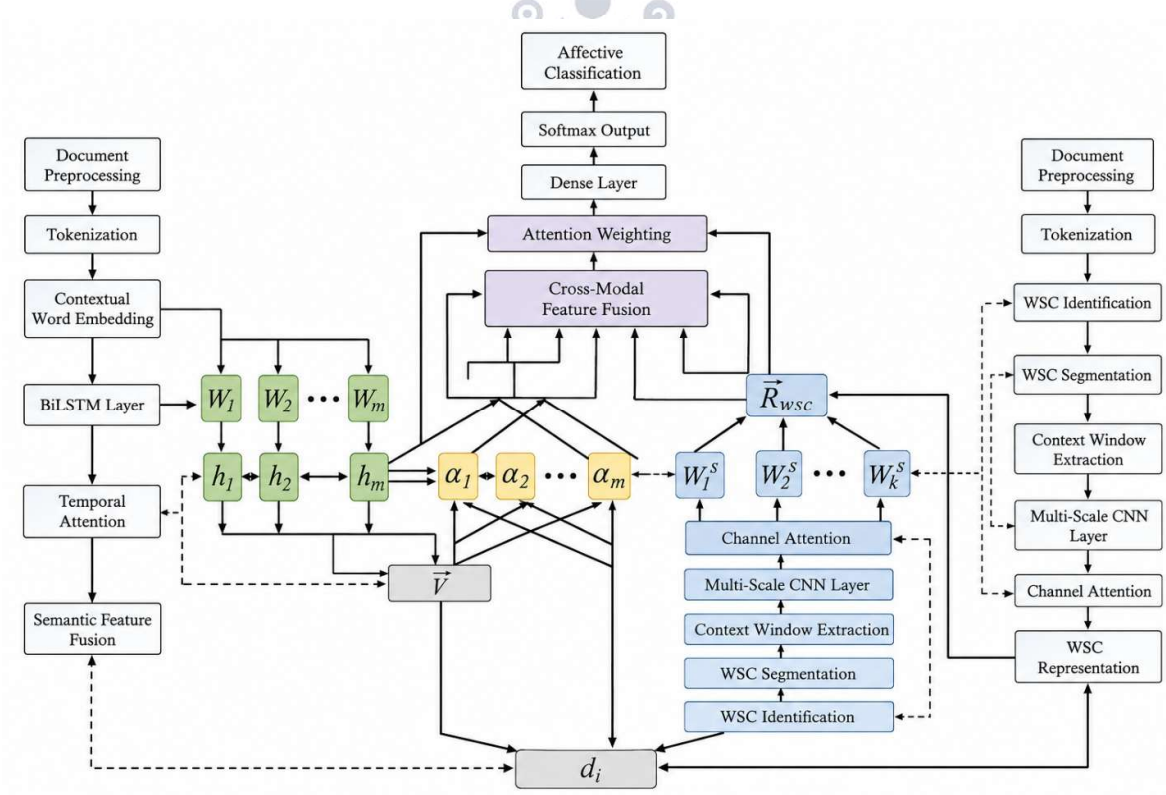
Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

2.3 Privacy-Preserving and Secure Financial Data Processing

Financial auditing systems process highly sensitive information, including transaction histories, account balances, authentication records, credit exposure, customer behavior, device identifiers, and historical audit findings. As auditing becomes increasingly data-driven and interconnected, protecting the confidentiality, integrity, and availability of this information has become a central requirement. Conventional centralized architectures often transmit large volumes of raw financial data to remote servers or cloud platforms, which may increase exposure to unauthorized access, interception, data leakage, and cyberattacks [9]. Privacy-preserving and secure processing is therefore essential for the practical deployment of intelligent financial auditing systems. Edge computing provides an important mechanism for reducing these risks by enabling selected analytical operations to be performed closer to the financial data source. Transaction screening, feature extraction, fraud scoring, anomaly detection, and preliminary risk assessment can be conducted at edge nodes before information is forwarded to centralized infrastructure. This approach can limit the transmission of complete raw datasets and reduce the amount of sensitive financial information moving across communication networks. As illustrated in Figure 2, the edge layer functions as an intermediate security and intelligence layer between financial data sources and centralized audit infrastructure.

Figure 2

Privacy-preserving and secure data-processing architecture for edge-enabled financial auditing.



Secure financial gateways can be used to authenticate incoming data streams, validate transaction integrity, and establish encrypted communication between operational systems and edge nodes. The edge layer then performs local analytical tasks while retaining sensitive information whenever centralized transmission is unnecessary. Only relevant features, model outputs, anomaly summaries, or high-risk events may be transferred for deeper analysis. This data-minimization strategy can reduce privacy exposure while preserving the analytical value required for continuous auditing. Several security and privacy controls can be integrated into an edge-enabled audit environment [10]. These include encryption of financial data during transmission and storage, role-based access control, identity verification, secure communication protocols,

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

pseudonymization, transaction logging, and continuous monitoring of unauthorized access attempts. Table 2 present the principal privacy and security mechanisms and their relevance to intelligent financial auditing.

Table 2

Privacy and security mechanisms for intelligent financial auditing

Security or privacy mechanism	Primary purpose	Expected benefit
Data encryption	Protect sensitive information	Reduces unauthorized data exposure
Strong authentication	Verify authorized users and systems	Limits unauthorized system access
Role-based access control	Restrict privileges	Supports confidentiality and accountability
Data minimization	Reduce unnecessary data movement	Improves privacy and communication efficiency
Pseudonymization	Protect personal identity	Supports privacy-aware analysis
Secure edge processing	Analyze data near its source	Reduces latency and raw-data transmission
Audit logging	Maintain traceable system activity	Strengthens accountability and compliance
Continuous security monitoring	Detect suspicious access or system behavior	Improves real-time cyber-risk detection

An additional advantage of privacy-aware edge processing is improved compliance with organizational and regulatory requirements related to financial-data governance. Limiting the unnecessary movement of raw customers and transaction data can reduce the potential impact of security breaches and provide organizations with greater control over where sensitive information is processed. This is particularly relevant in multi-institutional environments where data may originate from several banking, accounting, or payment systems with different access-control and governance requirements. However, decentralizing financial processing also introduces new security challenges. Edge devices and gateways may themselves become attack targets, particularly if they operate across distributed locations. Weak authentication, outdated software, insecure communication interfaces, and compromised edge nodes can create vulnerabilities within the overall auditing architecture. Therefore, edge-based systems require continuous security monitoring, controlled software updates, device authentication, intrusion detection, and comprehensive logging mechanisms.

Privacy preservation must also be balanced with audit transparency. Excessive data restriction may prevent auditors from accessing sufficient evidence to evaluate suspicious activities, while excessive data collection can create unnecessary privacy exposure. An effective architecture should therefore follow a selective-access approach in which auditors receive the information required for verification while sensitive attributes unrelated to the audit objective remain protected. Overall, privacy-preserving and secure financial data processing is a fundamental requirement for intelligent auditing. The combination of secure gateways, edge-based local processing, data minimization, encryption, controlled access, anonymization, and traceable audit logs can substantially reduce the privacy and security risks associated with centralized data-intensive systems. Integrating these mechanisms into an edge-enabled auditing framework can support real-time analytical performance while strengthening confidentiality, regulatory traceability, and institutional trust.

2.4. Research Objectives

The study is guided by the following objectives:

RO1. To develop an edge computing–enabled intelligent financial auditing framework for real-time fraud detection

RO2. To integrate predictive accounting analytics for cash-flow forecasting and early risk identification

RO3. To implement dynamic financial risk scoring for continuous audit prioritization

RO4. To evaluate the framework's predictive accuracy, operational efficiency, and practical usability

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

RO5. To incorporate explainable AI and human-in-the-loop validation for audit transparency and regulatory compliance

2.5 Research Questions

Correspondingly, the study poses four research questions:

RQ1. Can an edge computing–enabled attention-based deep learning framework achieves superior fraud-detection performance compared with conventional machine-learning benchmarks?

RQ2. How does edge-based processing affect fraud-detection latency, data-transmission requirements, and high-risk account identification?

RQ3. Can predictive accounting analytics effectively forecast cash flows and identify emerging financial-risk events before critical thresholds are reached?

RQ4. Does the integration of explainable AI and human-in-the-loop validation improve audit transparency and decision-making?

3. Research Methodology

3.1 Research Design and Philosophical Orientation

3.1.1 Research Design. The methodology was designed to develop and evaluate an edge computing–enabled intelligent financial auditing framework capable of supporting real-time fraud detection, predictive accounting analytics, and dynamic financial risk assessment. The proposed research design integrates financial data acquisition, preprocessing, feature engineering, distributed edge processing, machine-learning benchmarking, attention-based deep learning, explainable artificial intelligence, and human-in-the-loop audit validation within a unified analytical workflow. Particular emphasis was placed on ensuring that the framework could process heterogeneous financial information with low latency while maintaining predictive accuracy, security, privacy, and audit interpretability.

