International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 2, Mar-Apr 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Adaptive Zero Day Fraud Detection in Digital Banking

Subake M*, Joshua Koil Sahayam G**, Anto Sajin T***, Selva Kumar M****, Siddarth K V*****
*(Department of Information Technology, Loyola Institute of Technology and Science, Thovalai)

----------**********----------

Abstract:

The rapid growth of digital banking services has resulted in a massive increase in real-time financial transactions, creating new opportunities for innovation while simultaneously introducing advanced cybersecurity risks. Among these risks, zero-day fraud attacks represent a major challenge because they involve previously unseen patterns that traditional rule-based fraud detection systems cannot effectively identify. This research focuses on developing an adaptive fraud detection framework using machine learning-based anomaly detection combined with behavioral analytics to detect unknown fraud activities in real time. The proposed system builds dynamic behavioral profiles for individual users by analyzing historical transaction data, including transaction amount, time patterns, geographical location, device usage, login behavior, and spending habits. Machine learning algorithms learn normal behavioral patterns and continuously monitor new transactions to identify deviations that may indicate suspicious activity. Unlike conventional signature-based approaches, anomaly detection models such as Isolation Forest, Autoencoders, and One-Class classification techniques enable the identification of novel fraud strategies without requiring predefined fraud rules or labeled attack datasets. Key advantages include scalability for high-volume financial data, early detection of emerging threats, reduced dependency on manual rule updates, and enhanced customer protection.

Keywords — Zero-day fraud, Digital banking, Machine learning, Anomaly detection, Behavioral analytics, Isolation Forest, Autoencoders, Explainable AI.

----------**********----------

I. Introduction

Digital banking has transformed financial services by enabling fast, convenient, and secure transactions through online banking platforms, mobile applications, UPI payments, and digital wallets. As the volume of electronic transactions increases daily, banking systems have become prime targets for cyber fraud and financial attacks. Among these threats, zero-day fraud poses a significant challenge because it involves new and previously unknown attack methods that do not match existing fraud patterns, making traditional rule-based detection systems less effective.

To address this challenge, adaptive zero-day fraud detection systems leverage Artificial Intelligence (AI) and Machine Learning (ML) techniques to analyze real-time transaction data and understand normal user behavior patterns. These systems build behavioral profiles using factors such as transaction frequency, location, device information, and spending habits. Each incoming transaction is evaluated instantly against learned patterns to identify unusual or abnormal activities. By using anomaly detection and continuous learning mechanisms, the system can detect suspicious transactions even without prior knowledge of specific fraud types.

When anomalies are identified, the system can automatically flag, monitor, or block potentially fraudulent activities, improving security and reducing financial risks. This intelligent approach enhances fraud detection accuracy, enables real-time response, and provides a proactive solution for securing modern digital banking environments.

II. Problem Statement

The rapid growth of digital banking has increased the complexity and frequency of fraud attacks, creating significant challenges for traditional fraud detection systems. New and unknown fraud attacks, commonly known as zero-day fraud, cannot be effectively detected using conventional rule-based approaches because these systems rely on

predefined patterns and historical attack signatures. Additionally, fraud techniques evolve rapidly, often faster than security rule updates, making traditional methods insufficient for modern banking environments.

Existing fraud detection systems frequently generate high false alerts, which leads to operational inefficiencies and poor user experience. Moreover, delayed detection of fraudulent transactions may result in substantial financial losses and reduced customer trust. Therefore, there is a strong need for a smart, adaptive, and real-time fraud detection system that can learn user behavior patterns, identify anomalies, and respond proactively to emerging fraud threats.

III. Existing System

A. Overview

Traditional fraud detection systems mainly rely on rule-based or signature-based approaches to identify fraudulent activities in digital banking transactions. These systems use predefined rules, thresholds, and known fraud patterns to monitor transactions and detect suspicious behavior. Since fraudsters continuously develop new strategies, rule-based systems often struggle to keep up with changing attack patterns. Another limitation is the use of fixed thresholds, which may not accurately reflect individual user behavior, leading to high false positive rates. Additionally, updating rules requires manual intervention, making the system less adaptive and slower to respond to emerging threats.

