UPI Fraud Detection Using ML

[1]Mrs. Tasmiya Anjum H N, [2]Tanmaya M J, [3]Moulya A U, [4]Pratheeksha K, [5]Varshitha B S
Information Science and Engineering, Malnad College of Engineering
Hassan-573202, India
Email id: thn@mcehassan.ac.in, tanmayamj5@gmail.com, moulyaau@gmail.com, pratheeksha105@gmail.com, varshithaswamy@gmail.com

***Abstract*—The Unified Payments Interface (UPI) has drastically changed how digital transactions are conducted in India. But along with this expansion comes a rise in fraudulent activity that takes advantage of holes in digital infrastructure. A machine learning-based fraud detection system designed specifically for UPI transactions is shown in this study. The system detects abnormal behavior with high accuracy by using Random Forest and K-Nearest Neighbors (KNN) algorithms on a carefully selected dataset of transactional information (Transaction ID, Timestamp, Amount, Sender/Receiver UPI IDs, and Status). To deal with dimensionality and class imbalance, methods like data resampling and Principal Component Analysis (PCA) are used. The system's ability to boost security in digital payment ecosystems is demonstrated by experimental results that show better fraud detection performance.**

Keywords—PCA, Random Forest, KNN, Machine Learning, Fraud Detection, UPI, and Class Imbalance

I. INTRODUCTION

Financial technology has advanced significantly in today's digitally connected world, introducing speed, convenience, and inclusivity to routine financial transactions. The Unified Payments Interface (UPI), created by the National Payments Corporation of India (NPCI), is one of the most revolutionary developments in the Indian fintech industry. Because UPI enables smooth, instantaneous, and interoperable payments using mobile devices, it has completely changed the way financial transactions are carried out. UPI offers a simplified method that does away with the need for conventional banking obstacles like account numbers or branch codes, whether for business transactions, e-commerce purchases, or personal transfers. UPI's ease of use, availability around-the-clock, and bank interoperability have made it a vital tool for millions of people and accelerated India's transition to a cashless economy. Notwithstanding these benefits, a number of cyber security issues have been brought about by the increased reliance on UPI platforms.

These platforms are naturally vulnerable to a variety of fraudulent operations due to their digital nature. Fraudsters constantly take advantage of technology flaws and user vulnerabilities, from phishing scams and identity spoofing to transaction manipulation and bot-driven attacks. These malevolent actors frequently use advanced technologies and social engineering strategies that can fool even the most watchful consumers. Beyond monetary losses, these fraudulent acts can lead to systemic challenges to the integrity of digital economies, legal issues, harm to financial institutions' reputations, and a decline in user trust.

The frequency and sophistication of such attacks are only anticipated to rise as UPI usage becomes more ingrained in daily life, calling for more extensive countermeasures that are both operationally flexible and technologically sophisticated. Conventional techniques for detecting fraud, such as statistical models and rule-based systems, are constrained by their incapacity to adapt to changing fraud trends and function within predetermined parameters. These systems frequently produce a large percentage of false positives, which results in ineffective use of resources and unhappy users. Moreover, these systems are reactive by nature, necessitating the encoding of rules based on prior knowledge of the various forms of fraud. Such static solutions fall short in the ever-evolving world of digital payments, where fraudsters are always coming up with new ways to get around the law. Furthermore, these approaches are unable to capture intricate relationships and interactions within transactional data due to their analytical constraints.

The predominance of extremely unbalanced datasets in fraud detection, when genuine transactions greatly outweigh fraudulent ones, exacerbates these problems. Since many old and even some current models may be biased toward the majority class and hence fail to properly recognize rare but crucial fraudulent trends, this mismatch presents a substantial difficulty. This study offers a strong, perceptive, and expandable machine learning-based fraud detection system tailored for UPI transactions in order to overcome these constraints. To create a behavioral profile of acceptable user activity, the suggested system makes use of a wide range of transactional variables, such as Transaction ID, Timestamp, Sender and Receiver UPI IDs, Transaction Amount, and Transaction Status. Potentially fraudulent behaviors can be effectively flagged by the system by comparing fresh or unusual transactions to this learning profile.

Because supervised learning algorithms like Random Forest and K-Nearest Neighbors (KNN) have been shown to be successful in solving structured data classification challenges, they are used. To guarantee dependability, generalization, and robustness in a variety of settings, these models are assessed by cross-validation after being trained on meticulously labeled historical datasets. To maximize performance, the system incorporates a number of sophisticated preprocessing procedures in addition to algorithmic modeling. These include cleansing the data, dealing with inconsistent and missing values, normalizing numerical features, encoding categorical variables, and applying Principal Component Analysis (PCA) to reduce dimensionality.

These procedures reduce computational overhead and improve the accuracy of the machine learning models by improving the input data.

