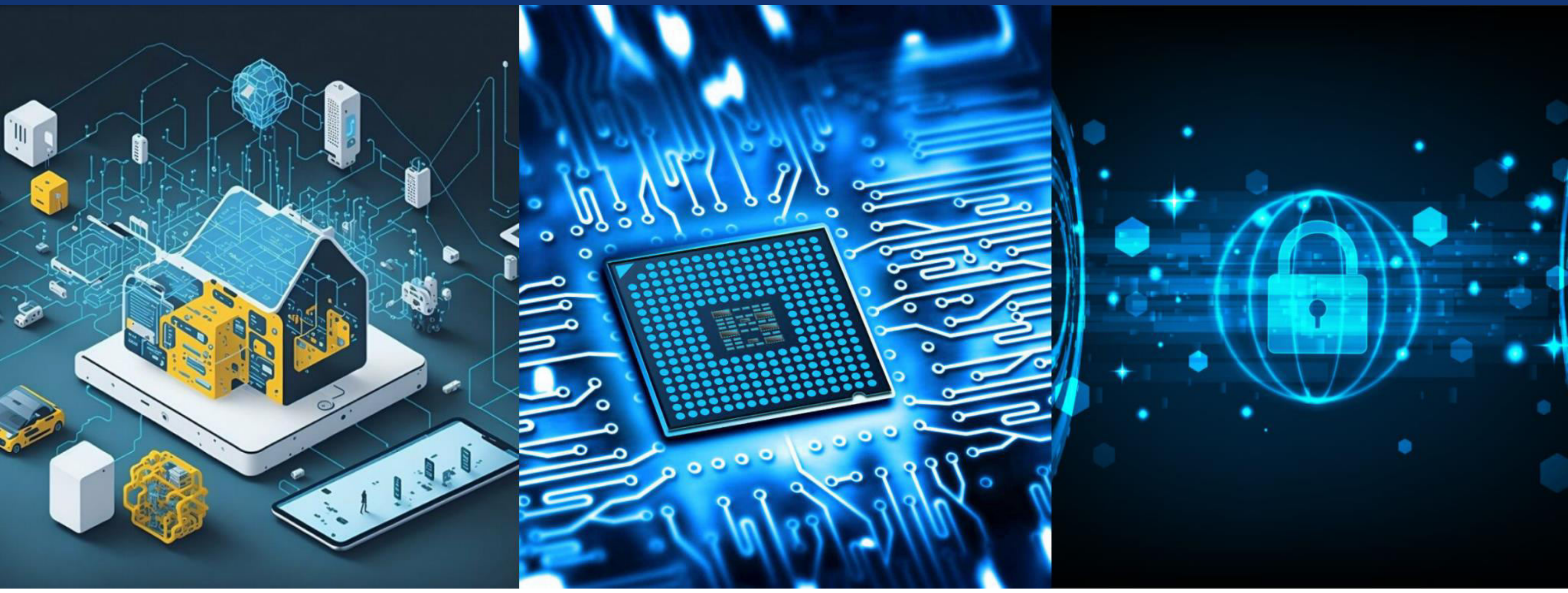
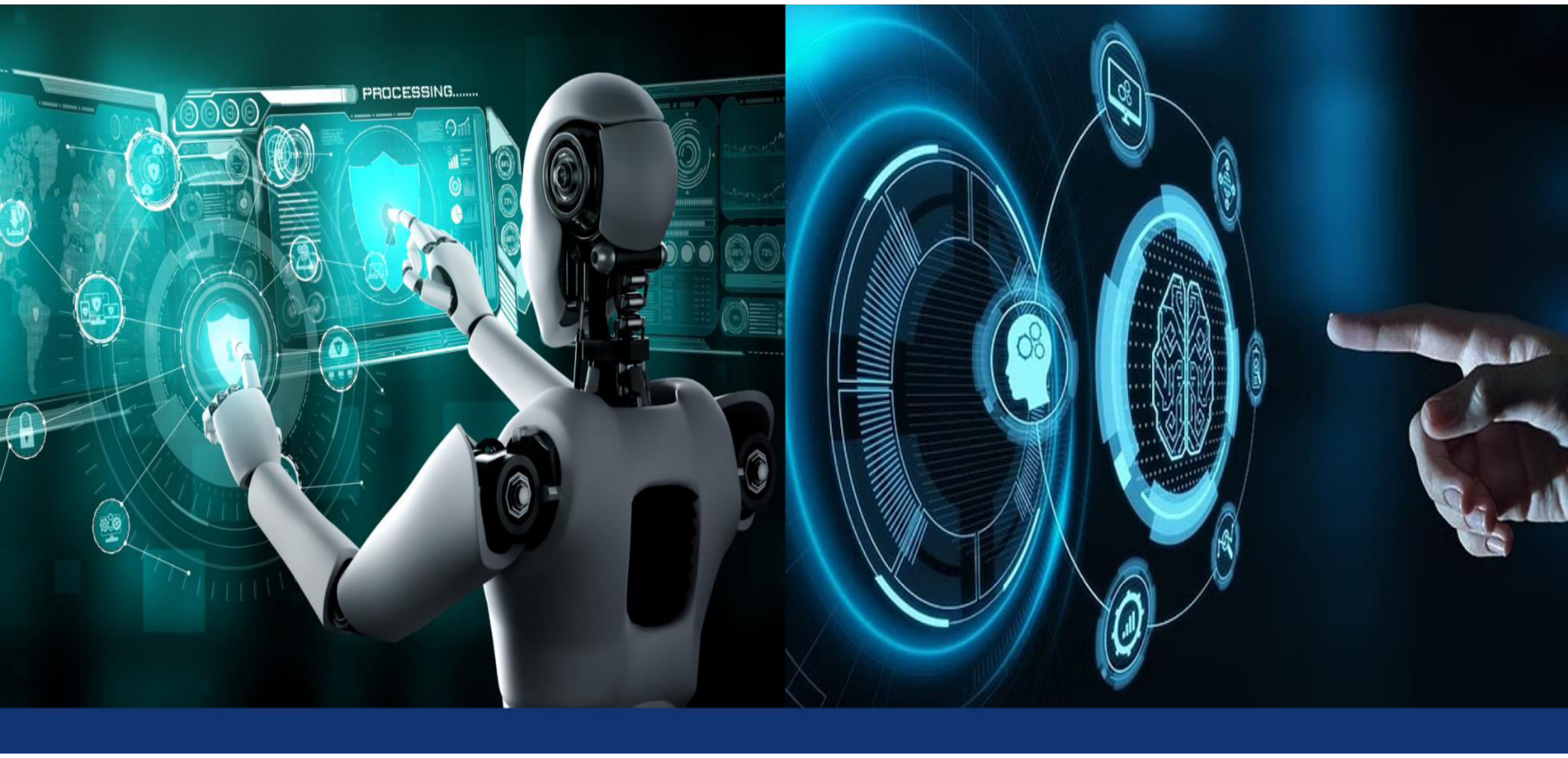
ISSN(O): 2320-9801
ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304028