3.2 Multi-Institutional Financial Dataset Construction

A multi-institutional financial dataset was constructed to provide a diverse and representative basis for evaluating the proposed edge computing–enabled intelligent auditing framework. The dataset comprised 285,000 anonymized financial transactions associated with 18,750 individual and corporate accounts collected over a three-year period. The records represented routine transactions, suspicious activities, confirmed fraud events, credit-risk conditions, behavioural anomalies, and historical audit observations. This structure enabled the framework to examine both transaction-level irregularities and longer-term changes in account behaviour.

The dataset contained 46 variables grouped into six principal categories: transactional, accounting, behavioural, device-related, network-related, and credit-risk indicators. Transactional variables captured characteristics such as transaction amount, payment velocity, transfer frequency, transaction timing, beneficiary novelty, and balance movement. Accounting indicators reflected cash-flow volatility, liquidity variation, receivable and payable behaviour, and revenue–expense patterns. Behavioural and security variables were included to represent unusual login activity, changes in transaction behaviour, device inconsistency, geographical deviation, and abnormal access patterns. Anonymization and integration were performed before the analytical dataset entered the preprocessing stage. Personally identifiable information was removed, while account and transaction identifiers were replaced with anonymized reference codes.

Table 3

Main categories and representative variables included in the financial dataset

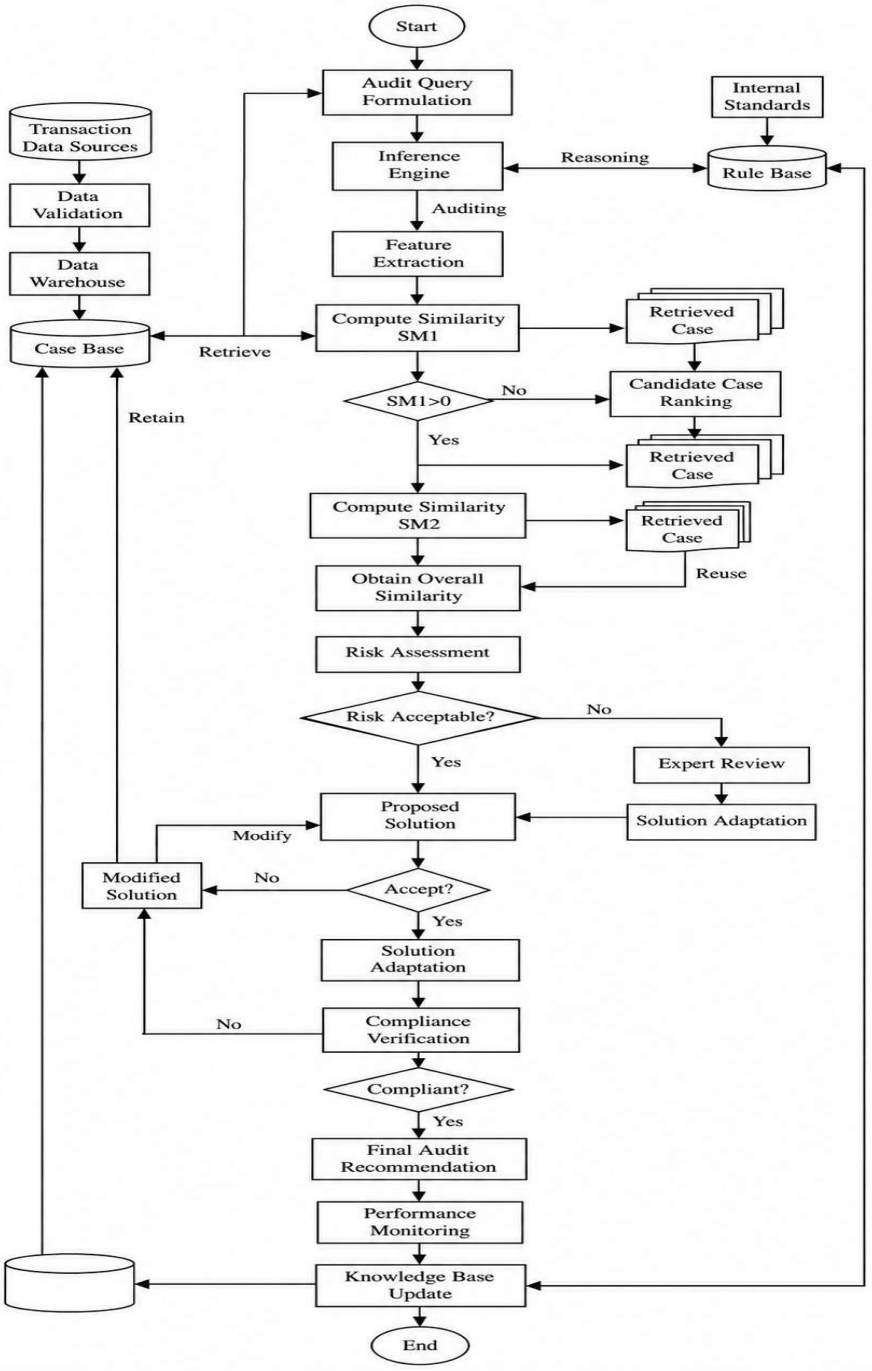
Variable category	Representative variables	Primary analytical purpose
Transactional	Transaction amount, payment velocity, transfer frequency, transaction timing, beneficiary novelty	Detect unusual payment and transfer behavior
Accounting	Cash-flow volatility, balance fluctuations, liquidity movement, receivable/payable patterns	Identify accounting anomalies and financial instability
Behavioral	Historical transaction deviation, unusual account activity, failed-login frequency	Capture changes in customer or account behavior

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Device-related	Device inconsistency, new-device activity, authentication changes	Detect technology-related fraud indicators
Network-related	Geographical deviation, unusual IP behavior, access-frequency variation	Identify abnormal digital-access conditions
Credit-risk	Credit exposure, repayment behavior, overdue activity, historical risk events	Support financial-risk assessment and early warning

Figure 3

Case-based intelligent auditing workflow for risk assessment and compliance verification.



Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

3.3 Secure Edge–Cloud Financial Auditing Architecture

The proposed financial auditing framework was designed using a secure edge–cloud architecture to support low-latency fraud detection, predictive accounting analytics, and continuous financial risk assessment. Instead of transmitting every raw financial record directly to centralized infrastructure, selected preprocessing and analytical tasks were performed at distributed edge nodes located closer to transaction sources. This arrangement was intended to reduce communication delay, limit unnecessary transmission of sensitive financial information, and improve the responsiveness of audit-risk detection. The architecture consisted of five interconnected layers: financial data sources, secure financial gateways, edge intelligence, centralized cloud analytics, and auditor decision support.

Transactional and accounting information originated from digital banking systems, payment platforms, enterprise accounting applications, authentication systems, and credit-risk databases. Secure gateways authenticated incoming requests, validated transaction integrity, and established protected communication between operational systems and analytical components. At the edge layer, incoming data were subjected to lightweight preprocessing, feature extraction, anomaly screening, fraud-probability estimation, and preliminary risk scoring. High-risk transactions were prioritized for immediate review, whereas lower-risk observations were summarized or processed locally where appropriate. The centralized cloud layer performed computationally intensive tasks such as historical analysis, model training, parameter optimization, long-term storage, and cross-account pattern discovery.

The major responsibilities of each architectural component are summarized in Table 4.

