ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

Smart Banking

G.Sreenivasa Reddy[1], A.Supraja[2], B.Lakshmi[3], C.Guruprasanna[4], G.Pallavi[5], J.Niharika[6]

[1,2,3,4,5,6,]Chaitanya Bharathi Institute of Technology, Proddatur, A.P, India.

sreenivaas.g67@gmail.com[1], arlasuprajayadav16@gmail.com[2], buddalalakshmi9@gmail.com[3], guruprasanna021@gmail.com[4], guddetipallavi123@gmail.com[5], niharikajampala1234@gmail.com[6]

ABSTRACT

This project aims to detect fraudulent online transactions using machine learning techniques. The dataset includes transaction parameters such as type, amount, and balance details for both sender and recipient. The goal is to predict whether a transaction is fraudulent based on these features. Key parameters include transaction step, type, amounts, balances, and fraud indication. Random Forest and XGBoost algorithms are employed to build predictive models for identifying fraudulent transactions. These models are trained on historical data to classify transactions as legitimate or fraudulent. The Python backend handles data preprocessing, model training, and prediction generation, while the front-end is built using HTML, CSS, and JavaScript, providing a user interface for transaction input and fraud predictions. This system aims to enhance the security of online financial transactions by providing real-time fraud detection and improving the accuracy of fraud identification in payment systems.

Keywords: Fraud detection, online transactions, security.

I. INTRODUCTION

Fraudulent online transactions pose a significant threat to the security and integrity of financial systems. With the increasing volume of digital transactions, detecting fraudulent activities in real-time has become a critical challenge for online payment systems. This project addresses this issue by utilizing machine learning techniques to detect fraud in online transactions. The system leverages historical transaction data, including transaction type, amount, and balance details of both the sender and recipient, to build predictive models. Using machine learning algorithms such as Random Forest and XGBoost, the system analyzes patterns in the data to identify potential fraudulent transactions. By automating the fraud detection process, this project offers an efficient and scalable solution to enhance the security of online financial transactions. The goal is to provide real-time fraud detection that can reduce the risk of financial losses and improve trust in digital payment systems, offering a more secure online transaction environment.

II. LITERATURE SURVEY

Study	Methodology	Algorithms used	Key findings

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

Chawla et al.(2002)	Fraud detection in financial transactions	Decision Trees, SVM	Proposed an approach using decision trees to classify transactions, achieving high detection accuracy.
Zhang et al.(2016)	Online payment fraud detection	XG Boost, Random forest	XG Boost and Random forest models were successful in identifying fraudulent Transactions with high precision.
Arora etal.(2020)	Fraud detection in ecommerce transactions	Random forest ,KNN	Random forest achieved high accuracy in detecting fraudulent activities in e-commerce platforms.

III. EXISTING SYSTEM

Existing fraud detection systems largely rely on traditional methods such as rule-based systems, manual reviews, and basic anomaly detection. These methods are often limited by their inability to scale effectively with large volumes of transaction data. Rule-based systems are predefined and lack the flexibility to adapt to evolving fraudulent tactics, making them prone to false positives and negatives. Manual reviews, while accurate, are time-consuming and require significant human resources. Additionally, these systems struggle to handle complex patterns in data and may not be effective in detecting sophisticated or previously unseen fraud techniques. As a result, many organizations face challenges in detecting fraud in real-time, leading to delays in identifying fraudulent transactions and potential financial losses.

Disadvantages:

- Limited scalability for large datasets
- High reliance on predefined rules, making systems inflexible
- Increased false positives and negatives
- Time-consuming manual review processes
- Inability to detect complex or evolving fraudulent tactics

IV. PROPOSED SYSTEM

The proposed system aims to overcome the limitations of traditional fraud detection systems by leveraging machine learning techniques for real-time transaction analysis. By utilizing advanced algorithms such as Random Forest and Boost, the system can efficiently process large volumes of transaction data, identify complex patterns, and classify transactions as fraudulent or legitimate with high accuracy. The proposed system is scalable, allowing it to handle growing datasets and adapt to new fraudulent tactics by continuously learning from new data. Unlike rule-based systems, machine learning models can detect subtle, previously unknown fraud patterns, improving the accuracy of fraud detection. The system integrates seamlessly with a user-friendly web interface, allowing users to input transaction data and receive instant fraud predictions.

