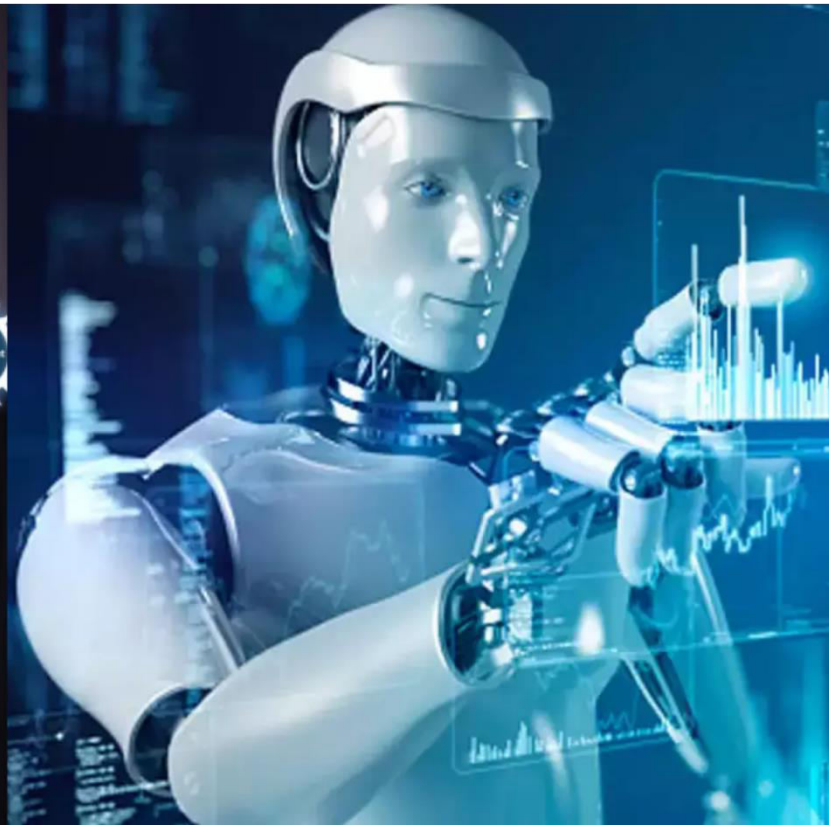
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Special Issue 1, January 2026

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

AI-Enabled Platform for Real-Time Transaction Risk Analysis

Prof. Gauri Bhosale[1], Yash Surve[2], Komal Shelavale[3], Yogesh Jadhav[4], Devendra Patil[5]

Professor, Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[1]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India [2]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India [3]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India [4]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India [5]

ABSTRACT: The growing reliance on digital transactions has led to a surge in financial fraud, emphasizing the need for intelligent and adaptive detection mechanisms. This project, AI-Enabled Platform for Real-Time Transaction Risk Analysis, presents an advanced system that leverages artificial intelligence and machine learning to detect and prevent fraudulent activities with high accuracy. The platform analyzes transactional data streams in real time using a combination of supervised and unsupervised learning algorithms, including Logistic Regression, Random Forest, and Autoencoders, to identify anomalies and assign dynamic risk scores. By integrating predictive analytics, behavioral profiling, and anomaly detection techniques, the system minimizes false positives while ensuring quick and reliable fraud identification. A user-friendly dashboard provides real-time alerts and visual insights, enabling faster decision-making and response. Overall, this AI-enabled platform enhances transaction monitoring efficiency, reduces financial losses, and strengthens trust and security across digital payment ecosystems.

KEYWORDS: Artificial Intelligence (AI), Machine Learning (ML), Real-Time Transaction Risk Analysis, Financial Fraud Detection, Predictive Analytics

I. INTRODUCTION

The rapid expansion of digital financial ecosystems has transformed the way transactions are processed across banking, e-commerce, and fintech platforms. With this increased reliance on online payment infrastructures, the frequency and sophistication of financial fraud have escalated, posing significant challenges to organizations in ensuring transaction integrity and user trust. Traditional fraud detection mechanisms, primarily based on static rule-based systems, often fail to capture evolving fraud patterns due to their limited adaptability, high false-positive rates, and inability to process massive real-time data streams. Consequently, there is a growing need for intelligent, dynamic, and scalable fraud detection solutions capable of addressing the complexities of modern digital transactions.Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful enablers for enhancing fraud detection efficiency by learning behavioral patterns, identifying anomalies, and adapting to new threat vectors. By leveraging transactional data, user activity logs, and contextual features, AI-driven systems can detect subtle deviations that conventional models may overlook. However, challenges such as data imbalance, real-time processing requirements, and the necessity for model interpretability continue to demand more advanced, hybrid, and adaptive solutions.