Table 4

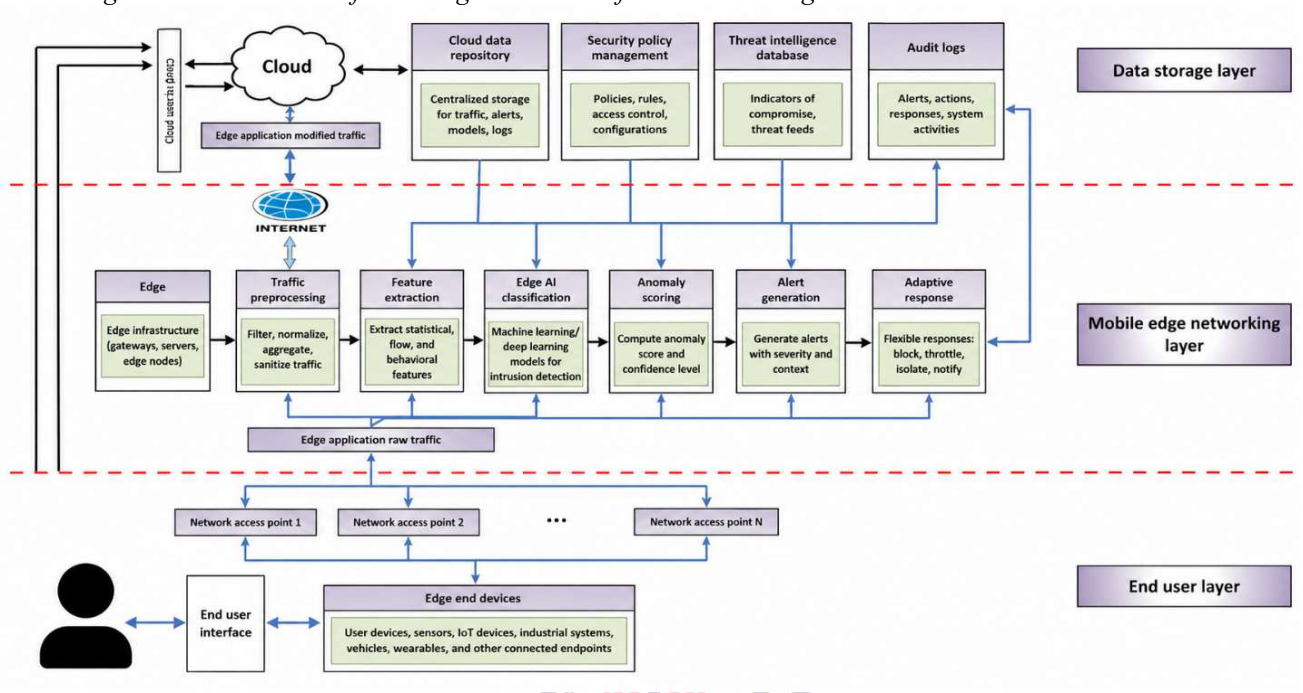
Functional components of the proposed secure edge–cloud financial auditing architecture

Architectural layer	Core functions	Main output
Financial data sources	Generate transactions, accounting, behavioral, device, and credit information	Raw financial events
Secure financial gateway	Authentication, encryption, integrity checking, access control	Validated and protected data stream
Edge intelligence layer	Preprocessing, feature extraction, anomaly detection, fraud scoring	Local fraud and risk indicators
Central cloud analytics	Model training, historical analytics, large-scale forecasting, storage	Updated models and enterprise-wide intelligence
Explainability layer	Feature-level interpretation and risk-factor prioritization	Interpretable alerts
Auditor interface	Alert review, validation, escalation, feedback	Confirmed audit action

The overall data and decision flow is illustrated in Figure 4. Financial transactions first pass through the secure gateway before reaching edge nodes. The edge layer performs immediate analytical screening and generates preliminary fraud and risk scores. High-priority events are transmitted to centralized analytical infrastructure for deeper investigation, while summarized outputs from lower-risk activity can be retained for historical learning and monitoring. Model updates generated by the cloud layer can subsequently be redistributed to authorized edge nodes.

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Figure 4
Secure edge–cloud architecture for intelligent real-time financial auditing.



3.4 Data Preprocessing and Feature Engineering

3.4.1 Missing-Value Treatment. The dataset was reviewed for duplicate observations, incomplete fields, structurally inconsistent records, and implausible values. Particular care was taken not to remove legitimate high-value or unusual transactions simply because they appeared statistically extreme, as such observations may contain important fraud-related information.

3.4.2 Normalization. Numerical features were normalized to ensure consistent scaling across variables. This step is particularly important for machine learning and deep learning models, which can be sensitive to the scale of input features.

3.4.3 Feature Selection. Feature selection was performed to identify the most relevant variables for fraud detection and risk assessment. Given the dataset's richness, feature selection also contributed to computational efficiency, particularly important for edge-based processing where resources may be limited.

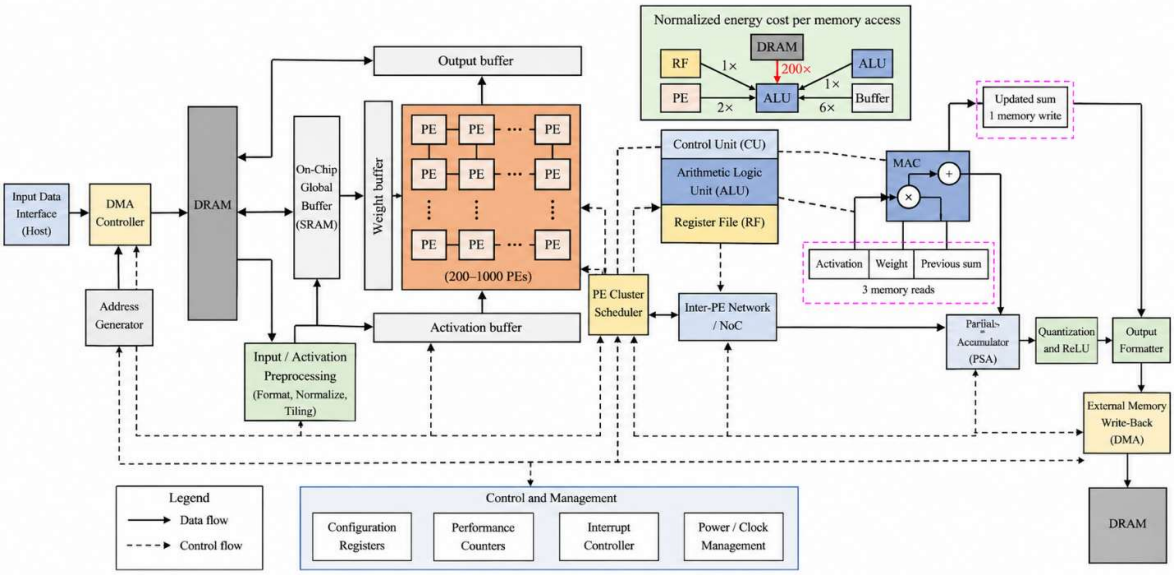
3.4.4 Temporal Segmentation. The data were divided into training, validation, and testing subsets using a 70:15:15 ratio. Temporal segmentation ensured that the model was evaluated on out-of-time data, providing a more realistic assessment of its ability to detect emerging fraud patterns.

3.5 Class Imbalance Correction and Fraud Label Preparation

Financial fraud datasets are typically characterized by substantial class imbalance because legitimate transactions occur far more frequently than confirmed fraudulent events. If this imbalance is not addressed appropriately, a predictive model may become biased toward the majority class and achieve apparently high overall accuracy while failing to detect a sufficient proportion of fraudulent transactions. Fraud labels were derived from confirmed historical audit findings, verified transaction investigations, internal-control reports, and previously validated fraud records. Transactions with sufficient documentary or investigative evidence were assigned to the fraud class, whereas verified routine transactions were classified as legitimate. Suspicious but unconfirmed observations were not automatically treated as fraud because doing so could introduce label noise and reduce model reliability. To reduce majority-class dominance during training, class-balancing procedures were applied only to the training subset. This restriction was important because modifying the validation or testing distributions could create unrealistic performance estimates. The original class distribution was therefore preserved in the validation and test subsets so that the final model was evaluated under conditions closer to real financial operations.

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Figure 5
Fraud-label preparation and class-imbalance correction workflow.



3.6 Real-Time Edge Inference and Fraud Intervention

The real-time edge inference module was designed to analyse incoming financial transactions immediately after basic validation and preprocessing. Rather than forwarding every transaction to a centralized cloud environment for analysis, the trained attention-based model was deployed at distributed edge nodes positioned close to financial transaction sources. Each incoming transaction was first processed through a lightweight edge pipeline consisting of data validation, feature transformation, normalization, and risk-sensitive feature extraction. The processed transaction was then passed to the trained attention-based inference model, which generated a fraud probability together with a preliminary financial-risk score. Relevant contextual information, including transaction velocity, beneficiary novelty, device inconsistency, geographical deviation, failed-login intensity, balance fluctuations, and historical account behaviour, was considered when producing the prediction. A risk-based intervention strategy was applied after inference. Transactions with low predicted risk were allowed to proceed through the normal financial workflow while their summarized analytical outputs were retained for continuous monitoring. Moderate-risk transactions generated monitoring alerts and could be subjected to additional verification. High-risk transactions were immediately escalated for enhanced authentication or auditor review, while critical-risk events could trigger temporary transaction restriction and urgent investigation.

The principal decision levels and corresponding interventions are summarized in Table 5.

