UPI transaction security: Fraud detection using machine learning algorithm

SELVI S[1], DHINOOVIKA D[2], HARSHANA R[3], MUTHULAKSHMI R[4]
[1]Associate Professor, [2,3,4]Final Year Students,
Department of Computer Science and Engineering, Government College of Engineering, Bargur, Krishnagiri, Tamil Nadu, India [1]s.selvi@gcebargur.ac.in, [2]dhinoovikadevarajan@gmail.com,
[3]Kaveripandurangan03902@gail.com, [4]muthulakshmi110104@gmail.com

Abstract

With the rapid adoption of digital payments, fraudulent transactions have end up a tremendous problem, in particular in Unified Payments Interface (UPI) transactions. Traditional rule-based fraud detection strategies often fail to stumble on sophisticated fraud patterns. The study provides a machine learning-driven UPI fraud detection system, integrating Random Forest, Decision Tree, and Convolutional Neural Network (CNN) models to categories transactions as fraudulent or non-fraudulent. The Random Forest model established sturdy performance because of its ensemble learning method, at the same time as the CNN model leveraged deep learning techniques to capture complex transaction patterns. The device is similarly incorporated into a Flask-based web application, allowing customers to test transaction authenticity in real-time. Comparative evaluation of the models primarily based on accuracy highlights the effectiveness of ensemble learning and deep learning for fraud detection. This research contributes to the development of financial security through improving the accuracy and performance of fraud detection mechanisms in digital payment systems.

Keywords: Convolutional Neural Network, Decision Tree, Digital Payments, Random Forest.

I. Introduction

A. Background and Motivation

The rapid evolution of digital payments has revolutionized financial transactions, offering users with seamless and immediate cash transfers. The Unified Payments Interface (UPI) has emerged as a leading digital payment system, enabling Peer-to-Peer (P2P) and business transactions with minimal latency. However, with the growing adoption of digital payments, fraudulent activities consisting of Identification theft, Unauthorized transactions, and Phishing attacks have become increasingly more familiar.

Traditional fraud detection systems depend upon rule-based algorithms, where transactions are flagged primarily based on predefined situations along with transaction amount thresholds, frequency, or suspicious IP addresses. While these methods offer a simple layer of security, they fail to discover sophisticated fraud patterns that evolve over time. Machine Learning (ML) and Deep Learning (DL) have emerged as effective solutions able to identifying hidden patterns in transactional data, improving fraud detection accuracy in real time.

B. Problem Statement

Detecting fraud in UPI transactions poses particular challenges due to the high extent of transactions, actual-time processing necessities and the evolving nature of fraudulent activities. Fraudsters employ numerous processes, together with social engineering, synthetic identities, and transaction manipulation, making it difficult for rule-primarily based systems to preserve up. false positives and false negatives further complicate fraud detection.

Table 1 Annual Fraud percentage trends (2014-2023)

YEAR	PERCENTAGE OF FRAUD
2014	1.8%
2015	2.9%
2016	4.7%
2017	6.6%
2018	9.45%
2019	11.8%
2020	14.1%
2021	13.9%
2022	16.9%
2023	17.8%

"Table 1" denotes data on the percentage of fraud determined annually from 2014 to 2023. It highlights a clear upward trend in fraudulent activities over the decade. In 2014, the fraud percentage was 1.8%, which gradually expanded every year, reaching 4.7% in 2016 and then growing sharply to 14.1% through 2020. although there was a slight dip in 2021, with the share falling to 13.9%, the numbers resumed their upward trajectory inside the following years, peaking at 17.8% in 2023. This consistent rise—especially the sharp surge between 2016 and 2020—may also reflect growing vulnerabilities in systems or an increase in digital transactions without corresponding enhancements in security. The statistics underscores the need for extra robust fraud detection and prevention measures.