This paper presents an AI-Enabled Platform for Real-Time Transaction Risk Analysis designed to overcome the limitations of existing fraud detection systems. The proposed platform integrates supervised and unsupervised machine learning algorithms—including Logistic Regression, Random Forest, and Autoencoders—to analyze historical and live transaction streams for anomaly detection and risk scoring. The system dynamically assigns risk levels to transactions by examining behavioral signatures, geographical irregularities, transaction frequency patterns, and user-specific attributes.

Furthermore, the platform incorporates real-time alerting, adaptive learning, and a user-friendly analytical dashboard to support rapid decision-making in operational environments. By continuously updating the model with new data, the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

system achieves higher detection accuracy while maintaining low false-positive rates, ensuring robust protection against emerging financial fraud techniques. The proposed work thus contributes toward building a scalable, intelligent, and transparent fraud detection framework suited for modern financial infrastructures.

II. SYSTEM MODEL AND ASSUMPTIONS

The proposed AI-Enabled Platform for Real-Time Transaction Risk Analysis operates on a financial transaction ecosystem consisting of heterogeneous digital payment channels, including online banking systems, e-commerce gateways, and mobile payment interfaces. It is assumed that all transactional events are generated as continuous data streams with high velocity and variability, reflecting the dynamics of modern digital financial environments. Each transaction is modeled as a structured data instance containing attributes such as transaction amount, timestamp, device metadata, geolocation identifiers, user historical behavior patterns, and contextual metadata. The system presumes that this data is available in near real time through secure APIs or streaming pipelines, ensuring minimal latency for model inference.

The entire transaction monitoring environment is considered to be distributed, where multiple data sources concurrently transmit high-volume event logs. It is assumed that the underlying infrastructure supports scalable data ingestion and that preprocessing modules consistently perform cleansing, normalization, and feature extraction before the data enters the analytics layer. In addition, the system assumes the presence of both labeled historical data and unlabeled live data, enabling the use of supervised, unsupervised, and hybrid machine learning models to identify anomalous activity patterns. The presence of class imbalance—typical of financial fraud datasets—is also assumed, requiring model optimization techniques and continuous feedback mechanisms.

For computational modeling, it is assumed that machine learning algorithms such as Logistic Regression, Random Forest, and Autoencoders operate on processed feature vectors to generate real-time risk scores for each transaction. The system further assumes that deviations in user behavior, unusual spending velocity, and inconsistencies in device or location parameters are reliable indicators of potential fraud. All model computations are assumed to be executed on local servers or cloud-based environments capable of supporting high-throughput analytics.

The platform also assumes that every transaction must undergo instantaneous risk evaluation, with the decision engine capable of flagging, prioritizing, or temporarily withholding suspicious transactions. It is further assumed that real-time alerts are delivered through a monitoring dashboard accessible to system administrators and analysts for rapid decision-making. The overall system model presupposes secure data handling practices, adherence to regulatory requirements, and consistent system updates to adapt to evolving fraud patterns.

III. EFFICIENT COMMUNICATION

The proposed AI-enabled platform enhances efficient communication within financial transaction networks by ensuring rapid, accurate, and adaptive risk assessment. It continuously monitors streaming transaction data and identifies anomalous patterns using machine learning models, enabling immediate fraud detection without interrupting workflow. Real-time analytics reduce latency, allowing the system to respond to emerging threats within milliseconds. The communication between system components—data ingestion, analysis engine, and risk scoring module—is optimized to maintain seamless information flow. By minimizing false positives, the platform improves operational efficiency and prevents unnecessary transaction delays. Automated alert mechanisms ensure that critical risk notifications reach stakeholders instantly. The model's ability to learn from behavioral patterns enhances coordination between detection and decision-making layers. Furthermore, the platform supports scalable communication across high-volume financial environments. Overall, the system ensures secure, high-speed, and intelligent communication essential for modern digital transaction ecosystems.