Interestingly, the system avoids more artificial approaches to dataset balance, instead focusing on real predictive learning instead of artificial augmentation and using selective training-validation splits. The suggested system's scalable and modular architecture enables deployment in real-time fraud detection pipelines as well as batch processing environments. Although the development and offline validation of the detection models are the main focus of this study, the design is meant to integrate seamlessly with UPI APIs and banking systems. This system may continually monitor transaction streams in a live situation, compare them to learned models in real-time, and initiate automated reactions like alerts, temporary holds, or escalations to human analysts.

Financial institutions would be able to respond quickly, shorten the time frame during which fraudulent conduct could occur, and eventually minimize losses in terms of money and reputation. The work's main contribution is to close the gap between conventional rule-based detection methods and the changing needs of contemporary digital financial ecosystems. By integrating machine learning into the fraud detection process, the system offers a data-driven, adaptable, and flexible method of thwarting fraud. The safeguards that protect digital payment platforms like UPI must also change as they do. By doing this research, we hope to strengthen the security and trust that underpin digital transactions and make sure that advancements in financial technology are accompanied by a similarly forward-thinking dedication to cybersecurity and user safety.

II. LITERATUE SURVEY

In this section, we summarize and examine current research related to UPI Fraud Detection. These researches examine the numerous algorithms, datasets, and methodologies used to detect UPI Fraud.

A. Paper Title: Secure UPI – A Machine Learning-Based Fraud Detection System for UPI Transactions

Description: This research explores a model utilizing XGBoost to recognize the fraud practices in UPI transactions, focusing on the problem faced by disproportion datasets through the usage of SMOTE. Furthermore, it incorporates feature extraction methods such as Principal Component Analysis (PCA) to facilitate dimensionality reduction. The proposed framework enables real-time transaction monitoring and delivers prompt alerts to bolster financial security.
Methodology: The strategy employs XGBoost for classification, SMOTE for balancing classes, and PCA for minimizing the feature set. Performance enhancement is achieved through hyperparameter optimization and K-fold cross-validation. The system's capability for real-time monitoring ensures rapid detection of anomalies.
Limitations: The model is associated with considerable computational demands linked to real-time monitoring and may face risks of overfitting due to the complexities involved in hyperparameter tuning.

Citation: Rani, R., Alam, A. (2024). Secure UPI: A Machine Learning-Based Fraud Detection System for UPI Transactions. 2nd International Conference on Disruptive Technologies (ICDT).

B. Paper Title: UPI Fraud Detection Utilizing Convolutional Neural Networks (CNN)

Description: This study presents the approach of the Convolutional Neural Networks (CNNs) for identifying fraudulent activities in UPI transactions, emphasizing their ability to detect complex patterns. The research aims to the problem related to the split datasets and highlights the flexibility of CNNs in handling unconventional data types.
Methodology: The architecture of the CNN is structured to evaluate sequences of transactions. The dataset undergoes pre-processing through standardization and the implementation of SMOTE. The various layers of the CNN are tasked with extracting hierarchical features that facilitate the detection of fraudulent behaviour.
Limitations: The model tends to produce a significant number of false positives and incurs considerable computational expenses during the training phase of the CNN models.
Citation: Nagaraju, M., et al. (2024). UPI Fraud Detection Utilizing Convolutional Neural Networks (CNN). Seshadri Rao Gudlavalleru Engineering College.

C. C. Paper title: Fraud Detection in UPI Transactions Utilizing Machine Learning (ML)

Description: This study combines Hidden Markov Models (HMM) with clustering methodologies to identify fraudulent activities. It highlights the system's ability to adapt to evolving fraud patterns through heuristic optimization and a variety of algorithmic strategies.
Methodology: HMM is employed to model standard user behavior, with any deviations indicating possible fraudulent actions. Techniques such as K-means clustering, autoencoders, and neural networks are utilized to improve detection capabilities. Heuristic approaches are implemented to enhance computational efficiency.
Limitations: The approach may exhibit high complexity and could lead to inaccuracies when modeling infrequent behavior patterns.
Citation: Kavitha, J., et al. (2024). Fraud Detection in UPI Transactions Utilizing ML. EPRA International Journal of Research and Development (IJRD).

D. *D. Paper Title:* Identification of Fraudulent Activities in Online Transactions Through Machine Learning

Description: This research utilizes supervised learning methods to detect fraudulent behavior within online payment systems. It evaluates the performance of models such as Decision Trees and Random Forest in terms of accuracy.
Methodology: The initial phase of data preparation includes scaling and dividing the datasets. The presentation of the algorithms is weighed using accuracy, exact and recall metrics.
Limitations: The model demonstrates restricted scalability when processing large datasets and shows heightened error rates when dealing with complex data.
Citation: Kadam, K. D. Identification of Fraudulent Activities in Online Transactions Through Machine Learning. International Journal of Advances in Engineering

E. *Paper Title:* Identification of Fraudulent Activities in Online Transactions Through Machine Learning

Description: This document presents a system that integrates both rule-based and machine learning methodologies. It emphasizes the advantages of ensemble learning techniques, specifically utilizing logistic regression, Naive Bayes, and
K- Nearest Neighbors.
Methodology: This document presents a system that integrates both rule-based and machine learning methodologies. It emphasizes the advantages of ensemble learning techniques, specifically utilizing logistic regression, Naive Bayes, and

K- Nearest Neighbors.
Limitations: The models are developed using pre-processed data, incorporating feature scaling. Parameter optimization is achieved through grid search and cross-validation.
Citation: Dhanwani, D. C., et al. (2024). Online Fraud Detection System. International Journal for Research in Applied Science & Engineering Technology (IJRASET).