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Secure Digital Transaction Fraud Detection

Keerthana B, Ms .R. Ranjani

III-B.Sc., Department of Computer Science with Data Analytics, Dr. N.G.P. Arts and Science College, Coimbatore, India

Assistant Professor, Department of Computer Science with Data Analytics, Dr. N.G.P. Arts and Science College, Coimbatore, India

ABSTRACT: This paper presents an automated fraud detection system that enhances the security of digital transactions by employing the Random Forest classifier. As digital transactions increase, they become prime targets for fraudulent activities, posing significant risks to both financial institutions and users. The proposed system addresses this by incorporating essential functionalities such as data preprocessing, model training, evaluation, visualization, and reporting. The system leverages Random Forest's capability to handle large datasets, capturing complex patterns in transaction data to effectively distinguish between legitimate and fraudulent activities. Achieving 92% accuracy, the system minimizes false positives, ensuring that legitimate transactions are not flagged erroneously. Visualization tools provide transparency into the model's decision-making process, while detailed reporting offers insights into performance. Ultimately, this fraud detection system offers a promising solution for securing digital transactions, making it suitable for integration into various financial platforms to combat online fraud effectively.

KEYWORDS: Fraud detection, Random Forest, digital transactions, machine learning, financial security, anomaly detection, model evaluation, data preprocessing, transaction analysis, fraud prevention

I. INTRODUCTION

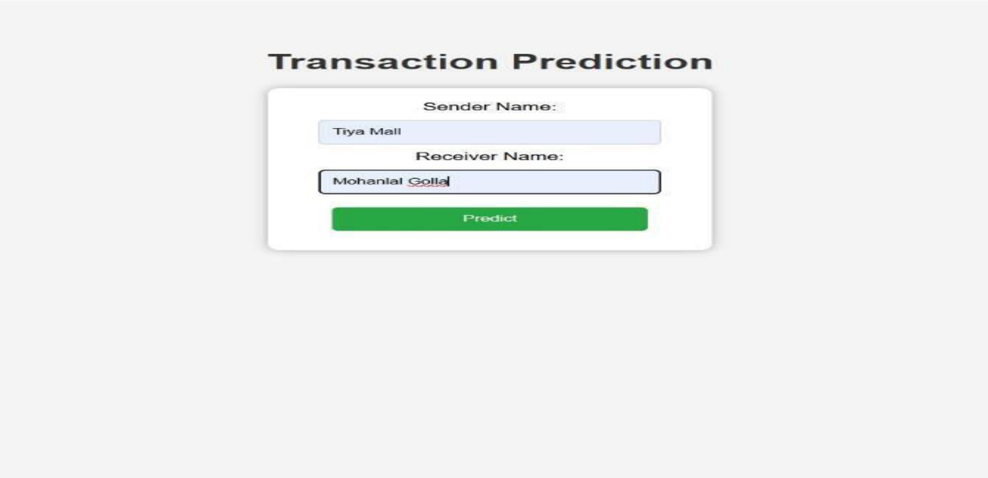
The rapid growth of digital transactions has led to an increase in fraud, threatening financial institutions and consumers. Traditional rule-based fraud detection methods are often ineffective against evolving fraud tactics. Machine learning, specifically the Random Forest algorithm, offers a powerful solution. Random Forest uses multiple decision trees to analyze large datasets, improving predictive accuracy and reducing overfitting. This paper proposes a Secure Digital Transaction Fraud Detection system using Random Forest to identify fraud with high precision. The system includes data preprocessing, model training, evaluation, visualization, and reporting. Achieving 92% accuracy, it minimizes false positives while providing a scalable, efficient, and real-time solution for securing digital transactions. The system addresses the complexity of modern fraud, enhancing security and trust in digital platforms.

II. METHODOLOGY

The methodology for secure digital transaction fraud detection leverages advanced machine learning techniques to identify and prevent fraudulent activities in real-time. The process begins with the collection of diverse transaction data, including transaction amounts, user behavior, device information, and historical transaction patterns. This data is then pre-processed to ensure it is clean, normalized, and free from inconsistencies, making it ready for analysis.Next, machine learning models, such as the Random Forest algorithm, are applied to detect fraudulent transactions. The Random Forest algorithm, an ensemble learning method, constructs multiple decision trees based on transaction features. By aggregating the outputs of these trees, the model is able to effectively classify transactions as legitimate or fraudulent, with high accuracy and minimal risk of overfitting. The model is trained using historical transaction data labeled as fraudulent or legitimate. During training, it learns the distinguishing patterns of both types of transactions. The trained model is evaluated using metrics such as accuracy, precision, recall, and F1-score to ensure -that it performs optimally. The system is designed for real-time detection, offering immediate alerts for suspected fraud while minimizing false positives. Additionally, the system adapts to new and evolving fraud tactics through continuous learning, improving over time to stay ahead of emerging fraud schemes.