The pie chart "Figure 1" represents the percentage of fraud detected in UPI transactions from 2014 to 2023. Each slice corresponds to a specific 12 months, showing the percentage of fraud cases identified. The statistics reveal a slow increase in fraudulent activities over the years, with significant jumps in certain periods. the highest fraud percentage is recorded in 2023 at 17.8%, indicating an ongoing challenge in securing digital payment structures. The chart provides a clear visual representation of the evolving fraud landscape and the need for continuous enhancements in fraud detection techniques.

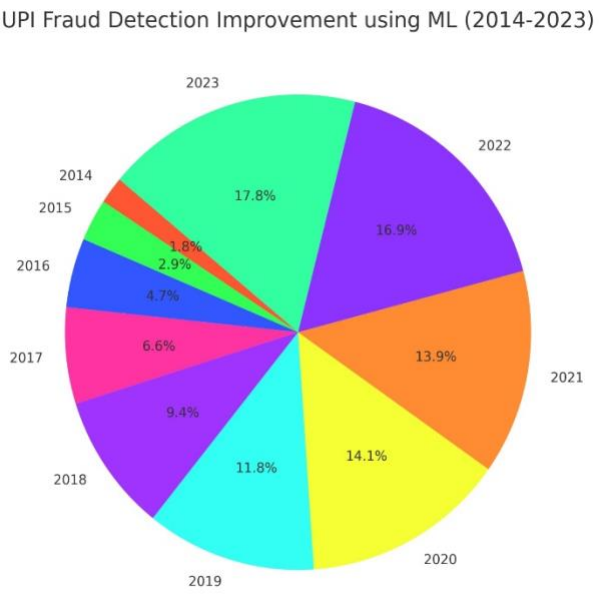

Figure 1: UPI fraud detection enhancement

C. Research Objectives

The primary goals of this research are to:

- Develop and examine multiple machine learning models for UPI fraud detection.
- Analyze key transaction attributes (UPI number, transaction amount, date, zip code) to pick out fraud patterns.
- Evaluate model performance in terms of accuracy.

D. Methodology Overview

The study follows a data-driven approach, beginning with information preprocessing, observed by Machine learning model training and evaluation, and finally deploying the best model into a web-primarily based fraud detection system. the key steps include:

- Dataset training: Gathering and Preprocessing a established dataset containing UPI transaction data.
- Version Training & Evaluation: Training three machine learning models (Random Forest, decision Tree, and CNN) and comparing their accuracy.
- Web Application Improvement: Deploying the trained model using Flask, enabling users to enter transaction details and receive fraud predictions in real time.

E. Datasets

The dataset used in this research is sourced from Kaggle and contains UPI transaction records for fraud detection. It includes transaction information such as UPI number, transaction quantity, date, and zip code, along with a fraud label indicating whether a transaction is fraudulent or legitimate. To ensure effective training and evaluation, the dataset is split into two separate documents: a training dataset containing 80% of the records and a testing dataset with the remaining 20%.

II. Related Work

Abdulaleem Ali et al. (2023) conducted a systematic review on financial fraud detection using machine learning, exploring Decision Trees and Random Forest models while assessing their accuracy, precision, recall, and F1-score, highlighting the challenges of real-world datasets and the reliance on synthetic data [1]. Amal Al Ali, Ahmed M. Khedr, and Magdi El-Bannany (2023) proposed an optimized XGBoost ensemble learning model for financial statement fraud detection in the MENA region, which outperformed traditional models but required extensive hyperparameter tuning [5]. Ebenezer Esenogho and Ibomoiye Dom or Mienye

(2022) introduced a neural network ensemble model with feature engineering to improve credit card fraud detection, where their LSTM-based approach enhanced sensitivity and specificity but required high-quality training data [8]. Gangi Setty Raj Charan and K. Deepa Thilak (2023) developed a machine learning-based detection model for phishing links and QR codes in UPI transactions, providing real-time fraud prevention but being computationally demanding [12]. Elena Flondor, Liliana Donath, and Mihaela Neamtu (2024) investigated decision tree algorithms for automatic credit card fraud detection, showing strong interpretability but struggling with data imbalance and overfitting [9].

