IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

Real Time Fraud Detection in Financial Transaction

Anushka Sanjay Badwane[1], Sakshi Vinod Bhale[2], Prof. N. S. Kharatmal[3]
Students, Computer Science and engineering [1,2]
Lecturer, Computer Science and engineering[3]
Matsyodari Shikshan Sanstha College Engineering and Polytechnic, Jalna, India
badwaneanushka@gmail.com[1], sakshibhale11@gmail.com[2], nanditakharatmal27@gmail.com[3]

Abstract: *Real-time fraud detection in financial transactions is a critical challenge in modern digital banking and payment systems due to the increasing volume and complexity of online transaction. This topic focuses on detecting financial fraud in real time. Financial transactions are increasingly vulnerable to sophisticated fraud techniques, resulting in significant losses. Real-time fraud detection systems use machine learning, data analytics, and rule-based approaches to identify suspicious activity and prevent unauthorized transactions. In recent times, the number of money fraud cases has increased, where fraudsters ask for OTPs and misuse financial transactions.*

Keywords: Real-time transaction analysis, financial fraud identification, anomaly-based detection, machine learning-driven security, risk evaluation mechanism, automated alert system

I. INTRODUCTION

Real-Time Fraud Detection in Financial Transaction In today's digital economy, financial transactions occur at high speed across online banking, mobile payments, and e-commerce platforms. Financial transactions are increasingly vulnerable to sophisticated fraud techniques, resulting in significant losses .To combat this, real-time fraud detection systems use machine learning, data analytics, and rule-based approaches to identify suspicious activity and prevent unauthorized transactions . This introduction sets the stage for exploring methodologies, challenges, and future directions in real-time fraud detection .Real Time Fraud Detection in Financial Transactions means that nowadays a lot of fraud occurs, just like fake OTP links and all. People trust them, open those links, and send OTP, which is why fraud happens. If everyone stays safe, don't trust fake links, don't send OTP, don't pick up fake calls.

Real-time fraud detection in financial transactions focuses on identifying and preventing fraudulent activities at the exact moment a transaction occurs.

II. LITERATURE SURVEY

1) Signature Based Detection: Signature-based detection identifies fraud by matching transactions against known patterns or signatures of fraudulent activity**.** Signature Based Detection means catching fraud using old records. Like checking past data to detect fraud for example, if many transactions are happening after a specific OTP, it flags

2) Anomaly Based Detection: Anomaly Based Detection means catching fraud based on normal behavior, just like if a person is doing transactions every day and suddenly does a high-level transaction, it's considered anomaly fraud and an alert is sent. Anomaly-based detection is highly effective in identifying new and unknown fraud patterns,

3) SSID-BSSID Mapping: SSID is the Wi-Fi network name, and BSSID is the unique identifier of the router. The system checks whether the Wi-Fi network is normal or not and detects fake Wi-Fi by verifying the SSID–BSSID combination. Aids in device profiling and anomaly detection. Useful for identifying suspicious location patterns.

4) RSSI Behavior and Signal Strength: RSSI Behavior and Signal Strength means that it checks the WiFi's behavior and strength. If the WiFi is not normal, then it means that it is fraud.

5) Vendor (OUI) Analysis: In real-time fraud detection for financial transactions, OUI analysis helps fingerprint devices involved in payments, flagging anomalies like spoofed or unusual hardware to prevent fraud such as account

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, January 2026 Impact Factor: 7.67

takeovers or unauthorized transactions. Vendor (OUI) Analysis means the system checks the router or device manufacturer company. If the company is unknown, the system considers that router or device as fraudulent.

6) Machine Learning Based Detection: Machine Learning–Based Detection means the system trains the computer so that it can automatically detect fraud using past transaction data. Key models include Random Forest, Light GBM, and Deep Learning (LSTM), using techniques like SMOTE for imbalanced data to achieve high accuracy and reduce false positives in banking, e-commerce, and mobile payments.