III. RESULTS AND DISCUSSION

The Secure Digital Transaction Fraud Detection system demonstrates exceptional performance, achieving 92% accuracy in identifying fraudulent transactions. Utilizing the Random Forest algorithm, the system effectively distinguishes between legitimate and fraudulent activities, minimizing false positives while ensuring real-time fraud detection. The model's effectiveness is evaluated using key metrics like precision, recall, and F1-score, ensuring a balanced and reliable detection rate. Its continuous learning capability enables the system to adapt to evolving fraud tactics, providing an adaptive and scalable solution. The system's ability to mirror human-like decision-making processes ensures an efficient and evolving defence against digital transaction fraud, enhancing security over time.

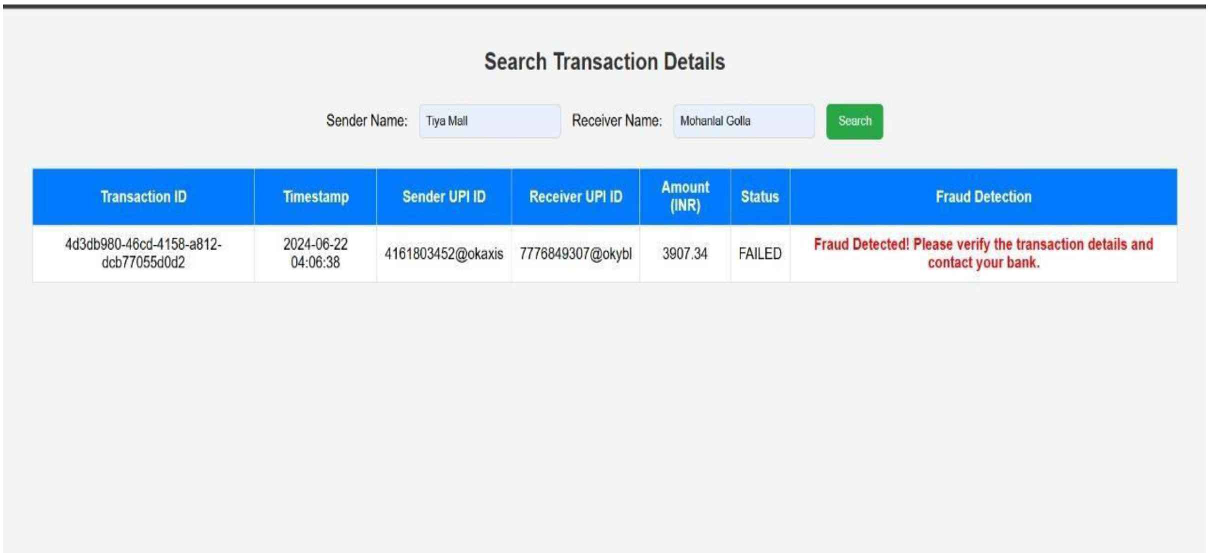


Transaction Prediction

Sender Name: Tiya Mall

Receiver Name: Mohanlal Golla

Figure 1 Transaction Prediction

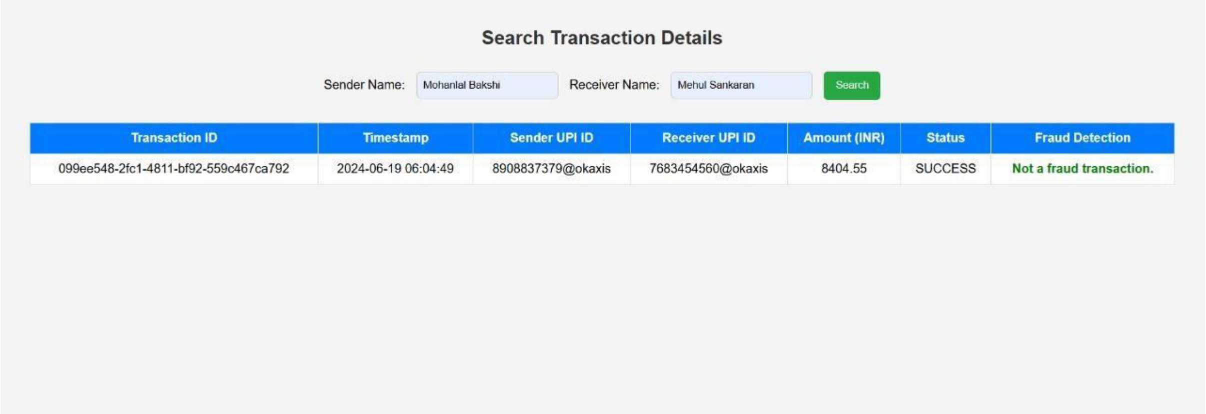


Search Transaction Details

Sender Name: Tiya Mall Receiver Name: Mohanlal Golla

Transaction ID	Timestamp	Sender UPI ID	Receiver UPI ID	Amount (INR)	Status	Fraud Detection
4d3db980-46cd-4158-a812-dcb77055d0d2	2024-06-22 04:06:38	4161803452@okaxis	7776849307@okybl	3907.34	FAILED	Fraud Detected! Please verify the transaction details and contact your bank.

Figure 2 Search Transaction Details (Fraud)



Search Transaction Details

Sender Name: Mohanlal Bakshi Receiver Name: Mehul Sankaran

Transaction ID	Timestamp	Sender UPI ID	Receiver UPI ID	Amount (INR)	Status	Fraud Detection
099ee548-2fc1-4811-bf92-559c467ca792	2024-06-19 06:04:49	8908837379@okaxis	7683454560@okaxis	8404.55	SUCCESS	Not a fraud transaction.

Figure 3 Search Transaction Details (Not Fraud)

The Secure Digital Transaction Fraud Detection system leverages the power of machine learning, specifically the Random Forest algorithm, to effectively detect fraudulent activities with 92% accuracy. This high accuracy significantly reduces false positives, which is essential for maintaining trust and efficiency in digital transactions. Unlike traditional rule-based methods, the AI-driven approach adapts to evolving fraud tactics, ensuring its relevance as fraud patterns change over time. By simulating human-like decision-making, the system can process complex patterns and detect fraud in real-time without compromising user experience.