Table 5
Real-time edge inference levels and fraud-intervention actions

Risk level	Model interpretation	Edge-level response	Audit or operational action
Low risk	Transaction consistent with expected behavior	Transaction processed normally	Routine monitoring and logging
Moderate risk	Minor behavioral or transactional deviation detected	Additional risk checks performed	Monitoring alert or secondary verification
High risk	Strong combination of fraud-related indicators	Immediate alert generated	Enhanced authentication and auditor review
Critical risk	Very high probability of fraud or severe anomaly	Transaction prioritized or temporarily restricted	Urgent investigation and escalation

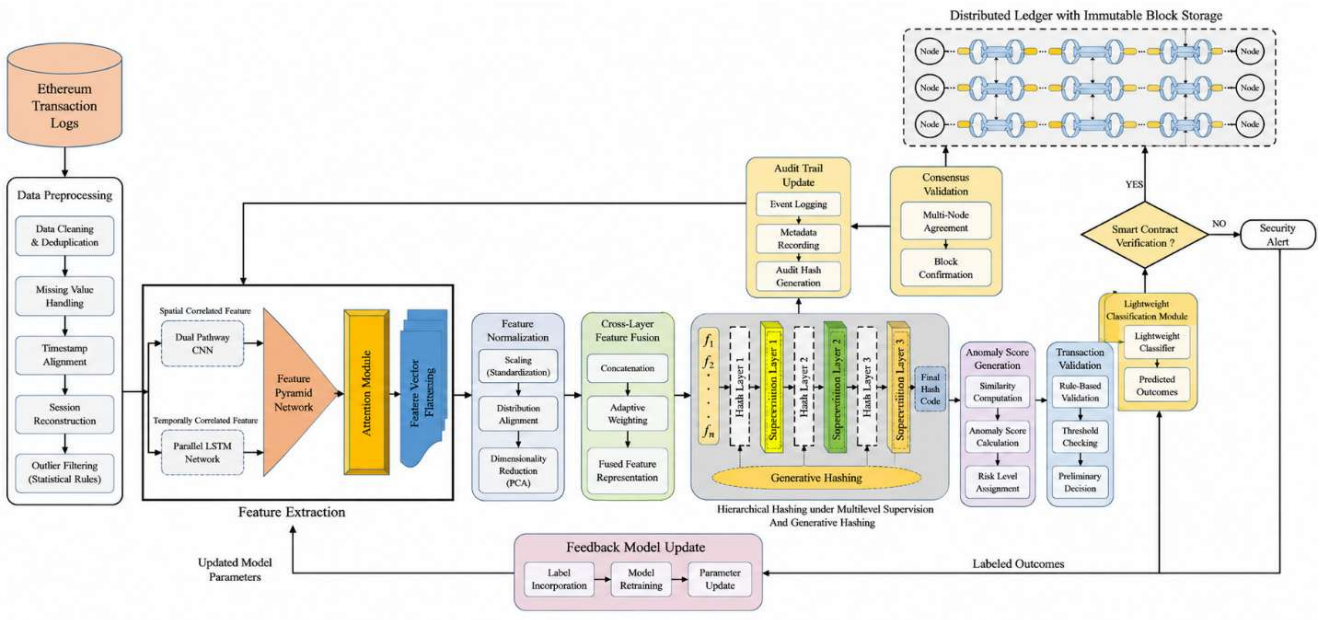
Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Risk level	Model interpretation	Edge-level response	Audit or operational action
Confirmed fraud	High-risk alert validated through investigation	Incident information recorded	Fraud response, audit documentation, and model feedback

The complete inference and intervention workflow is illustrated in Figure 6. Incoming transactions pass through the secure financial gateway before being processed by the edge intelligence layer. The model then evaluates transaction-level and account-level indicators and assigns an appropriate risk category. Intervention intensity increases according to the estimated level of financial risk.

Figure 6

Real-time edge inference and automated fraud-intervention workflow.



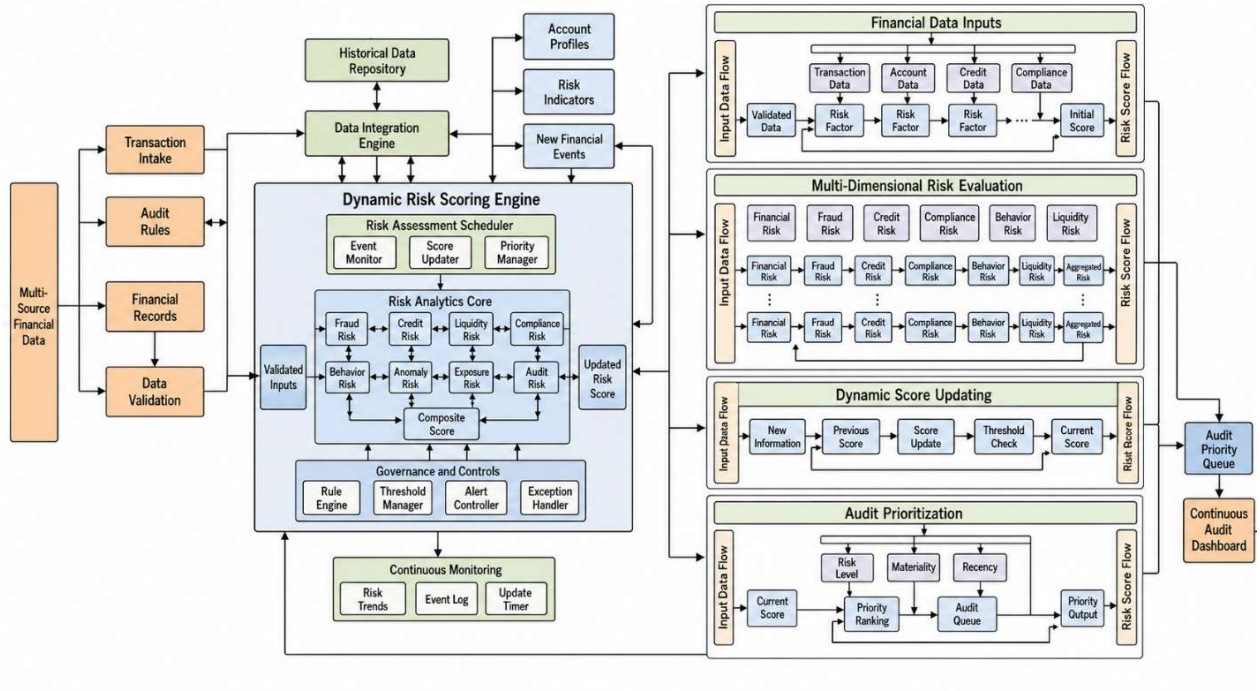
3.7 Dynamic Financial Risk Scoring Framework

The dynamic financial risk scoring framework was developed to convert multiple transaction-level, accounting, behavioural, security, and credit-risk indicators into continuously updated account-level risk profiles. Unlike conventional audit approaches that assign static risk categories at fixed reporting intervals, the proposed framework recalculated financial risk as new information became available. Risk assessment incorporated outputs from both the fraud-detection and predictive accounting modules. Major input indicators included fraud probability, transaction irregularity, payment velocity, beneficiary novelty, cash-flow volatility, liquidity pressure, credit exposure, repayment deterioration, failed-login intensity, device inconsistency, geographical deviation, and previous audit findings. The contribution of these indicators was consolidated into an integrated risk profile that reflected both the probability and potential severity of emerging financial problems. The framework did not depend on any single indicator to determine financial risk. Instead, it combined multiple dimensions so that weak signals occurring simultaneously could collectively elevate the overall risk profile.

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Figure 7

Dynamic financial risk scoring and continuous audit-prioritization framework.



3.8 Data Analysis Technique

The proposed framework utilized the following analytical techniques:

3.8.1 Benchmark Machine Learning Models

- Logistic Regression: Provides a baseline linear classification approach
- Support Vector Machine: Effective for high-dimensional feature spaces
- Random Forest: Ensemble learning for robust classification
- Artificial Neural Network: Deep learning for complex pattern recognition
- XGBoost: Gradient boosting for high-performance classification

3.8.2 Proposed Attention-Based Deep Learning Model. The proposed model incorporates a multi-head self-attention architecture with residual connections and feed-forward processing. The attention mechanism enables the model to dynamically weight the importance of different financial indicators, prioritizing those most relevant for fraud detection and risk assessment.

3.8.3 Model Evaluation Metrics

- **Accuracy:** Proportion of correctly classified observations
- **Precision:** Proportion of positive predictions that are correct
- **Recall:** Proportion of actual positives correctly identified
- **F1-Score:** Harmonic mean of precision and recall
- **ROC–AUC:** Area under the Receiver Operating Characteristic curve

3.8.4 Operational Performance Metrics

- Fraud-detection latency
- Financial-data transmission requirements
- High-risk account identification
- Cash-flow forecasting accuracy (MAPE)
- Emerging risk event detection rate

4. Results and Discussion of the Study

The experimental evaluation demonstrated that the proposed edge computing–enabled intelligent financial auditing framework achieved strong predictive and operational performance across fraud detection,

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

predictive accounting analytics, and financial risk assessment. The framework was evaluated using the held-out testing subset after model training and validation under the predefined 70:15:15 temporal data partition. Its performance was compared with logistic regression, support vector machine, random forest, artificial neural network, and XGBoost to determine whether the proposed edge-enabled attention architecture offered measurable advantages over conventional statistical, machine-learning, and deep-learning approaches.

