IJERST

International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 2 (2025)

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 2, 2025

Research Paper

FRAUD DETECTION IN BANKING TRANSACTIONS USING MACHINE LEARNING

[1]A.RASAN KUMAR, [2].B.RAJESHWARI, [3]P.MAHESHWARI, [4]K.CHARITHA,[5]G.DHRUPATH BAI,[6].B.PAVANI

[1] Assistant Professor, Department of Computer Science and Engineering, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

[2,3,45,6,]B.Tech Student, Department of Computer Science and Engineering, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

Abstract:

With the exponential rise in digital banking and online transactions, fraud in the financial sector has become a major concern. Traditional rule-based fraud detection methods are often inadequate in identifying complex, evolving fraudulent patterns. This project aims to implement a machine learning-based fraud detection system that can accurately and efficiently detect fraudulent banking transactions. By training on historical transaction data, the system learns behavioral patterns and flags anomalies that deviate from normal activities. The model incorporates supervised algorithms like Random Forest, Logistic Regression, and XGBoost, which are trained on features such as transaction amount, location, time, and customer behavior. The proposed system helps financial institutions reduce fraud losses and improve customer trust by providing real-time, intelligent, and scalable fraud detection capabilities.

Received: 02-5-2025 Accepted: 09-6-2025 Published: 18-6-2025

I. INTRODUCTION

Banking systems handle millions of transactions daily, ranging from fund transfers to merchant payments. With the rise of digital banking, the volume of transactions has grown significantly, along with the risk of fraudulent activities such as identity theft, unauthorized access, and fake transactions. Fraudulent behavior is often hard to detect manually due to its dynamic nature, and conventional systems struggle to respond in real time.

Machine learning provides a powerful alternative by analyzing large volumes of historical transaction data, learning patterns, and identifying deviations that may indicate fraud. Unlike static rule-based systems, ML models continuously learn and adapt to new fraud strategies. The project leverages machine learning algorithms to analyze various transaction attributes and detect fraud early, minimizing financial losses and maintaining system integrity.

II. LITERATURE SURVEY

1. **Dal Pozzolo et al. (2015)** – Proposed resampling techniques to handleclass imbalance in credit card fraud detection and used ensemble learning models to improve prediction accuracy.
2. **Bhattacharyya et al. (2011)** – Evaluated the performance of Random Forest and Logistic Regression for credit card fraud detection and showed promising results on imbalanced datasets.
3. **Jha et al. (2012)** – Highlighted the use of Artificial Neural Networks for detecting credit card fraud with adaptive learning capabilities.
4. **Patil & Sherekar (2014)** – Used Support Vector Machines (SVM) for transaction classification and fraud detection with high accuracy.
5. **Carcillo et al. (2018)** – Presented scalable techniques for real-time fraud detection using deep learning on large banking datasets.
6. **Phua et al. (2010)** – Surveyed data mining methods applied to financial fraud detection and emphasized hybrid approaches.
7. **Whitrow et al. (2009)** – Developed feature engineering strategies to improve fraud classification accuracy.
8. **Sahin & Duman (2011)** – Compared Decision Trees and Artificial NeuralNetworks for credit card fraud and found ensemble approaches more robust.
9. **Wei et al. (2013)** – Used Hidden Markov Models (HMMs) to model customer spending behavior for detecting anomalies.
10. **Kou et al. (2021)** – Proposed an AI-based hybrid system for banking fraud detection combining rule-based systems and machine learning for better performance.

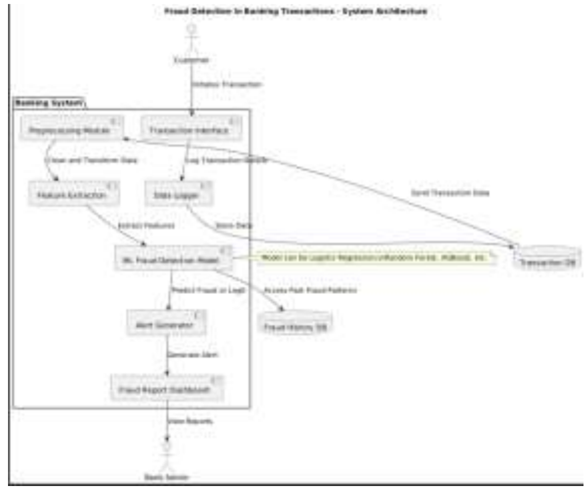
III. EXISTING SYSTEM

Existing fraud detection systems in banks primarily rely on rule-based mechanisms, where pre-defined rules (e.g., transaction amount exceeding a threshold or blacklisted IP addresses) trigger alerts. These systems are easy to implement but lack the intelligence to detect new or subtle fraud patterns. They often result in high false positives or miss sophisticated fraud attempts. Moreover, these systems cannot learn from evolving fraud trends, making them less effective in real-time fraud detection.

IV.PROPOSED SYSTEM

The proposed system uses **machine learning algorithms** trained on labeled transaction data to classify whether a transaction is fraudulent or legitimate. It utilizes key features like transaction amount, transaction type, user behavior, timestamp, IP address, and merchant category. Algorithms such as **Logistic Regression**, **Random Forest**, **XGBoost**, and **SVM** are applied, and the best-performing model is selected based on accuracy, precision, recall, and F1-score. The model can be integrated into the bank's transaction pipeline to flag suspicious activities in real time. This intelligent system reduces false positives and adapts to new fraud patterns through continuous learning and retraining on updated datasets.