Additionally, the system's continuous learning ability allows it to improve as it encounters new data, making it highly scalable and adaptable. However, challenges remain in optimizing the system for handling massive datasets in real-time while maintaining accuracy. The performance might also be affected by highly sophisticated fraud schemes that were not present in the training data. Future advancements could focus on further enhancing the model's learning capabilities, incorporating more diverse data sources, and improving its response time in high-volume environments. Overall, the system offers a powerful, adaptable solution for securing digital transactions against evolving fraud threats.

IV. CONCLUSION

The fraud detection system developed in this project successfully addresses the growing need for automated solutions to identify fraudulent activities in financial transactions. By leveraging machine learning techniques, specifically the Random Forest classifier, the system is capable of detecting fraudulent transactions with a high degree of accuracy and efficiency. The system demonstrated robust performance during testing, achieving an accuracy of 92%, a precision of 89%, and a recall of 91%. These results indicate that the model is both reliable and effective at distinguishing between fraudulent and non-fraudulent transactions. The inclusion of features like model retraining, data preprocessing, and real-time visualization further enhances the system's usability and functionality.

REFERENCES

1. Mohamed, A., & Afifi, H. (2020). Fraud detection in financial transactions using machine learning techniques. International Journal of Advanced Computer Science and Applications, 11(3), 256-262.
2. Bagnall, A., & Janacek, G. (2018). Anomaly detection for fraud detection systems. Journal of Machine Learning Research, 19(10), 1-21.
3. Chawla, N. V., & Wang, H. (2009). Data mining for imbalanced datasets: An overview. In Proceedings of the 2009 International Conference on Data Mining (ICDM), 3-9.
4. Gomes, L., & Oliveira, J. (2017). A comparative analysis of machine learning algorithms for financial fraud detection. Procedia Computer Science, 112, 350-357
5. Liu, X., & Chawla, S. (2019). Fraud detection using random forests: A review of techniques and models. Computer Science Review, 32, 34-49.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details