The comparative results presented in Table 6 show that the proposed model achieved the highest performance across all principal fraud-detection metrics. The model produced 97.4% accuracy, 96.8% precision, 97.1% recall, a 96.9% F1-score, and a ROC–AUC of 0.991. Among the benchmark models, XGBoost achieved the strongest performance, with 94.6% accuracy and a ROC–AUC of 0.967, followed by the artificial neural network and random forest. Logistic regression generated the lowest overall performance, indicating the limited ability of simpler linear models to capture the complex and nonlinear relationships present in multidimensional financial data.

Table 6

Comparative fraud-detection performance of benchmark and proposed models

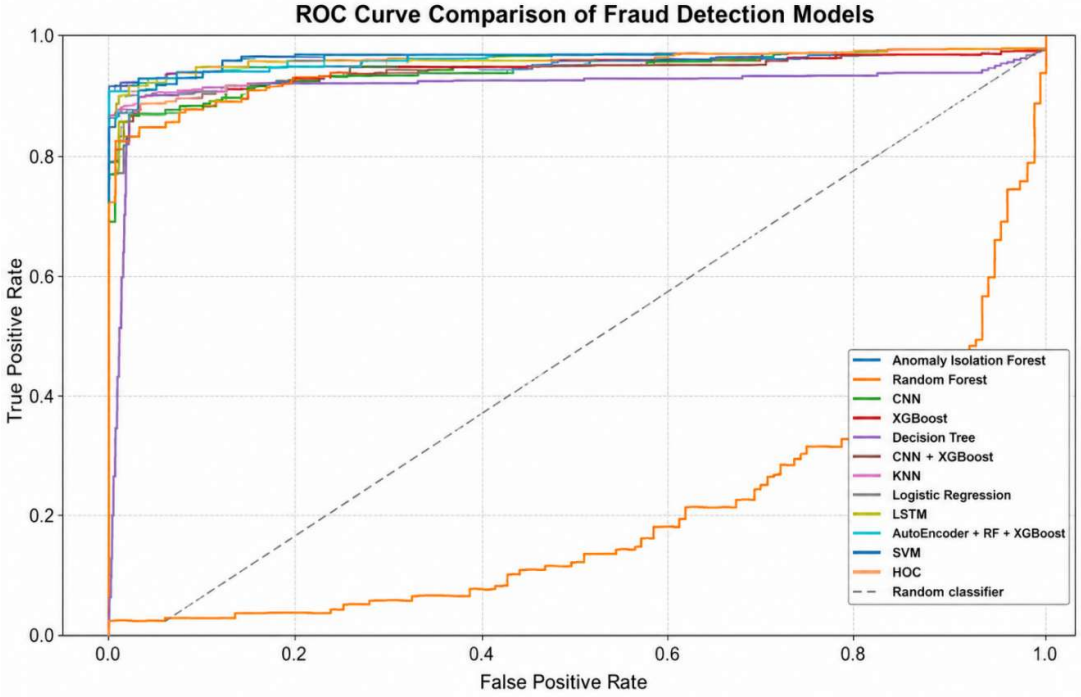
Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	ROC–AUC
Logistic Regression	84.9	82.7	81.9	82.3	0.873
Support Vector Machine	89.7	88.6	87.8	88.2	0.918
Random Forest	92.8	92.1	91.4	91.7	0.949
Artificial Neural Network	93.7	93.0	92.6	92.8	0.958
XGBoost	94.6	94.0	93.8	93.9	0.967
Proposed Edge-Enabled Attention Model	**97.4**	**96.8**	**97.1**	**96.9**	**0.991**

The comparatively high recall of the proposed model is particularly significant in financial auditing because missed fraudulent transactions may result in substantial financial loss, regulatory exposure, and reputational damage. At the same time, the precision value of 96.8% indicates that the improved sensitivity was not achieved by generating an excessive volume of false alerts. The balanced precision, recall, and F1-score suggest that the model can provide strong fraud-detection capability while avoiding unnecessary investigation workload (Mollah, 2026). The comparative accuracy and ROC–AUC results are further illustrated in Figure 8. The progression from conventional statistical modelling toward ensemble learning and deep-learning techniques demonstrates that more advanced methods were increasingly effective in capturing heterogeneous financial risk patterns. The proposed edge-enabled attention model exceeded XGBoost by 2.8 percentage points in classification accuracy, while the ROC–AUC increased from 0.967 to 0.991.

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Figure 8

Comparative accuracy and ROC–AUC performance of benchmark and proposed fraud-detection models.



The strongest performance was obtained when attention-based learning was combined with the multidimensional financial feature space. This improvement can be attributed to the ability of the attention mechanism to prioritize particularly informative indicators such as unusual transaction amounts, payment velocity, beneficiary novelty, failed-login frequency, device inconsistency, geographical deviation, cash-flow volatility, credit exposure, and historical audit findings. Instead of giving identical importance to every variable, the proposed model selectively emphasized combinations of indicators that were most strongly associated with fraudulent or high-risk activity (Nawaz & Musah, 2025). The operational evaluation also demonstrated a substantial advantage for edge-based processing. The centralized auditing configuration required an average of 2.84 seconds to generate a fraud classification, whereas the proposed edge-enabled architecture reduced average fraud-detection latency to 0.41 seconds. This represents an approximate 85.6% reduction in detection latency. The improvement occurred because preprocessing, feature extraction, and model inference were performed closer to transaction sources rather than waiting for complete data transfer to centralized infrastructure. The operational comparison is presented in Table 7.

Table 7

Operational performance of centralized and edge-enabled financial auditing

Performance indicator	Centralized auditing	Proposed edge-enabled auditing	Improvement
Average fraud-detection latency	2.84 s	0.41 s	85.6% reduction
Relative data-transmission requirement	100%	61.3%	38.7% reduction
High-risk account identification	Baseline	+21.6%	Improved
Real-time intervention capability	Limited	High	Substantially improved
Local fraud screening	No	Yes	Enabled
Priority-based escalation	Limited	Integrated	Improved

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

The latency reduction is operationally important because modern digital financial transactions can occur within fractions of a second and fraudulent funds may be rapidly transferred across multiple accounts. A system that identifies suspicious behavior several seconds after a transaction has been completed may have limited intervention capability. By reducing average detection time to 0.41 seconds, the proposed architecture provides a stronger basis for immediate risk screening, transaction verification, alert escalation, and potential intervention. The edge-enabled architecture also reduced financial-data transmission requirements by 38.7% compared with the centralized configuration. Rather than forwarding all raw transaction records to centralized servers, edge nodes performed local screening and selectively transmitted higher-value analytical information, including anomaly indicators, fraud probabilities, risk scores, and suspicious transaction summaries. This approach improved communication efficiency while reducing unnecessary movement of sensitive financial information. The reduction in data transmission has implications beyond network efficiency. Financial records frequently contain highly sensitive information related to customer activity, account history, payment behavior, authentication events, and credit exposure. Processing selected information locally reduces the amount of raw data continuously moving across networks and can therefore support more privacy-aware financial auditing (Akinsanya et al., 2023). At the same time, centralized infrastructure remains essential for historical analysis, long-term storage, model retraining, and cross-account pattern recognition.

Figure 9

Comparative Fraud-Risk Scoring Performance of New and Traditional FICO Falcon CNP Technologies