IV. SECURITY

In AI-enabled financial systems, security plays a critical role in ensuring the integrity of real-time transaction monitoring and fraud detection. As digital transactions continue to grow, the platform must be capable of identifying anomalous activities without interrupting legitimate user operations. The proposed system integrates multiple layers of security mechanisms designed to safeguard transaction data, model decisions, and user confidentiality.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

Risk Detection and Anomaly Identification:
The platform employs both supervised and unsupervised learning techniques to detect deviations from normal spending patterns. By continuously analyzing transaction streams, the system identifies unusual behaviors such as abnormal transaction amounts, rapid transfers, suspicious geolocations, and device inconsistencies. These anomalies are used to generate real-time risk scores that indicate potential fraudulent intent.

Behavioral Profiling:
Each user is associated with a behavioral profile based on historical financial activity, transaction velocity, and device usage patterns. Machine learning models rely on these profiles to detect impersonation attempts and unauthorized access. If an attacker attempts to mimic a legitimate user's behavior, deviations in the profile trigger a security alert.

Cooperative Threat Intelligence:
Similar to cooperative sensing in cognitive radio networks, the system utilizes cooperative intelligence by aggregating threat indicators from multiple sources such as transaction histories, known fraud patterns, blacklisted accounts, and external financial threat databases. This shared intelligence increases detection accuracy and reduces the chances of false-negative outcomes.

Security Threats in Transaction Environments:
Two major categories of threats commonly observed in digital financial ecosystems are:

Selfish Transaction Manipulation (STM):
Attackers attempt to exploit system weaknesses by manipulating transaction attributes such as amount or timestamp to bypass risk filters. These attackers aim to maximize their fraudulent gains while avoiding detection.

Malicious Transaction Injection (MTI):
In this attack, adversaries deliberately inject high-risk or fabricated transactions into the system to disrupt risk analysis processes or trigger denial-of-service conditions. Such attacks can confuse detection models and degrade system performance.

Trust-Worthy Validation Mechanism:
To combat these threats, the platform applies a trust-based validation algorithm that assigns trust scores to transactions, devices, and user identities. Suspicious transactions undergo additional verification, while trusted sources pass through standard processing. This threshold-based trust mechanism helps mitigate manipulation attacks and strengthens overall system resilience.

By integrating these multi-layered security measures, the AI-enabled platform ensures secure, reliable, and efficient real-time transaction risk analysis while maintaining minimal interference with legitimate financial activities

V. CONCLUSION

Thus, the proposed AI-Enabled Platform for Real-Time Transaction Risk Analysis effectively enhances the detection of fraudulent and high-risk transactions by integrating supervised and unsupervised machine learning models. The system analyzes large volumes of transactional data streams in real time and assigns dynamic risk scores, enabling faster and more reliable decision-making. By utilizing algorithms such as Random Forest, Logistic Regression, and Autoencoders, the platform minimizes false positives while maintaining high prediction accuracy. The real-time dashboard and alerting mechanism further support analysts in monitoring evolving fraud patterns. Overall, the system demonstrates strong capability in adapting to dynamic financial environments and provides a scalable, intelligent, and efficient solution for modern transaction risk management.

REFERENCES

1. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255.
2. Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit card fraud detection using AdaBoost and majority voting. IEEE Access, 6, 14277–14284.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

3. Sethi, M., & Kantardzic, M. (2018). Handling imbalanced data: A review. IEEE Transactions on Knowledge and Data Engineering, 31(9), 1672–1689.
4. Zareapoor, M., & Shamsolmoali, P. (2015). Application of credit card fraud detection: Based on machine learning. Journal of Computer Engineering and Information Technology, 4(1), 1–12.
5. Y., Lu, C.-T., Sirwongwattana, S., & Huang, Y.-P. (2004). Survey of fraud detection techniques. IEEE International Conference on Networking, Sensing and Control, 2, 749–754.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details