B. Disadvantages

- Rely on rule-based or signature-based methods; fail to identify new or unknown (zero-day) fraud attacks.
- Fixed thresholds do not adapt to individual user behavior, leading to inaccurate fraud detection.
- High false positive rates cause inconvenience to customers and increase manual investigation workload.
- Rule updates require manual intervention, making the system slow to respond to evolving fraud techniques.
- Lack of adaptive learning capabilities prevents continuous improvement based on new data.
- Difficulty handling large volumes of real-time transaction data efficiently.
- Delayed detection results in financial loss, security risks, and reduced customer trust.

IV. Proposed System

A. Architecture

The proposed adaptive zero-day fraud detection system uses Artificial Intelligence (AI), Machine Learning (ML), and behavioral analytics to provide an intelligent and real-time solution for detecting fraudulent activities in digital banking environments. Unlike traditional rule-based systems, the proposed system learns from historical transaction data and continuously adapts to evolving fraud patterns. The system monitors digital banking transactions in real time and analyzes multiple parameters such as transaction amount, time, geographical location, device information, and user behavior patterns to identify suspicious activities.

The system begins by collecting transaction data and performing preprocessing to ensure data quality. Machine learning models are trained to understand normal user behavior by building personalized behavioral profiles. When a new transaction occurs, anomaly detection algorithms compare it with learned behavior patterns to determine whether it deviates from normal activity. If the transaction shows unusual characteristics, the system assigns a risk score and flags it as potentially fraudulent.

B. System Modules

1) User / Digital Banking System: The entry point of the fraud detection process. Users perform financial transactions through mobile banking applications, UPI payments, net banking, or digital wallets. The system continuously monitors user actions and sends transaction data to the fraud detection system for analysis.

2) Data Collection Module: Gathers all relevant transaction and user activity data including user ID, transaction amount, frequency, login time, geographic location, IP address, and device information. Data is preprocessed to remove inconsistencies and handle missing values.

3) Behavior Analysis Module: Analyzes historical user transaction patterns to build a behavioral profile for each customer, evaluating spending habits, preferred transaction times, common locations, device usage, and transaction frequency to establish a baseline of normal activity.

4) Anomaly Detection Engine: The core component using machine learning algorithms such as Isolation Forest, SVM, Random Forest, or Autoencoders to compare new transactions with learned behavioral patterns and assign risk scores to detect zero-day fraud.

5) Adaptive Learning Module: Continuously retrains machine learning models as new transaction data becomes available, adapting to changing user behavior and evolving fraud techniques through feedback from confirmed fraud cases.

6) Alert and Action Module: Responds to suspicious activities by generating alerts for fraud analysts, requesting additional authentication, blocking suspicious transactions, or logging fraud events for investigation to prevent financial losses.

C. Advantages

- Capable of detecting new and unknown (zero-day) fraud attacks.
- Real-time monitoring and instant fraud detection.
- Uses AI and ML for intelligent and automated decision-making.
- Builds personalized user behavior profiles for accurate detection.
- Reduces false positives compared to traditional rule-

based systems.

- Adaptive learning allows continuous improvement and model updates.
- Scalable to handle large volumes of digital banking transactions.
- Enhances customer security and trust by preventing financial loss.

V. Machine Learning Algorithms

Isolation Forest: An unsupervised anomaly detection algorithm that isolates observations by randomly selecting features and splitting values. Fraudulent transactions are isolated faster, resulting in higher anomaly scores. Efficient for large datasets and suitable for real-time fraud detection.

Random Forest: A supervised learning algorithm that uses multiple decision trees to classify transactions as normal or fraudulent via majority voting. Improves accuracy, reduces overfitting, and handles large datasets effectively.

Support Vector Machine (SVM): Separates normal and fraudulent transactions using a decision boundary hyperplane. One-Class SVM learns normal behavior and flags deviations as potential fraud.

Autoencoders (Deep Learning): Neural network models for unsupervised anomaly detection that learn to reconstruct normal transaction patterns. High reconstruction error during inference signals fraudulent activity.

Logistic Regression: A supervised classification algorithm predicting fraud probability based on transaction features, serving as a simple, interpretable baseline model.

K-Means Clustering: Groups similar transactions into clusters. Transactions that do not belong to any cluster or fall far from cluster centers may be considered anomalous or suspicious.