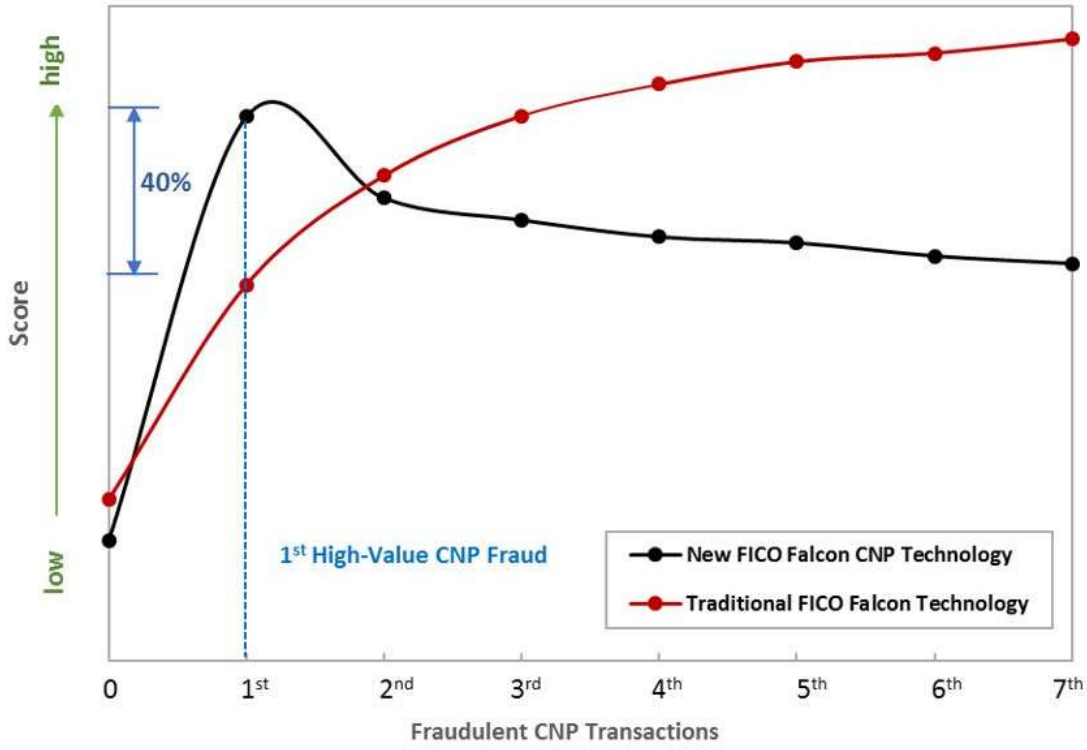


Figure 9 compares risk scores across successive fraudulent card-not-present (CNP) transactions. The new FICO Falcon technology produces a substantially higher score at the first high-value fraud event approximately 40% above the traditional system supporting earlier fraud detection. Although its score gradually declines after the initial peak, the traditional technology increases more slowly and reaches high-risk scores only after multiple fraudulent transactions. The results therefore support a collaborative edge–cloud model rather than a complete replacement of centralized computing. Another important outcome was the 21.6% improvement in high-risk account identification compared with the centralized baseline. This improvement was achieved through the integration of fraud probabilities, accounting abnormalities,

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

behavioral deviations, credit exposure, repayment deterioration, security indicators, and historical audit findings into the dynamic financial risk-scoring process. The results suggest that account-level risk cannot always be assessed adequately through isolated transaction anomalies. A transaction may appear only moderately unusual when viewed independently, but its significance can increase when the associated account simultaneously exhibits cash-flow deterioration, unusual device activity, repeated failed logins, or historical control exceptions.

The predictive accounting analytics engine also produced encouraging results. Cash-flow forecasting achieved a mean absolute percentage error of 6.8%, indicating relatively low average forecasting deviation. Forecasting was based on historical inflows and outflows, account balances, transaction frequencies, cash-flow volatility, receivable and payable movements, repayment behaviour, and credit exposure. The ability to generate forward-looking financial information expands the auditing function beyond retrospective anomaly identification and allows the framework to support proactive assurance. The principal predictive accounting and financial-risk outcomes are summarized in Table 8.

Table 8

Predictive Accounting and Financial-Risk Assessment Performance

Analytical task	Evaluation indicator	Result
Cash-flow forecasting	Mean Absolute Percentage Error	6.8%
Emerging financial-risk detection	Events identified before critical threshold	93.5%
High-risk account identification	Improvement over centralized baseline	21.6%
Financial-data transmission	Reduction	38.7%
Fraud-detection latency	Edge-processing time	0.41 s

The predictive engine further identified 93.5% of emerging financial-risk events before critical thresholds were reached. These events were recognized through changes in cash-flow volatility, transaction intensity, liquidity pressure, repayment behaviour, balance fluctuations, credit exposure, authentication anomalies, and other risk-sensitive signals. Rather than waiting until a predefined limit had already been exceeded, the framework evaluated the direction and combination of multiple indicators to identify deteriorating financial conditions earlier. This result is particularly relevant to continuous financial auditing because it demonstrates the value of combining predictive accounting with fraud detection. Traditional auditing primarily verifies completed transactions and historical financial records, whereas the proposed framework also provides information about expected future conditions.

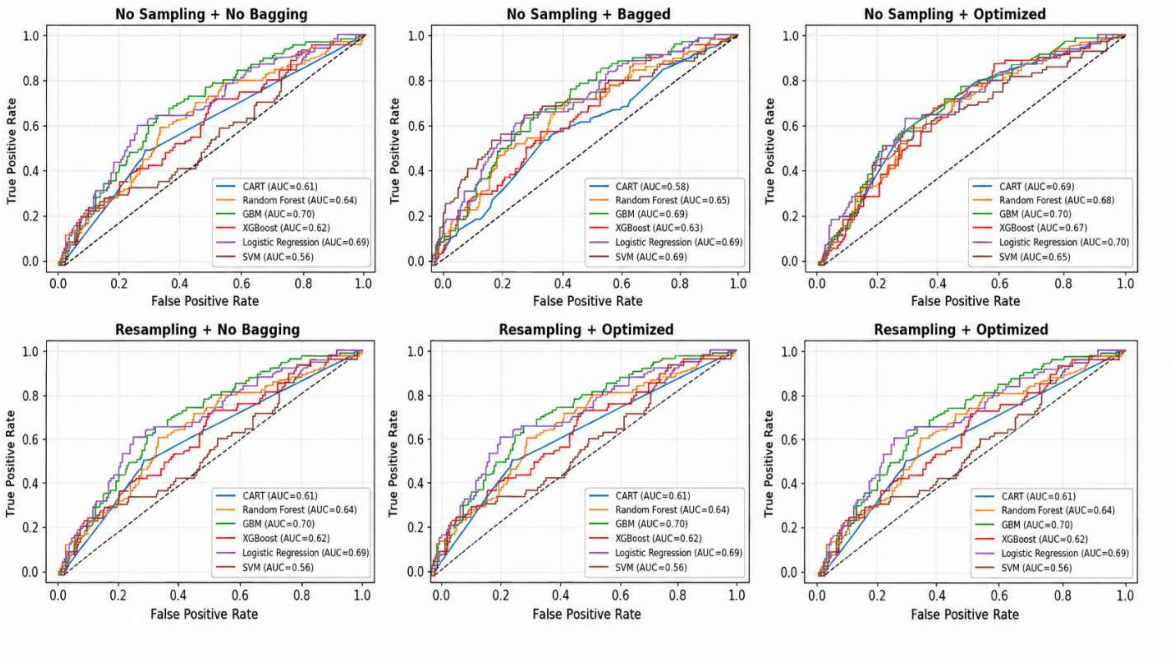
Early-warning capability can help financial institutions initiate additional monitoring, request documentation, adjust credit exposure, strengthen internal controls, or begin targeted investigation before a financial problem develops into a critical event. Explainable artificial intelligence also contributed to the practical usefulness of the proposed framework. High-risk classifications were accompanied by information on the principal variables contributing to each decision. Important factors frequently included transaction amount deviation, rapid payment velocity, unusual beneficiary activity, device inconsistency, failed-login intensity, geographical deviation, cash-flow volatility, deteriorating repayment behaviour, and previous audit findings (Kalaiselvi, 2026). This feature-level interpretation allowed automated predictions to be connected with understandable financial evidence.

Explainability is particularly important in auditing because a highly accurate model cannot be relied upon solely as a black-box decision system. Auditors need to understand why a particular transaction or account has been classified as high risk before initiating corrective action. The human-in-the-loop component therefore allowed auditors to confirm alerts, identify legitimate exceptions, request further investigation, or escalate potentially material cases. Auditor validation also provided feedback that could later support model recalibration and refinement. The integrated results of the proposed framework are summarized in Figure 10. The results demonstrate benefits across predictive accuracy, operational efficiency, accounting forecasting, risk prioritization, and audit transparency rather than improvement in only a single performance dimension.

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Figure 10

ROC Comparison of Machine-Learning Models Under Different Sampling, Bagging, and Optimization Settings



The experimental findings demonstrate that the primary contribution of the proposed framework lies in the integration of several complementary capabilities. Strong fraud-classification performance was combined with low-latency edge inference, reduced communication requirements, predictive accounting intelligence, dynamic risk scoring, and interpretable auditor decision support. This combination provides a more comprehensive approach than systems that focus exclusively on fraud-classification accuracy. The superiority of the proposed model over the benchmark algorithms indicates that complex financial irregularities are more effectively detected when nonlinear learning is combined with selective attention to important financial signals. The strong recall and ROC–AUC values demonstrate that the model can discriminate effectively between legitimate and fraudulent observations, while the high precision suggests that this sensitivity does not create an excessive number of irrelevant alerts.

The operational findings further demonstrate that model architecture and computational deployment are equally important. A highly accurate fraud detector may provide limited practical value if processing delays prevent timely intervention. The reduction from 2.84 seconds to 0.41 seconds confirms that placing inference closer to transaction sources can substantially increase responsiveness. Similarly, the 38.7% reduction in data transmission demonstrates that intelligent edge filtering can improve communication efficiency while supporting privacy-aware financial-data processing.