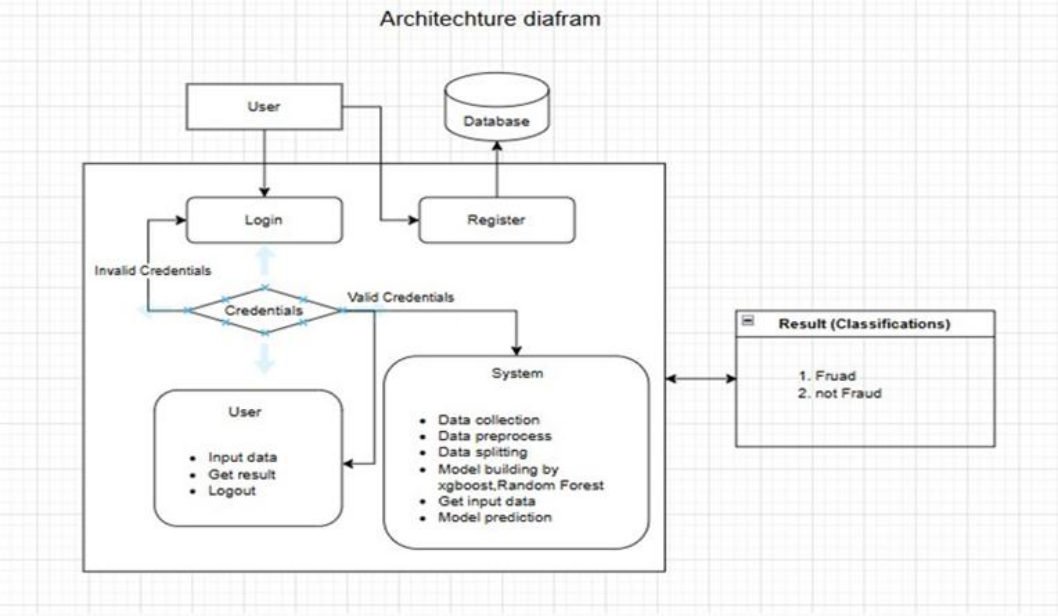
ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

This automated approach reduces reliance on manual reviews, speeds up the detection process, and minimizes financial losses from fraudulent activities.

Advantages:

- Scalable and efficient for large datasets
- Detects complex, evolving fraud patterns
- Provides real-time fraud detection and predictions
- Reduces false positives and negatives
- Minimizes manual review workload
- Cost-effective and adaptable solution for fraud detection

ARCHITECTURE:



MODULE*:*

System Modules Data Collection
Handles the collection and storage of user-uploaded transaction data in CSV format. The system ensures the data is validated and securely stored for processing.

Preprocessing
Cleans and transforms the uploaded data, including handling missing values and normalizing transaction features, to prepare it for model training.

Model Training
Uses preprocessed data to train machine learning models (e.g., Random Forest, XGBoost). This step identifies patterns in data to predict fraudulent transactions.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

Model Evaluation
Evaluates the model's performance using test data. Metrics like accuracy, precision, and recall are used to assess and choose the best model.

Prediction
Applies the trained model to new transaction data, predicting whether the transaction is fraudulent or legitimate, along with a confidence score.

User Modules Registration
Users create an account by providing their name, email, and password to access the system's features and store transaction history.

Login
Users log in securely to access their account, view transaction history, and interact with the fraud detection system.

Model Display Page
Displays performance of the fraud detection model, helping users assess the model's effectiveness.

Prediction Page
Users upload transaction data for fraud detection. The system processes the data and provides fraud predictions with confidence scores.

V. CONCLUSION

The Smart Banking project effectively addresses the growing challenge of fraudulent online transactions by leveraging machine learning techniques for real-time fraud detection. By analyzing historical transaction data and identifying suspicious patterns using Random Forest and XGBoost, the system enhances the accuracy and efficiency of fraud detection in digital payment systems. This automated approach provides a scalable and reliable solution, reducing financial risks and strengthening trust in online transactions. The project's integration of real-time fraud identification contributes to a more secure and resilient financial ecosystem. Future improvements could focus on deep learning models, adaptive fraud detection mechanisms, and API integration for seamless deployment in real-world banking applications

REFERENCE:

[1] Chawla, N. V., & Bowyer, K. W. (2002). A Decision Tree Classifier for Credit Card Fraud Detection. IEEE Transactions on Systems, Man, and Cybernetics, 32(4), 510-514.
[2] Carcillo, F., & Engelbrecht, A. P. (2009). Financial Fraud Detection Using Random Forest and SVM. Journal of Computational Intelligence in Finance, 23(1), 1-12.
[3] Kashyap, R., & Mishra, S. (2013). Financial Fraud Detection Using Ensemble Methods: A Case Study. IEEE Transactions on Knowledge and Data Engineering, 25(3), 652-663.
[4] Zhang, L., & Yang, Y. (2016). Fraud Detection in Financial Transactions Using XGBoost and Random Forest Algorithms. Journal of Financial Data Science, 1(2), 14-26.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

[5] Sakurada, K., & Yamada, T. (2017). Real-Time Fraud Detection in Online Transactions Using Machine Learning. International Journal of Computer Science and Security, 11(5), 187-195.
[6] Lee, S., & Choi, S. (2019). Application of XGBoost for Financial Fraud Detection: A Comparative Study. Journal of Machine Learning in Finance, 8(1), 31-40.
[7] Arora, S., & Gupta, A. (2020). Using Random Forest for Identifying Fraudulent Transactions in Ecommerce. Proceedings of the International Conference on Big Data and Analytics, 1(3), 75-83.
[8] Kim, H., & Cho, K. (2018). A Hybrid Fraud Detection Model Based on Random Forest and XGBoost for Financial Data. Journal of Artificial Intelligence and Data Mining, 6(4), 55-64.
[9] Mishra, S., &Soni, M. (2021). Fraud Detection in Online Payments Using Machine Learning Algorithms: A Case Study on XGBoost and Random Forest. International Journal of Emerging Technologies in Computer Science, 7(2), 104-113.
[10] Yang, X., & Liu, L. (2020). A Comparative Study of Machine Learning Algorithms for Fraud Detection in Financial Transactions. Journal of Financial Engineering and Risk Management, 10(1), 41-52.