VI. Behavioral Analytics

Behavioral analytics plays a critical role in the adaptive zero-day fraud detection system by analyzing and understanding the normal behavioral patterns of users during digital banking transactions. Instead of relying only on fixed rules or known fraud signatures, behavioral analytics focuses on how users typically interact with banking services by studying factors such as transaction amount, frequency, timing, geographical location, device usage, login patterns, spending habits, and transaction history.

By building dynamic behavioral profiles for each user, the system establishes a baseline of normal activity. Machine learning models then compare new transactions against these behavioral patterns in real time to identify deviations or anomalies that may indicate suspicious activity. This approach is especially effective for detecting zero-day fraud attacks because it identifies unusual behavior even when the specific fraud method has never been encountered before. Behavioral analytics also reduces false alerts and continuously adapts as user behavior evolves over time.

VII. System Design

A. Data Flow Diagram

The system architecture follows a pipeline from data ingestion through behavioral analysis to anomaly detection and alert generation. User Data flows into the Data Collection Module, which feeds into Behavioral Analysis. The Anomaly Detection Engine processes behavioral outputs and triggers the Alert and Action Module when fraud is detected. A feedback loop from confirmed fraud cases returns to the Adaptive Learning Module to retrain models continuously.

B. System Flow Diagram

The system flow begins when a user initiates a transaction. Data collection and behavior analysis execute in parallel. The fraud detection module is triggered, evaluating whether an anomaly is present. If no anomaly is found, the transaction is approved. If an anomaly is detected, a further fraud confirmation check is performed. Upon confirmation, a fraud alert is generated, the bank security system is notified, and fraud patterns are updated for future detection cycles.

VIII. System Development

A. System Environment

Hardware Configuration:

- Processor: Intel Core i5 or higher
- RAM: 8 GB or more
- Storage: 256 GB SSD or higher

Software Configuration:

- Operating System: Windows 10/11
- Programming Language: Python 3.6 or higher
- Libraries: NumPy, Pandas, Scikit-learn, TensorFlow/PyTorch, Matplotlib, Seaborn, Imbalanced-learn, Joblib/Pickle, Flask

B. Development Phases

Development followed nine key phases: (1) Requirement Analysis to understand challenges in traditional systems; (2) Data Collection and Preparation including preprocessing, normalization, and feature selection; (3) Feature Engineering to extract meaningful attributes such as transaction velocity, location changes, and device switching; (4) Behavioral Profiling to build per-user baseline models; (5) ML Model Development using Isolation Forest, Random Forest, SVM, and Autoencoders; (6) Real-Time Transaction Monitoring with instant risk scoring; (7) Adaptive Learning and Model Updating based on feedback; (8) Alert Generation and Response Mechanisms; and (9) System Integration and Deployment into digital banking platforms.

IX. System Testing

Software testing ensured correct, secure, and efficient operation under real-world digital banking conditions, validating accuracy, reliability, performance, and security across all modules. The testing process verified that each module operates correctly both individually and collectively.

A. Types of Testing

Unit Testing verified individual components including data collection functions, feature extraction modules, ML model prediction functions, and alert generation logic. Integration Testing confirmed correct data flow between all modules. Functional Testing validated fraud detection, alert generation, and transaction blocking. Performance Testing measured processing speed and model response time under heavy load. Security Testing verified data encryption, authentication mechanisms, and unauthorized access protection. Regression Testing ensured model updates did not affect existing functionality. User Acceptance Testing (UAT) confirmed system usability and reliability with banking administrators. Accuracy and Model Validation Testing evaluated Accuracy, Precision, Recall, and F1-Score metrics.

B. Test Results

The Adaptive Zero-Day Fraud Detection system passed all functional and non-functional testing phases successfully. AI and Machine Learning models effectively detected fraudulent activities, including unknown attack patterns. Behavioral analytics enhanced anomaly detection accuracy, and the system demonstrated strong performance, scalability, and reliability for real-time digital banking environments with low false-positive rates and fast response times.

X. Implementation Results

The system was implemented using Python with Scikit-learn's Isolation Forest as the primary anomaly detection algorithm. During preprocessing, raw transaction data is cleaned, normalized using StandardScaler, and transformed into structured feature vectors. The behavior analysis module computes per-user statistical profiles including mean, standard deviation, and Z-scores for amount and time features to measure how abnormal each transaction is compared to the user's normal behavior.