The results of the predictive accounting component indicate that intelligent auditing can also provide meaningful forward-looking capabilities. The 6.8% cash-flow forecasting error and 93.5% early detection of emerging risk events demonstrate the potential for auditors to identify deteriorating financial conditions before they become critical (Brinkkemper, 2026). This capability transforms the auditing process from a predominantly retrospective control activity into a more proactive financial assurance mechanism. The 21.6% increase in high-risk account identification further highlights the importance of dynamic rather than static risk assessment. Financial risk profiles change continuously as new transactional, accounting, behavioural, and credit information becomes available. A dynamic scoring process can therefore provide a more realistic representation of current risk and improve audit resource allocation by directing professional attention toward accounts requiring the greatest level of investigation. The findings confirm that combining edge computing, attention-based deep learning, predictive accounting analytics, dynamic risk scoring, explainable artificial

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

intelligence, and human-in-the-loop validation can strengthen the effectiveness of modern financial auditing. The proposed framework achieved higher predictive performance than the benchmark models while simultaneously reducing detection latency and communication requirements (Dash et al., 2026). Its ability to forecast financial conditions, identify emerging risks, and provide interpretable alerts further supports its potential application in banks, accounting organizations, financial institutions, and audit firms seeking continuous, responsive, and proactive financial assurance.

5. Conclusion and Recommendations

This study developed an edge computing–enabled intelligent financial auditing framework designed to support real-time fraud detection, predictive accounting analytics, and dynamic financial risk assessment. By integrating distributed edge processing, secure financial gateways, attention-based deep learning, predictive analytics, explainable artificial intelligence, and human-in-the-loop validation, the framework was designed to overcome important limitations of conventional centralized and periodically executed auditing systems. The proposed approach shifts financial auditing toward a more continuous, proactive, and data-driven model in which suspicious activity can be identified and evaluated closer to the point of transaction generation. The framework was evaluated using a multi-institutional dataset containing 285,000 anonymized financial transactions from 18,750 individual and corporate accounts over a three-year period. The dataset incorporated 46 transactional, accounting, behavioural, device, network, and credit-risk variables, providing a multidimensional representation of financial activity.

Comparative evaluation against logistic regression, support vector machine, random forest, artificial neural network, and XGBoost demonstrated the effectiveness of the proposed edge-enabled attention-based model. The framework achieved 97.4% accuracy, 96.8% precision, 97.1% recall, a 96.9% F1-score, and a ROC–AUC of 0.991, outperforming the strongest benchmark model. Beyond predictive accuracy, the proposed architecture demonstrated substantial operational advantages. Edge-based processing reduced average fraud-detection latency from 2.84 seconds to 0.41 seconds and lowered financial-data transmission requirements by 38.7% compared with centralized auditing. High-risk account identification improved by 21.6%, demonstrating the value of combining real-time transaction analysis with dynamic risk prioritization. The predictive accounting component also achieved a mean absolute percentage error of 6.8% for cash-flow forecasting and identified 93.5% of emerging financial-risk events before critical thresholds were reached. A major contribution of the framework is the integration of fraud detection with forward-looking accounting intelligence and continuous financial-risk assessment.

Instead of treating fraud classification, accounting forecasting, and risk monitoring as separate analytical processes, the proposed architecture combines their outputs within a unified audit environment. Explainable risk indicators and feature-level alerts further improve transparency by enabling auditors to understand the principal factors contributing to high-risk classifications. Human-in-the-loop validation preserves professional oversight and provides a mechanism for reviewing, confirming, or rejecting automated predictions. The findings indicate that edge computing can significantly strengthen intelligent financial auditing by improving response speed, reducing unnecessary data movement, and enabling rapid risk assessment without eliminating the analytical advantages of centralized cloud infrastructure. The collaborative edge–cloud architecture therefore provides an effective balance between low-latency inference, large-scale model training, historical analysis, security, and operational scalability (Khan et al., 2026).

Future research can extend the proposed edge computing–enabled intelligent financial auditing framework in several important directions. First, larger and more geographically diverse multi-institutional datasets should be used to evaluate the generalizability of the framework across different banking systems, accounting environments, transaction channels, regulatory settings, and customer populations. Incorporating cross-border payments, digital wallets, open-banking transactions, cryptocurrency-related activity, and real-time enterprise accounting records could further improve the ability of the system to recognize emerging and previously unseen financial-risk patterns. Second, future studies should investigate more advanced learning architectures capable of modelling complex temporal and relational dependencies among financial entities. Transformer-based models, temporal graph neural networks, graph attention networks, and hybrid deep-

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

learning architectures could be integrated to analyse relationships among accounts, beneficiaries, merchants, devices, transactions, and organizational entities (Alatawi, 2025).

Such models may improve the identification of coordinated fraud, money-movement networks, collusive activity, and multi-account financial anomalies that cannot be detected effectively through transaction-level analysis alone. Another important direction involves privacy-preserving distributed learning. Federated learning could enable several financial institutions to collaboratively improve fraud-detection and risk-assessment models without transferring complete customer-level datasets to a centralized location. This approach could be combined with secure aggregation, differential privacy, encryption, and trusted edge environments to strengthen confidentiality while maintaining cross-institutional learning capabilities (Darwish et al., 2026). Future research should evaluate the trade-offs among privacy protection, computational overhead, communication cost, and predictive performance. The edge infrastructure itself should also be examined under more realistic operational conditions (Khan et al., 2025). Future experiments could evaluate model performance under variable transaction loads, temporary network failures, limited edge-device resources, cyberattacks, model-update delays, and rapidly changing fraud patterns. Adaptive workload allocation between edge and cloud environments could be developed so that computational tasks are dynamically assigned according to latency requirements, network availability, risk severity, and resource utilization.

Further work is also required to strengthen model explainability and auditor interaction. Future systems could provide case-specific explanations, counterfactual scenarios, visual risk trajectories, and evidence-based recommendations that allow auditors to understand not only why an alert was generated but also what changes would reduce the predicted risk. Auditor feedback could be incorporated through active learning so that professional decisions continuously improve the model and reduce repeated false-positive alerts. The predictive accounting component can be expanded beyond cashflow forecasting to include revenue prediction, liquidity stress estimation, credit deterioration, earnings-quality assessment, bankruptcy risk, working-capital forecasting, and early identification of material misstatement. Integrating external economic variables, market conditions, interest-rate movements, sector-level indicators, and macroeconomic uncertainty may further improve the accuracy of forward-looking financial-risk assessment. Future research should additionally investigate concept drift and adversarial adaptation. Fraud strategies evolve continuously, meaning that models trained on historical data may gradually lose effectiveness (Garg & Mishra, 2026). Online learning, continuous model recalibration, drift-detection mechanisms, and adaptive threshold selection could enable the framework to respond more effectively to new financial behaviours and emerging fraud techniques. Finally, large-scale real-world deployment studies are needed to assess the framework from technical, organizational, regulatory, and economic perspectives. Future evaluations should measure not only classification accuracy but also financial loss prevention, false-alert reduction, auditor workload, investigation time, compliance efficiency, infrastructure cost, energy consumption, and return on investment. Such extensions would provide stronger evidence regarding the long-term feasibility of edge-enabled intelligent auditing and support its transition from experimental research toward secure, scalable, and continuously adaptive financial assurance systems.

Author Contributions

All authors participated in ideation, development, and writing the manuscript. All authors read and approved the final manuscript.

Conflict of Interest Statement

The authors declare that there is no conflict of interest regarding the publication of this article.

Funding Statement

The authors did not receive financial support from any funding agency or external organization for the research, authorship, or publication of this article.

Informed Consent

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Not applicable. This study did not involve human participants requiring informed consent. The data used in this research were obtained from anonymized financial records with all personally identifiable information removed. No private or sensitive information was collected from individuals.

Data Availability

The datasets generated and analysed during the current study are available from the corresponding author upon reasonable request. Due to privacy and confidentiality considerations, raw financial data may not be publicly distributed but can be accessed through the corresponding author with appropriate data use agreements and institutional approvals. The authors are committed to transparency and will provide detailed methodological information, model specifications, and analysis protocols upon request.

References

Ahmad, B., Ali, S., Muneer, M., Fatima, A., & Abbas, N. (2025). Wind energy integration into the SAARC region: A comprehensive review of optimal wind sites for a sustainable super smart grid. *Dialogue Social Science Review, 3*(2), 488–515. https://doi.org/10.5281/zenodo.20999213

Ahmad, B., Jillani, S. A., Rafique, M., & Soomro, A. A. (2026). Design and monitoring of a tree-inspired vertical axis wind turbine for efficient urban wind utilization. In *2026 1st International Conference on Innovations in Information and Communication Technologies (IICT)* (pp. 1–6). IEEE. https://doi.org/10.1109/IICT68374.2026.11468465

Ahmad, B., Majeed, M. K., Soomro, A. A., & Jillani, S. A. (2026). Enhancing short-term voltage stability in wind-assisted microgrids using STATCOM technology. In *2026 1st International Conference on Innovations in Information and Communication Technologies (IICT)* (pp. 1–6). IEEE. https://doi.org/10.1109/IICT68374.2026.11468707

Akter, M. S. (2025). AI-enhanced financial information systems for real-time fraud detection and cash flow optimization in US logistics and retail sectors. *American Journal of Scholarly Research and Innovation, 4*(1), 813–855.