Abdulwahab Ali Almazroi and Nasir Ayub (2023) developed a real-time fraud detection model using ResNeXt-GRU (RXT) and Jaya optimization, achieving a 10%-18% performance improvement over existing models but facing challenges in implementation complexity [2]. Emmanuel Ileberi, Yanxia Sun, and Zenghui Wang (2022) applied Genetic Algorithms (GA) for feature selection in fraud detection, improving accuracy and reducing computational complexity but facing issues with imbalanced datasets [10]. Dahee Choi and Kyungho Lee (2017) applied machine learning techniques such as expectation maximization (EM) and K-Means for fraud detection in mobile payment systems, effectively detecting fraudulent patterns but being computationally intensive [6]. Hadeel Ahmad, Bassam Kasasbeh, and Enas Rawashdeh (2023) introduced a class balancing framework for credit card fraud detection, where their fuzzy C-Means clustering approach improved accuracy but required resource-intensive computation [13]. Sayalee S. Bodade and P.P. Pawade (2023) reviewed UPI fraud detection methods using supervised learning classifiers and anomaly detection techniques, emphasizing the need for continuous to detect emerging fraud patterns [24].

Ibrahim Y. Hafez et al. (2025) conducted a systematic review of AI techniques in credit card fraud detection, covering machine learning, deep learning, and meta-heuristic optimization approaches but noting difficulties in training models due to the rarity of fraud cases [14]. Mengran Zhu, Yulu Gong, and Yafei Xiang (2024) investigated the use of Generative Adversarial Networks (GANs) for fraud detection, effectively identifying fraudulent transactions but facing challenges in generating high-fidelity synthetic data [17]. Jonathan Kwaku Afriyie et al. (2023) analyzed supervised machine learning models for fraud detection, identifying Random Forest as the best-performing model with 96% accuracy but noting high computational costs [15]. Jonathan M. Karpoff (2021) examined financial fraud trends over time, highlighting the influence of technology and wealth on fraud incidence while exploring fintech innovations like blockchain for fraud prevention [16]. Ahsan RB and Suresh Kumar KR (2021) developed a fraud detection model using Artificial Neural Networks (ANN), Support Vector Machines (SVM), and k-nearest Neighbors (KNN), highlighting ANN's effectiveness in handling complex transaction patterns but requiring extensive computational resources [4].

Mohapatra S. et al. (2017) analyzed the security vulnerabilities of UPI and digital payment systems in India, identifying key threats and proposing mitigation strategies for improved financial security [18]. Paolo Vanini et al. (2023) integrated anomaly detection with economic risk management for online fraud prevention, balancing detection accuracy with economic considerations but facing challenges in implementation complexity [20]. Rupa Rani and Adnan Alan (2022) proposed a machine learning-driven fraud detection system for UPI transactions, using Random Forest, XGBoost, and SVM to provide real-time detection but requiring extensive dataset training [21]. Sara Makki et al. (2019) conducted an experimental study on imbalanced classification approaches in fraud detection, evaluating SMOTE-based neural networks and decision forests while highlighting the challenges of class imbalance [23].

Abhilash Sharma M., Ganesh Raj B., and Ramamurthy B. (2022) proposed an auto-encoder-based deep learning approach for credit card fraud detection, where the unsupervised learning method demonstrated high adaptability to evolving fraud patterns but was dependent on the quality of input data [3]. Sakeena Kanakkayil (2023) contributed to financial fraud detection in the MENA region by optimizing the XGBoost algorithm. The model, which included SMOTE, SVM, AdaBoost, and Random Forest, showed better predictive power than traditional models but required extensive hyperparameter tuning, making it computationally demanding [25]. S.K.L. Naikl, A. Kiran, and V.P. Kumar (2024) explored AI and ML techniques for UPI fraud detection, improving real-time fraud prevention but struggling with evolving fraud patterns [22]. Eleanor Mill, Wolfgang Garn, and Nick Ryman-Tubb (2023) explored Explainable AI (XAI) in real-time fraud detection, emphasizing the importance of