7) Hybrid Detection System: A hybrid detection system combines multiple detection techniques to overcome the weaknesses of any single method. Combines multiple techniques. Hybrid Detection System means that one system uses many fraud methods, but it catches fraud accurately, mistakes do not happen, meaning it combines signature-based detection, anomaly-based detection.

III. EXISTING MODAL (CURRENT LIMITATIONS)

Some of the limitations include the following:

1. Lack of Unified Detection Logic- Due to the lack of a unified detection logic to combine multiple techniques, the final fraud decision remain unclear. increases false positives and false negatives, negatively impacting customer trust and transaction efficiency.

2. High False Positive in dynamic Environments- it is occur when a fraud detection system incorrectly identifies especially in changing or dynamic environments.

3. Weakness Against MAC and Vendor Spoofing- limited resistance to MAC address and vendor spoofing attacks allowing fraudulent transactions to bypass authentication and monitoring mechanisms.

4. Limited Zero Day Attack Recognition Without Training data- systems cannot effectively recognize new or unseen (zero-day) attacks struggles with completely new frauds since the system has no prior examples

5. Insufficient Real-Time Decision Capabilities- proposing a hybrid AI-driven framework combining edge computing and reinforcement.

Due to these limitations, real-time fraud detection systems often fail to detect fraud accurately and instantly. These appear to be limitations of a network security system, like an Intrusion Detection System (IDS) or similar tool.

IV. PROPOSED/WORKING MODEL AND METHODOLOGY

System Architecture

The system has five separate steps

WIFI Monitoring: helps identify if a transaction comes from a trusted or suspicious network It helps detect threats like man-in-the-middle attacks or unauthorized access in real-time

Attack Detection: Attack Detection in real-time fraud detection refers to identifying suspicious or fraudulent activities instantly. identifies malicious activities like phishing, malware, DDoS

Alert Genration: Alert generation is the process of automatically notifying stakeholders when a transaction is identified as potentially fraudulent

PCAP Loggins: refers to the process of capturing and storing network data packets during transaction communication.

System Automation: System automation enables automatic monitoring, detection, and response to fraudulent transactions in real time, reducing human effort and response time.

B: Methodology

The following steps are taken to execute the projrct using this using Methodology:

1.Hardware Setup:

Server

Network Device

Storage

Network Security

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

2.Software Installation:
transaction monitoring software, real-time analysis modules, fraud detection algorithms

3.Monitor Mode Configuration:
Transaction flow
Network activity

4. Packet Capture Module:
module unusual packet patterns
unauthorized communication

5. Detection Logic:
incoming transactions analyze
fraud risk evaluate
alerts generate
automatic action

Transaction Sources
↓
API Gateway / Kafka
↓
Feature Engineering (Streaming)
↓
Fraud Detection Engine
↓
Rules + ML Models)
↓
Decision Engine
↓
Approve / Block / Review
↓
Alerts Notifications
↓
Data Storage & Model Transaction

Fig. System Architecture

V. ALGORITHM USED IN EXISTING MODEL

Isolation Forest	Unsupervised anomaly detection algorithm
One-Class SVM	Effective for identifying outliers and anomalie
Gradient Boosting	Ensemble model for improving prediction accuracy
Transaction History	Analyzing past transactions to identify patterns

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, January 2026 Impact Factor: 7.67

Device Fingerprinting	Identifying device characteristics to prevent device-based fraud
Location-Based Analysis	Using location data to identify suspicious activity

However, most existing models still suffer from limitations such as lack of unified detection logic, high false alerts, and difficulty in handling evolving fraud patterns. The system uses various algorithms to detect fraud. Rule-based algorithms work on predefined rules created from known fraud patterns, such as high transaction amounts or sudden location changes. Machine learning algorithms learn from historical transaction data and classify transactions as fraudulent or legitimate. Anomaly detection algorithms identify transactions that deviate from normal user behavior and help detect new or unknown fraud activities.