The anomaly detection engine assigns risk scores and classifies transactions as Low, Medium, or High risk. The alert and action module sends email notifications summarizing fraud statistics and automatically blocks high-risk transactions. The adaptive learning module updates detection thresholds based on confirmed fraud cases and false alarms, logging False Positives (5,672) and False Negatives (469) during evaluation. The graphical output displays fraud detection distribution showing the proportion of Normal, Suspicious, and Highly Risky transactions.

XI. Conclusion

The Adaptive Zero-Day Fraud Detection in Digital Banking System presents an advanced and intelligent approach to addressing the growing challenges of fraud in modern digital financial environments. With the rapid increase in online banking, mobile payments, and digital transactions, traditional rule-based fraud detection methods are no longer sufficient to identify evolving and unknown fraud techniques.

This project demonstrates how AI, Machine Learning, and behavioral analytics can be effectively integrated to create a smart and adaptive fraud detection framework capable of identifying both known and zero-day fraud attacks. The system continuously monitors real-time transaction data and builds behavioral profiles based on user activity. The adaptive learning capability ensures the model improves over time, and the reduction of false positives improves customer experience and operational efficiency. The scalable architecture ensures the system can handle high transaction volumes, contributing significantly toward building secure and reliable digital financial services for the future.

XII. Future Enhancement

Future work can focus on integrating more advanced AI and Deep Learning models such as Transformer-based architectures, Graph Neural Networks, or Reinforcement Learning to improve fraud detection accuracy and reduce false positives. Integration of blockchain technology can provide secure, transparent, and tamper-proof transaction records. Collaboration between financial institutions through secure data-sharing frameworks can enable faster identification of emerging fraud patterns.

Performance optimization through edge computing and cloud-based distributed architectures can improve scalability and response speed. The system can be expanded to support cross-border payments, cryptocurrency transactions, and emerging financial technologies. Implementation of Explainable AI (XAI) techniques and privacy-preserving machine learning methods such as federated learning will further strengthen transparency and customer trust.

ACKNOWLEDGMENT

The authors express sincere thanks to Dr. M.T. Nicholas, MS., Ph.D. (Chairman), Dr. J.D. Darwin, M.E., Ph.D. (Principal), and Dr. A. Shakeela Joy, M.E., Ph.D. (Head of Department and Internal Guide) of Loyola Institute of Technology and Science, Thovalai, for their invaluable guidance, constant support, and encouragement throughout the project work.

REFERENCES

[1] Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2025). Year-over-year developments in financial fraud detection via deep learning: A systematic literature review.

[2] Akinnagbe, O. B., & Akintayo, T. A. (2025). The impact of machine learning on fraud detection in digital payment. Asian Journal of Science, Technology, Engineering and Art.

[3] George, M. Z. H., et al. (2025). Machine learning for fraud detection in digital banking: A systematic literature review.

[4] Abdulalem Ali, et al. (2022). Financial fraud detection based on machine learning: A systematic review. Applied Sciences (MDPI).

[5] Mohammed, H. S., Sallow, Z. B., & Zangana, H. M. (2026). AI-driven fraud detection in digital banking: Hybrid deep learning and anomaly detection.

[6] Zheng, Y. (2025). Bank data protection and fraud identification using adaptive federated learning and WGAN. Scientific Reports.

[7] Almalki, F., & Masud, M. (2025). Financial fraud detection using explainable AI and stacking ensemble methods.

[8] Sabuhi, M., Zhou, M., Bezemer, C., & Musilek, P. (2021). Applications of GANs in anomaly detection: A systematic review.

[9] Tsai, W. (2025). Deep learning-based financial fraud detection with temporal and feature-level adaptation.

[10] IBM Cloud. AI-driven fraud detection in digital banking. https://www.ibm.com/cloud/learn/fraud-detection

[11] Google Cloud. Machine learning for real-time fraud detection. https://cloud.google.com/architecture/real-time-fraud-detection

[12] Reserve Bank of India (RBI). (2025). Guidelines on digital banking fraud and AI monitoring. https://www.rbi.org.in