transparency in AI decision-making but facing challenges in balancing explainability with accuracy [7]. Fawaz Khaled Alarfaj and Shabnam Shahzadi (2023) leveraged Graph Neural Networks (GNNs) and Autoencoders for real-time credit card fraud detection, capturing complex transaction relationships but requiring large labeled datasets [11]. Noor Saleh Alfaiz and Suliman Mohamed Fati (2022) developed a credit card fraud detection model using CatBoost and AllKNN under sampling, achieving high accuracy but being computationally expensive [19].

III. PROPOSED WORK

The proposed work focuses on improving UPI fraud detection through leveraging machine learning models, along with the Random Forests, Decision Tree, and Convolutional Neural Networks (CNNs). Unlike the conventional rule-based detection, these models can analyze massive datasets, identify hidden patterns, and predict unseen transactions. The dataset is preprocessed by extracting transaction info, normalizing values, splitting the facts into training, and testing units. This ensures better generalization and accurate fraud detection.

"Figure 2" outlines a machine learning pipeline for detecting UPI fraud. It starts with loading a UPI fraud dataset from a CSV file, followed by splitting the dataset into features and target variables. The dataset is then divided into 80% training and 20% testing units. multiple models are trained, including a Random Forest, decision Tree, and a Convolutional Neural network with Min-Max feature normalization. The pipeline also involves developing a Flask web application where an index page is created for user input, and transaction details are captured. finally, the Flask application is deployed to allow users to check the fraud status of transactions.

The Random Forest and Decision Tree classifiers help detect fraudulent transactions by analysing decision-based patterns in transaction attributes. Meanwhile, the CNN model, normally used for picture recognition, is adapted to process numerical transaction data. CNNs use multiple layers, including batch normalization and dropout, to improve accuracy and prevent overfitting. Training those models on a large dataset allows them to examine complex fraud patterns, leading to better fraud detection compared to static rule-based systems. Additionally, the system compares the accuracy of all models using bar charts and performance metrics. By incorporating predictive analytics, the machine can proactively come across fraudulent transactions, even when no exact match exists in historic records. This ensures a more robust and dynamic method for UPI fraud detection, enhancing security for digital transactions.

"Figure 3" illustrates the architecture of a UPI Fraud Detection system, integrating Random Forest, decision trees, and Convolutional Neural Networks for fraud detection. It consists of multiple layers, each serving a particular purpose. The data input Layer includes the UPI Transaction Dataset, which provides transaction information such as UPI number, amount, date, and zip code.

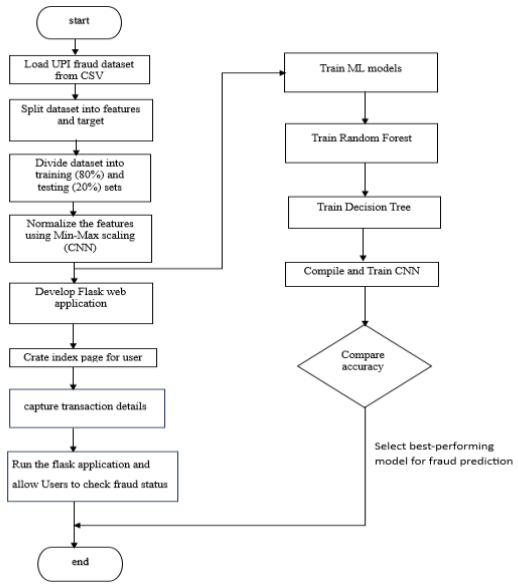

Figure 2: Flowchart of UPI fraud detection.

The dataset is fed into the model training Layer, where three models, Random Forest, decision Tree, and a CNN architecture, are trained for fraud detection. The CNN consists of multiple layers, which include dense layers with ReLU activation, batch normalization, dropout, and a final sigmoid activation layer for classification.