VI. OUTPUT/RESULT AND DISCUSSION

Transaction ID	User ID	Amount (₹)	Transaction Type	Location	Risk Score	Detection Result	System Action
TXN001	U101	2500	Online Payment	Mumbai	0.15	Legitimate	Approved
TXN002	U101	4800	Card Payment	Pune	0.82	Fraudulent	Blocked
TXN003	U101	6500	UPI Transfer	Hingoli	0.45	Legitimate	Approved
TXN004	U101	9500	Net Banking	Indore	0.35	Fraudulent	Account Frozen
TXN005	U101	4800	ATM Withdrawal	Delhi	0.75	Suspicious	OTP Verification

The discussion centers on performance metrics, operational efficiency, and the continuous need to adapt to evolving fraud tactics. Each transaction contains multiple attributes, including transaction amount, time, location, device information, and customer behavior history.

The effectiveness of real-time fraud detection systems is measured using specific performance metrics, with machine learning models demonstrating significant improvement over traditional rule-based systems. The implementation of a real-time fraud detection system is expected to yield significant improvements in detecting and preventing fraudulent transactions. The system's performance will be evaluated based on metrics such as detection accuracy, false positive rate, and transaction processing speed. The implementation of a real-time fraud detection system is expected to yield significant improvements in detecting and preventing fraudulent transactions. The system's performance will be evaluated based on metrics such as detection accuracy, false positive rate, and transaction processing speed.The core idea behind real-time fraud detection is to analyze transaction data as a continuous stream and determine whether a transaction is legitimate or fraudulent based on learned patterns.

VII. CONCLUSION

This study explores the role of real-time monitoring and machine learning in enhancing fraud detection and prevention within financial transactions. Combines rule-based, ML, and behavioral analysis for robust detection. Systems use advanced algorithms, machine learning, and AI to analyze patterns, anomalies, and risks in real-time, reducing losses from fraud like credit card scams, identity theft, and money laundering.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, January 2026 Impact Factor: 7.67

Effective systems use machine learning, data analytics, and rule-based approaches to identify suspicious activity. Key challenges include high false positives, data quality, and adapting to evolving fraud patterns. By addressing these challenges, financial institutions can improve detection accuracy and reduce operational costs.

Regular updates and monitoring are crucial. Fraudsters continuously adapt their strategies, requiring ongoing model updates and robust monitoring frameworks. Balances Security & User Experience: Reduces fraud while minimizing disruptions.

REFERENCES

[1]. Eason, G., Noble, B., & Sneddon, I. N. (1955). On certain integrals of Lipschitz-Hankel type involving products of Bessel functions. Philosophical Transactions of the Royal Society A, 247, 529–551.

[2]. Jacobs, I. S., & Bean, C. P. (1963). Fine particles, thin films, and exchange anisotropy. In G. T. Rado & H. Suhl (Eds.), Magnetism (Vol. III, pp. 271–350). New York: Academic.

[3]. Reddy, C., Prabhagaran, S., & Vaid, A. (2024). Deep learning-based real-time credit card fraud detection in financial transactions. International Journal of Advanced Research in Engineering and Technology, 15(6), 20–30.

[4]. Immadisetty, A. (2025). Real-time fraud detection using streaming data in financial transactions. Journal of Recent Trends in Computer Science and Engineering, 13(1), 85–92.

[5]. Rahmati, M., & Rahmati, N. (2025). Adversarially robust and explainable AI for real-time financial fraud detection. International Journal of Management and Data Analytics, 5(1), 241–252.

[6]. Nguyen, H., & Le, B. (2025). Real-time transaction fraud detection via heterogeneous temporal graph neural networks. Proceedings of the International Conference on Data Analytics and Machine Learning, 112–120

[7]. Dal Pozzolo, A., Bontempi, G., Snoeck, M., & Snoeck, M. (2015). Adaptive machine learning for credit card fraud detection. IEEE Intelligent Systems, 30(4), 79–83.

[8]. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. (2009). Transaction aggregation as a strategy for credit card fraud detection. Data Mining and Knowledge Discovery, 18(1), 30–55