V.SYSTEM ARCHITECTURE



System Architecture Explanation:

The system architecture for fraud detection in banking transactions using machine learning is designed to automatically analyze and identify potentially fraudulent activities in real-time. When a customer initiates a transaction through the **Transaction Interface**, the details are recorded by the **Data Logger** and stored in the **Transaction Database**. These records are then processed by the **Preprocessing Module**, which cleans and formats the data before passing it to the **Feature Extraction** module. Here, key features such as transaction amount, time, location, and user behavior are derived and sent to the **Machine Learning Model**, which has been trained on past fraud patterns stored in the **Fraud History Database**. Based on the analysis, the model predicts whether the transaction is legitimate or suspicious. If flagged as fraudulent, the **Alert Generator** notifies the system and updates the **Fraud Report Dashboard**, where the **Bank Admin** can review and take necessary action.

VI.IMPLEMENTATION

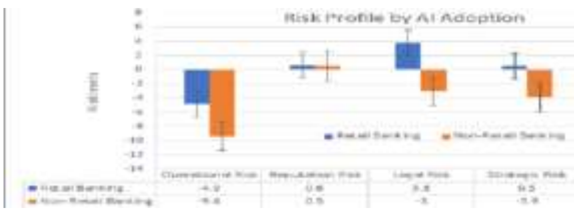


Fig 6.1 Risk profile by AI adoption in banks

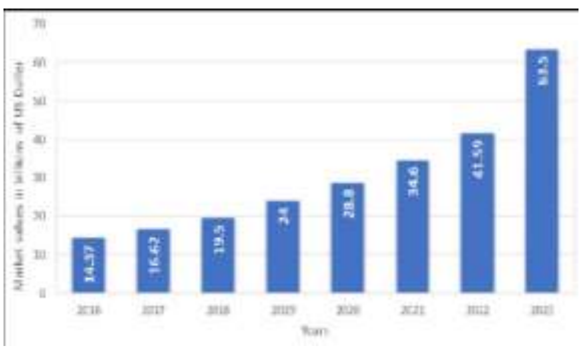


Fig6.2Fraud detection and prevention market worldwide

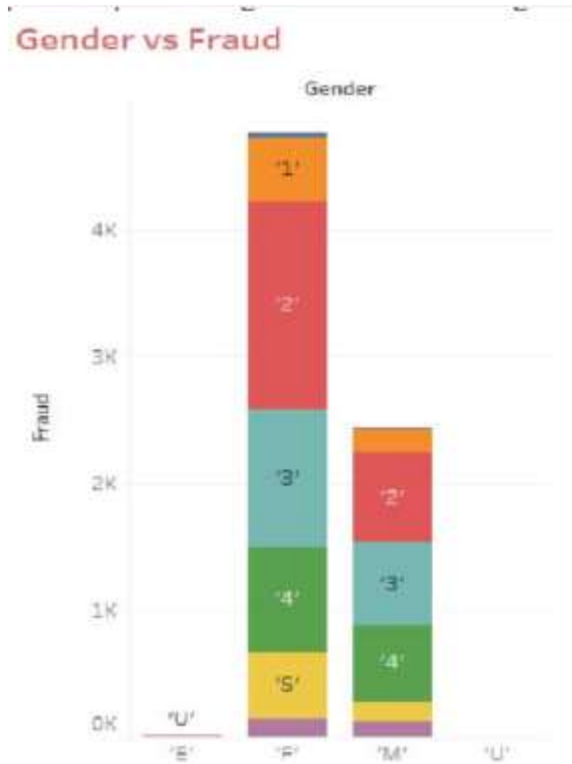


Fig 6.3 Fraud based on gender

VII.CONCLUSION

This project presents an effective machine learning approach for fraud detection in banking transactions by utilizing behavioral and transactional data to identify suspicious patterns. The system addresses the limitations of traditional rule-based methods by offering higher accuracy, adaptability, and real-time analysis. The results demonstrate that algorithms like Random Forest and XGBoost can significantly enhance fraud detection performance while reducing false alarms. This approach strengthens the overall security framework of financial institutions and helps in gaining customer trust by proactively mitigating fraud risks.

VIII.FUTURE SCOPE

In the future, the system can be improved by integrating deep learning models such as LSTM or Autoencoders for sequential pattern recognition. Additionally, using real-time streaming platforms like Apache Kafka can enable real-time fraud detection at scale. Incorporating graph-based techniques can help uncover hidden relationships between fraudulent accounts and transaction networks. Moreover, integrating blockchain technology may further enhance transparency and traceability in financial transactions. A global fraud detection consortium using shared anonymized datasets across banks could also lead to a more powerful and unified defense system.

IX.REFERENCES

1. Dal Pozzolo, A., et al. (2015). Calibrating probability with undersampling for unbalanced classification. IEEE Symposium Series on Computational Intelligence.
2. Bhattacharyya, S., et al. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems.
3. Jha, S., Guillen, M., & Westland, J. C. (2012). Employing transaction aggregation strategy to detect credit card fraud. Expert Systems with Applications.
4. Patil, P., & Sherekar, S. (2014). Performance analysis of Naive Bayes and J48 classification algorithm for data classification. International Journal of Computer Science.
5. Carcillo, F., et al. (2018). Streaming active learning strategies for real-life credit card fraud detection. International Journal of Data Science.
6. Phua, C., et al. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.
7. Whitrow, C., et al. (2009). Transaction aggregation as a strategy for credit card fraud detection. Data Mining and Knowledge Discovery.
8. Sahin, Y., & Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines. Proceedings of the International MultiConference of Engineers and Computer Scientists.
9. Wei, W., et al. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. World Wide Web Journal.
10. Kou, Y., et al. (2021). Artificial

intelligence for detecting banking fraud: A survey and new hybrid framework. Financial Innovation.