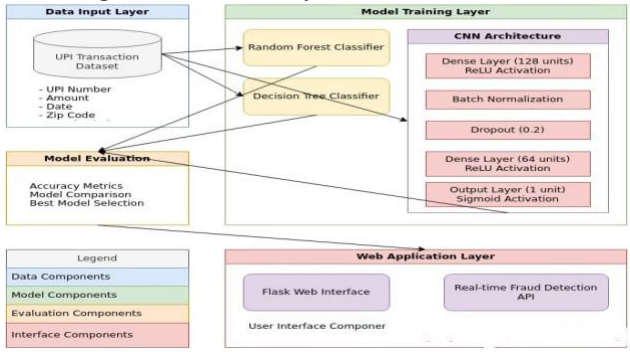

Figure 3: System Architecture of UPI Fraud Detection using Machine Learning

III. Pseudocode

The pseudocode of the RF, DT and CNN are explained here under.

A. Random Forest Algorithm

Importing the necessary packages
Example: import pandas as pd
def RF
Step 1: START
Step 2: Reading the dataset. pd.read.csv (file name) reads the dataset file
Step 3: Data cleaning and preprocessing of data. Data is scaled and normalized using Equation (1). Here X' is scaled value, X is original value, X_{min} is minimum value and X_{max} is maximum value.

$$X' = \frac{X - Xmin}{Xmax - Xmin} \quad (1)$$

Dataset is splited into two set as train data and test data using split() on training data is used to split the data.
Step 4: Training the data using the RF algorithm. RF classifier is called as RandomForestclassifier() which predicts whether transaction fraud or nonfraud.
Step 5: Calculating the fraud transactions and valid transactions, then calculating the accuracy using Equation (2) and stored in the respective locations. Here TP is True Positive, TF is True Negative, FP is False Positive and FN is False Negative.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

Step 6: STOP

B. Decision Tree

Importing the necessary packages
Example: import pandas as pd
def DT
Step 1: START
Step 2: Reading the dataset. pd.read.csv.
Step 3: Data Cleaning and Preprocessing of Data. Scale and normalize features using Equation (1).
Split the dataset into train and test sets using train_test_split().
Step 4: Train Decision Tree Model
Decision tree classifier is called as DecisionTreeClassifier() which predicts whether transaction fraud or nonfraud.
Step 5: Predict and Evaluate Model.
Assess the performance of the transaction model and determine its accuracy using Equation (2) and then stored in the respective location.
Step 6: STOP

C. Conventional Neural Network

The CNN algorithm has two parts: the Training part and the Testing part .

Training Part:

def CNN
Step 1: START
Step 2: Load and read the dataset.pd.read_csv
Step 3: Data Pre-processing
Feature scaling using Equation(1)
Split data into training and testing sets using train_test_split()
Step 4: Training the CNN Model using Equation (3)
Define CNN layers with the Dense, Batch Normalization, Dropout.

$$ReLU(X) = \max(0, X) \quad (3)$$

Compile model with the optimizer using Equation (4) and loss. Here V represents momentum, β denotes exponential decay rate, ∇W is gradient of loss function.

$$V = \beta V + (1 - \beta)\nabla W \quad (4)$$

Step 5: Save trained model (as training takes time)
Step 6: STOP

Testing Part:

def Test_CNN
Step 1: START
Step 2: Load trained CNN model
Step 3: Use model.predict() on new transaction data.
Step 4: Determine if the transaction is fraudulent or not.
Step 5: STOP

IV. Results and discussions

Random Forest demonstrated strong overall performance due to its ensemble learning mechanism, which reduces overfitting and effectively captures complex data patterns. Decision trees, although easy to interpret, suffered from overfitting, main to decrease generalization and reduced accuracy. CNNs, that are usually powerful in picture-primarily based obligations, have been applied to tabular data in this case.