Al Montaser, M. A., & Bannett, M. (2025). Beyond anomaly detection: Redesigning real-time financial fraud systems for multi-channel transactions in emerging markets. *Baltic Journal of Multidisciplinary Research, 2*(3), 1–17.

Alatawi, M. N. (2025). EdgeGuard-IoT: 6G-enabled edge intelligence for secure federated learning and adaptive anomaly detection in Industry 5.0. *Computers, Materials & Continua, 85*(1), 695–727. https://doi.org/10.32604/cmc.2025.066606

Akinsanya, M. O., Bello, A. B., & Adeusi, O. C. (2023). A comprehensive review of edge computing approaches for secure and efficient data processing in IoT networks. *Communication in Physical Sciences, 9*(4), 870–877.

Alves, J. F. R. M. (2025). Privacy-aware explainable AI framework for multi-modal big data analytics in real-time payment fraud detection and pharmaceutical network intelligence. *International Journal of Research and Applied Innovations, 8*(Special Issue 1), 86–95.

Amirineni, S., & Abhilash, K. S. (2025). AI-driven fraud detection in IoT-enabled payment ecosystems: Challenges, hybrid edge-cloud framework, and emerging trends. In *2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 1406–1413). IEEE. https://doi.org/10.1109/ICESC65114.2025.11212351

Aroh, I. (2025). Developing explainable AI-enabled edge cloud framework for financial analytics and intelligent risk governance. *International Journal of Science, Research and Technology, 8*(6), 15431–15439.

Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. *European Journal of Computer Science and Information Technology, 11*(6), 84–102.

Brinkkemper, S. (2026). Intelligent cloud-native financial analytics frameworks for fraud detection risk prediction and autonomous governance systems. *International Journal of Computer Technology and Electronics Communication, 9*(3), 1080–1095.

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Burugulla, J. K. R. (2024). The future of digital financial security: Integrating AI, cloud, and big data for fraud prevention and real-time transaction monitoring in payment systems. *MSW Management Journal, 34*(2), 711–730.

Darwish, S. M., El-Naggar, S., & Elkaffas, S. M. (2026). Securing financial transactions: Exploring the role of lightweight blockchain-enabled deep learning for fraud detection in FinTech systems. *Cybersecurity, 9*(1), Article 8. https://doi.org/10.1186/s42400-025-00436-8

Dash, A., Samantray, B. S., Reddy, K. H. K., Amin, F., & Mishra, S. K. (2026). *A secure framework for smart waste management using IoT, machine learning, and blockchain*. In *2026 1st International Conference on Emerging Trends in Advancements and Applications of Computational Intelligence Techniques (ETAACT)* (pp. 1-7). IEEE. https://doi.org/10.1109/ETAACT69135.2026.11541497

Fonkem, B. N. (2025). AI-powered risk scoring models for real-time fraud detection in digital banking ecosystems. *Journal of Computational Analysis and Applications, 34*(11), 349–371.

Garg, V., & Mishra, G. (2026). Smart financial surveillance: Blockchain and explainable AI for fraud detection in smart healthcare organizations. In *Blockchain solutions for securing Internet of Things networks* (pp. 225–266). Wiley. https://doi.org/10.1002/9781394417131.ch9

Gkegkas, M., Kydros, D., & Pazarskis, M. (2025). Using data analytics in financial statement fraud detection and prevention: A systematic review of methods, challenges, and future directions. *Journal of Risk and Financial Management, 18*(11), Article 598. https://doi.org/10.3390/jrfm18110598

Hasibuan, A. A., & Nasution, M. I. (2025). The impact of real-time and continuous auditing on financial transparency and fraud detection: A systematic literature review. In *Proceedings of International Conference on Islamic Community Studies* (pp. 415–428).

Ikeh, C. O. (2025). Hybrid AI frameworks for real-time fraud detection in cross-border digital payment ecosystems. *International Journal of Advance Research Publication and Reviews, 2*(5), 21–44. https://doi.org/10.5281/zenodo.15386508

Kalaiselvi, R. (2026). Explainable AI models for cloud-based fraud detection risk assessment and secure financial decision intelligence. *International Journal of Technology, Management and Humanities, 12*(2), 35–46.

Khan, A., Amin, F., & Imtiaz, U. (2026). *SecurePulse-GRID: Trust-aware predictive load balancing and rapid cyber containment in distributed smart microgrids*. *The Asian Bulletin of Big Data Management, 6*(1), 697-708. https://doi.org/10.62019/smxj7m37

Khan, A., Imtiaz, U., & Amin, F. (2025). *Honeytoken-augmented AI model for insider threat detection using cyber deception and isolation forest*. *Kashf Journal of Multidisciplinary Research, 2*(9), 294-313. https://doi.org/10.71146/kjmr625

Khan, I., Japa, C., Muthukumarasamy, K., & Gadam, H. (2025). Real-time financial fraud detection with cognitive 6G networks and distributed AI autonomous risk management. *Advances in Consumer Research, 2*, 4063–4072.

Lambropoulos, G., Mitropoulos, S., & Douligeris, C. (2026). Emerging technologies in financial services: From virtualization and cloud infrastructures to edge computing applications. *Computers, 15*(1), Article 41. https://doi.org/10.3390/computers15010041

Mollah, M. A. R. (2026). AI-driven business intelligence for real-time fraud risk monitoring in digital payment platforms: A framework-based review. *International Journal of Scientific Interdisciplinary Research, 7*(1), 527–580. https://doi.org/10.63125/0ef34271

Moreau, A. L. (2025). AI-enabled real-time financial fraud detection and encryption impact analysis in high-performance cloud-based enterprise networks. *International Journal of Computer Technology and Electronics Communication, 8*(6), 11763–11770. https://doi.org/10.15680/IJCTECE.2025.0806021

Naaz, J., Patel, H., & Syed, Z. (2026). Cloud-native event-driven orchestration architecture for real-time fraud and sanctions screening. *American International Journal of Computer Science and Technology, 8*(4), 12–24. https://doi.org/10.63282/3117-5481/AIJCST-V8I4P102

Journal of Business Insight and Innovation
Volume 5 Issue 5, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Nawaz, Y., & Musah, M. (2025). *Enhancing FinTech security and efficiency: A unified framework for real-time fraud detection using deep neural networks*. https://doi.org/10.13140/RG.2.2.11842.29126

Nofel, M., Marzouk, M., Elbardan, H., Saleh, R., & Mogahed, A. (2024). From sensors to standardized financial reports: A proposed automated accounting system integrating IoT, blockchain, and XBRL. *Journal of Risk and Financial Management, 17*(10), Article 445. https://doi.org/10.3390/jrfm17100445

Nowak, A. M. (2022). Secure AI-enabled cloud platforms for healthcare image analysis and financial fraud detection across web applications and 5G networks. *International Journal of Engineering & Extended Technologies Research (IJEETR), 4*(5), 5333–5341.

Pan, X. (2025). Detection and compliance in financial management via 6G-enabled standardized AI-powered digital twins. *IEEE Communications Standards Magazine*.

Prabha, M., Nandhini, S., Dayanidhy, M., & Pradeep, R. (2025). Edge-AI integrated secure wireless IoT architecture for real-time healthcare monitoring and federated anomaly detection. *Scientific Reports, 16*(1), 574.

Rajput, A., & Katamba, I. (2024). Leveraging artificial intelligence and big data in public accounting: Redefining audit practices and financial reporting. *International Journal of Research Publication and Reviews, 5*(11), 5516–5531. https://doi.org/10.55248/gengpi.5.1124.3341

Ramli, A. I. B. (2024). Big data and artificial intelligence to develop advanced fraud detection systems for the financial sector. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, 8*(12), 31–44.

Sethupathy, U. K. A. (2025). Risk-aware AI models for financial fraud detection: Scalable inference from big transactional data. *International Journal of Intelligence Science, 15*(4), 162–183. https://doi.org/10.4236/ijis.2025.154009

Singh, D. (2025). Explainable graph-based AI for real-time fraud detection in distributed healthcare claims processing systems. *International Journal of Science, Technology and Convergence, 7*(7).

Timileyin, O. (2026). *Secure edge AI frameworks for real-time fraud detection in financial and digital banking systems*.

Zakaria, R. M., Rahman, M. M., Rahman, H., Rafi, M. A., Minto, A., Hossain, M. S., & Saimon, S. I. (2025). Detecting financial fraud in real-time transactions using graph neural networks and anomaly detection techniques. *Journal of Economics, Finance and Accounting Studies, 7*(6), 1–13. https://doi.org/10.32996/jefas.2025.7.6.1

Zhong, H., Yang, D., Shi, S., Wei, L., & Wang, Y. (2024). From data to insights: The application and challenges of knowledge graphs in intelligent audit. *Journal of Cloud Computing, 13*(1), Article 114. https://doi.org/10.1186/s13677-024-00674-0

Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial Internet of Things–edge computing integration: Challenges, threats, and future directions. *Sensors, 25*(1), Article 213. https://doi.org/10.3390/s25010213