© May 2026 | IJIRT | Volume 12 Issue 12 | ISSN: 2349-6002

AI Fraud Detection in Transactions

Pratik Ramesh Tupsamindra[1], Sarthak Uddhav Thorat[2], Parth Prakash Undale[3]
Govind Phulchand Verma[4]
[1,2,3,4] *JSPM University*

I. INTRODUCTION

Over the past few years, digital payment systems have become an essential part of everyday life. Whether it is paying bills, transferring money, or making purchases, people increasingly depend on platforms such as UPI, mobile wallets, and online banking. While this shift has made financial transactions faster and more convenient, it has also opened the door to new types of fraud. As financial systems grow more connected, cybercriminals are finding smarter ways to exploit them.

Fraud today is no longer limited to simple scams. Attackers use techniques like phishing, identity theft, SIM swapping, and unauthorized account access to target users. What makes this more concerning is that victims often realize the fraud only after money has already been lost. This delay shows that traditional detection systems are no longer sufficient. Most of these systems rely on fixed rules, which work only for known fraud patterns. However, fraud methods keep evolving, making such systems less effective over time.

Artificial Intelligence offers a more flexible approach. Instead of relying only on predefined rules, AI systems learn from transaction data and user behavior. They can identify unusual patterns and respond much faster than traditional systems. Because of this, AI is becoming an important tool in strengthening the security of digital financial systems.

II. LITERATURE REVIEW

The field of fraud detection has changed significantly with the growth of digital transactions. Earlier systems mainly depended on rule-based methods, where transactions were flagged based on fixed conditions. While these methods were simple to implement, they struggled to handle new and complex fraud patterns. This often resulted in either too many false alerts or missed fraud cases.

With the introduction of machine learning, researchers began focusing on data-driven approaches. Models such as decision trees, logistic regression, and neural networks are now widely used to analyze transaction data. These models do not just look at individual transactions but also consider user behavior over time. For example, they study how often a user spends, where transactions usually occur, and how spending patterns change.

Recent research also emphasizes anomaly detection, where systems identify activities that deviate from normal behavior. Even though these methods have improved detection accuracy, challenges still remain. One major issue is the imbalance in datasets, where fraudulent transactions are much fewer compared to genuine ones. Another concern is that some advanced models are difficult to interpret, which can be problematic in financial systems where transparency is important.

III. PROBLEM STATEMENT

Even with modern technology, detecting financial fraud remains a difficult task. One of the biggest problems is false positives, where genuine transactions are mistakenly flagged as suspicious. This can frustrate users and reduce trust in the system. At the same time, some fraudulent transactions still go unnoticed because attackers constantly change their methods.

Another challenge is the sheer volume of transactions processed every day. Banks and digital platforms handle millions of transactions, and each one needs to be checked within seconds. Manual monitoring is clearly not practical in such situations. Additionally, fraud-related data is highly imbalanced, which makes it harder for machine learning models to accurately identify fraud.

These issues highlight the need for a smarter system that can adapt to changing patterns, work in real time, and maintain a balance between accuracy and user convenience.

IV. OBJECTIVES

This research aims to develop an AI-based system that can detect fraudulent transactions more effectively. The focus is on understanding user behavior and identifying unusual activities that may indicate fraud. The system should reduce unnecessary alerts while still catching actual fraud cases. It should also be capable of analyzing transactions in real time and providing results that can be understood and reviewed by analysts. Another important goal is scalability, ensuring that the system can handle increasing amounts of transaction data without losing performance.

V. METHODOLOGY

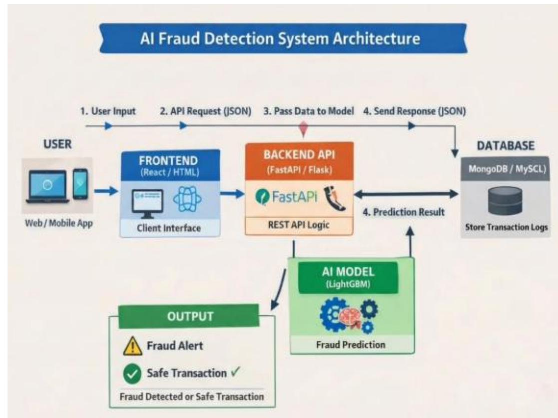
The process begins with collecting transaction data from different sources such as banks and payment systems. This data includes information like transaction amount, time, location, and user activity. Since raw data is often messy, it needs to be cleaned by removing errors, duplicates, and missing values.

After cleaning, useful features are created to better understand user behavior. These may include average spending, frequency of transactions, or unusual location changes. These features help the system distinguish between normal and suspicious activity. Machine learning models are then trained using this processed data to classify transactions. The performance of these models is tested using different evaluation metrics to ensure reliability.

VI. SYSTEM ARCHITECTURE

The system starts with the user, who initiates a transaction through a mobile or web application. This request is sent to the backend through secure APIs, where initial checks are performed. The transaction data is then passed to the AI model, which analyzes it based on previous patterns and assigns a risk score.

As shown in the diagram on page 4, the system follows a structured flow from user input to backend processing, then to the AI model, and finally to the output decision. Based on the risk score, the system decides whether to approve the transaction, flag it for review, or block it. All transaction data is stored in a database, which helps in both real-time analysis and future improvements.



VII. EXPECTED OUTCOMES

The proposed system is expected to improve the overall accuracy of fraud detection. By identifying suspicious transactions earlier, it can help reduce financial losses. At the same time, genuine users are less likely to face unnecessary interruptions. The system can also make the work of fraud analysts easier by allowing them to focus only on high-risk cases. As more data is collected, the system will continue to improve over time.

VIII. APPLICATIONS

AI-based fraud detection can be used in many areas, including banking, online shopping, insurance, and telecommunications. It is also useful in cryptocurrency platforms and government systems where financial transactions need to be monitored closely. Any system that deals with digital payments can benefit from such technology.

IX. CHALLENGES AND LIMITATIONS

Although AI provides many advantages, it also comes with certain challenges. High-quality data is required for accurate predictions, and such data is not always available. Privacy is another major concern since financial data is sensitive. Some machine learning models are complex and difficult to interpret, which can make decision-making less transparent. Additionally, implementing such systems can be expensive, especially for smaller organizations. Fraudsters also continue to evolve, which means the system needs regular updates.

X. FUTURE SCOPE

In the future, fraud detection systems may become more advanced by using techniques like graph analysis to detect networks of fraudulent activities. Federated learning could allow organizations to improve models without sharing sensitive data. Systems may also become more adaptive, updating themselves in real time as new patterns emerge. The role of explainable AI is also expected to grow, ensuring that decisions made by models can be understood and trusted.

XI. CONCLUSION

As digital transactions continue to grow, the risk of financial fraud is also increasing. Traditional detection methods are no longer enough to handle modern threats. AI-based systems provide a more effective solution by analyzing patterns and detecting unusual behavior in real time. When used correctly, these systems can improve security, reduce losses, and build trust among users. In the long run, intelligent fraud detection will play a key role in maintaining safe and reliable financial systems.

REFERENCES

[1] J. Smith, Introduction to Fraud Detection Using AI, Tech Journal, 2020.
[2] R. Kumar and S. Patel, Machine Learning for Fraud Detection in Banking, 2019.
[3] H. Lee, Detecting Credit Card Fraud with Machine Learning, 2021.
[4] M. Johnson, Basics of AI in Financial Fraud Detection, 2018.
[5] Gupta and P. Singh, Real-Time Fraud Detection in Online Transactions, 2022.