The comparison indicates that traditional machine learning models like Random Forest are more effective for tabular fraud detection data. decision trees, in spite of their simplicity, lacked robustness, and CNNs, even as effective, had been not optimized for structured fraud datasets. Random forest struck a balance between interpretability and overall performance, making it the most suitable choice

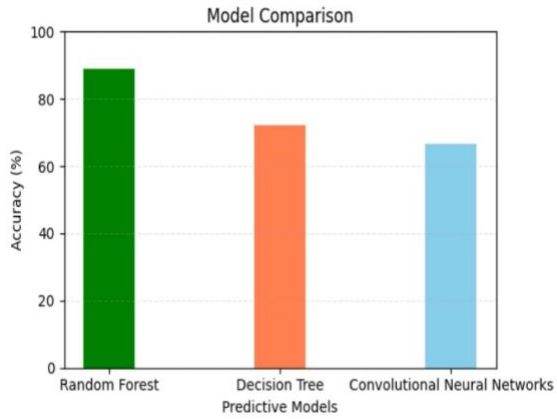

Figure 4: Accuracy comparison of predictive models

"Figure 4" provides a comparison of the accuracy of three predictive models: Random Forest, Decision Tree, and Convolutional Neural Networks (CNN). The y-axis represents accuracy as a percentage, while the x-axis lists the 3 models. Each bar is colored differently to distinguish between the models. The chart provides a visual representation of how each
model performed in terms of accuracy, allowing for an easy comparison of their effectiveness in the given task.

V. Conclusion

The proposed method has demonstrated its effectiveness in addressing the challenges in the area. By leveraging advanced methodologies, the study presents promising results that highlight the potential for further improvement. The findings indicate that refining key parameters, expanding the dataset, and integrating models and hybrid approaches may yield further insights and enhance the robustness of the solution.

While the current study makes valuable contributions, its applicability can be further extended to real-world scenarios through additional validation and testing on diverse datasets. Future research can also focus on incorporating real-time adaptability and automation to optimize decision-making processes. Moreover, assessing the ethical and security implications of the proposed methodology will ensure its responsible deployment in realistic environments. This work lays a robust foundation for persevering improvements, encouraging further exploration and refinement in this field. By addressing these areas, researchers can unlock new possibilities and drive

References

1. Abdulaleem Ali et al, "Financial Fraud Detection Based on Machine Learning", www.taylorandfrancis.com, CC BY-NC-ND 4.0license, 2023.

2. Abdulwahab Ali Almazroi, Nasir Ayub, "Online Payment Fraud Detection Model Using ML", IEEE Access, DOI:10.1109/ACCESS.2023.3339226,2023.

3. Abhilash Sharma M, Ganesh Raj B, Ramamurthy B, Hari Bhaskar R, "Credit Card Fraud Detection Using Deep Learning Based on Auto-Encoder" ITM Web of Conferences DOI: 10.1051/itmconf/20225001001,2022.

4. Aha RB, Suresh Kumar KR, "Credit Card Fraud Detection Using Artificial Neural Network, Global Transitions Proceedings", DOI:10.1016/j. gltp.2021.01.006,2021.

5. Amal Al Ali, Ahmed M. Khedr, Magdi El-Bannany, Sakeena Kanakkayil, "A Powerful Predicting Model for Financial Statement Fraud Based on Optimized XG Boost Ensemble Learning Technique", MDPI, DOI:10.3390/app13042272,2023.

6. Dahee Choi, Kyungho Lee, "Machine Learning-Based Approach to Financial Fraud Detection Process in Mobile Payment System", IT Convergence Practice (INPRA), volume: 5,2017.

7. Eleanor Mill, Wolfgang Garn, Nick Ryman-Tubb, Chris Turner, "Opportunities in Real-Time Fraud Detection: An Explainable Artificial Intelligence (XAI) Research Agenda", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 14, No. 5, 2023.

8. Ebenezer Esenogho, Ibomoiye Domor Mienye, "A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection", IEEE Access, DOI: 10.1109/ACCESS.2022.3148298, 2022.

9. Elena Flondor, Liliana Donath, Mihaela Neamtu, "Automatic Card Fraud Detection Based on Decision Tree Algorithm", www.tandfonline.com/journals/uaai20, DOI:10.1080/08839514.2024.2385249,2024.

10. Emmanuel Ileberi, Yanxia Sun, Zenghui Wang, "A Machine Learning-Based Credit Card Fraud Detection Using the GA Algorithm for Feature Selection", Journal of Big Data, DOI:10.1186/s40537-022-00573-8,2022.

11. Fawaz Khaled Alarfaj, Shabnam Shahzadi, "Enhancing Fraud Detection in Banking with Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention", IEEE Access, DOI 10.1109/ACCESS.2024.3466288,2024.

12. Fawaz Khaled Alarfaj et al., "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms", IEEE Access, DOI: 10.1109/ACCESS.2022.3166891,2022

13. Gangi Setty Raj Charan, K. Deepa Thilak, "Detection of Phishing Link and QR Code of UPI Transaction Using Machine Learning". International Conference on Innovative Mechanisms for Industry Applications DOI:10.1109/ICIMIA60377.2023.10426613,2023

14. Hadeel Ahmad, Bassam Kasasbeh, Balqees Aldabaybah, Enas Rawashdeh, "Class Balancing Framework for Credit Card Fraud Detection Based on Clustering and Similarity-Based Selection (SBS)", DOI:10.1007/s41870-022-00987-w ,2022.

15. Ibrahim Y. Hafez et al, "A Systematic Review of AI-Enhanced Techniques in Credit Card Fraud Detection", Journal of Big Data, DOI:10.1186/s40537-024-01048-8,2025.

16. Jonathan Kwaku Afriyie et al., "A Supervised Machine Learning Algorithm for Detecting and Predicting Fraud in Credit Card Transactions", ELSEVIER -Decision Analytics Journal, DOI: 10.1016/j.dajour.2023.100163,2022.

17. Jonathan M. Karpoff, "The Future of Financial Fraud", Journal of corporate finance, DOI: 10.1016/j.jcorpfin.2020.101694,2021.

18. Mengran Zhu, Yulu Gong, Yafei Xiang, Hanyi Yu, Shuning Huo, "Utilizing GANs for Fraud Detection: Model Training with Synthetic Transaction Data", DOI:10.48550/arXiv.2402.09830,2024.

19. Mohapatra S. et al., "Unified Payment Interface (UPI): A Cashless Indian Transaction Process", International Journal of Applied Science and Engineering, DOI: 10.5958/2322-0465.2017.00004,2017.

20. Noor Saleh Alfaiz, Suliman Mohamed Fati, "Enhanced Credit Card Fraud Detection Model Using Machine Learning", MDPI, DOI:10.3390/electronics11040662,2022.

21. Paolo Vanini et al., "Online Payment Fraud: From Anomaly Detection to Risk Management", Springer, Volume 9, DOI:10.1186/s40854-023-00470-w,2023.

22. Rupa Rani, Adnan Alan, "Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions", IEEE Access, DOI:10.1109/ICDT61202.2024.10489682,2022.

23. S. Jagadeesan, K.S. Arjun, G. Dhanika, G. Karthikeyan, K. Deepika, "UPI Fraud Detection Using Machine Learning", Taylor and Francis Group, DOI:10.1201/9781003559085-130, 2025.

24. Sara Makki et al., "An Experimental Study with Imbalanced Classification Approaches for Credit Card Fraud Detection", IEEE Access, DOI 10.1109/ACCESS.2019.2927266,2022.

25. Sayalee S. Bodade, P.P. Pawade, "Review Paper on UPI Fraud Detection Using Machine Learning, International Journal for Research in Applied Science and Engineering Technology", DOI:10.22214/ijraset.2023.57551,2023.