III. PROPOSED METHODOLOGY

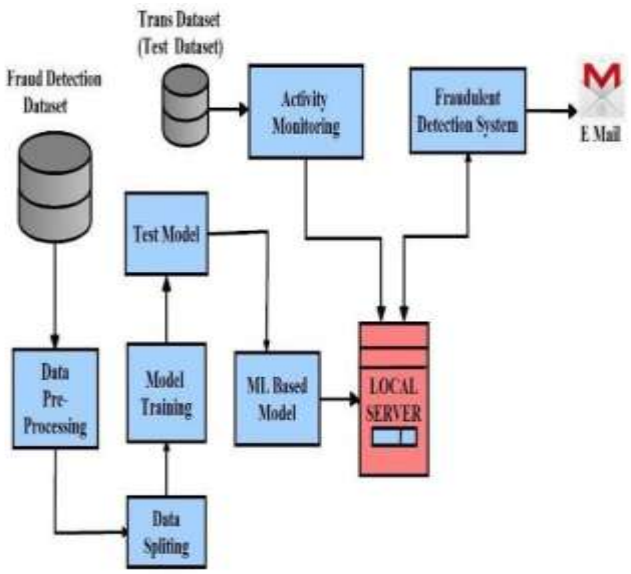


Fig. Methodology

The UPI Fraud Detection System was created using a methodical approach intended to guarantee precision, dependability, and effectiveness in identifying fraudulent transactions. Every phase of the creation process played a distinct part in forming the finished system. Each phase is broken down in depth below, along with its description and purpose:

1.Gathering Data: The initial phase entailed compiling a dataset of UPI transactions that had a number of attributes, including the Transaction ID, Timestamp, Sender and Receiver UPI IDs, Transaction Amount, User Age, Location information (State, Zip), and a label indicating whether the transaction was fraudulent.

Purpose: A representative dataset comprising both legitimate and fraudulent transactions is essential for developing a trustworthy fraud detection model. This serves as the basis for training and assessing the model.

2. Preparing Data: Missing values, duplicate entries, and inconsistent formats are common in raw data. In this step, duplicates were eliminated, missing values were removed or imputed, and categorical data was formatted. Numerical values were used to encode categorical data, such as states and UPI IDs. To put them on a consistent scale, transaction amounts and other numerical characteristics were standardized.
Purpose: To ensure that the dataset is clean, consistent, and in a format that the models can process efficiently in order to prepare it for machine learning models. Additionally, standardizing data helps distance-based algorithms like KNN avoid bias.

3. Managing Data Inequalities: The dataset is unbalanced since fraudulent transactions are usually far less common than authentic ones. Rather than employing oversampling methods such as SMOTE, this project maintained the natural distribution and addressed imbalance by focusing on evaluation metrics that take class distribution into account (e.g., precision and recall) and carefully choosing a model (Random Forest, which is robust to imbalance).
Purpose: To make sure the model can reliably identify infrequent fraudulent cases without adding artificial data, and to prevent it from becoming biased toward forecasting only the majority class.

4. Engineering and Feature Selection: The most instructive aspects were found during this stage. As possible signs of fraud, characteristics such as transaction frequency, odd transaction times, or unusually high transaction amounts were noted. To lessen feature redundancy, dimensionality reduction strategies like Principal Component Analysis (PCA) were optionally used.
Purpose: To improve prediction accuracy and computational efficiency by minimizing noise and choosing only the most pertinent features, the model's performance will be improved.

5. Splitting Data: Training and testing sets were created from the preprocessed dataset, usually in an 80:20 ratio. The model was constructed using the training set, and its performance on unseen data was assessed using the testing set.
Purpose: To evaluate the trained model's generalization ability to fresh, untested data. A realistic assessment is ensured and overfitting is avoided with proper data separation.

6. Training Models: Random Forest and K-Nearest Neighbors (KNN) are two machine learning techniques that were used. The training dataset was used to train these models. Cross-validation methods were employed to improve robustness, and hyperparameters were adjusted to maximize performance.
Purpose: Using the patterns identified in the training data, create prediction models that can differentiate between transactions that are fraudulent and those that are legitimate.

7. Model Assessment: The testing dataset was used to test the models following training. The efficacy of the model was assessed using metrics including Accuracy, Precision, Recall, F1-Score, and the Confusion Matrix, with a particular emphasis on the identification of minority (fraudulent) groups.
Purpose: The objective is to assess the models' performance and make sure they are not only generally accurate but also successful in detecting fraudulent transactions with a low number of false positives or false negatives.

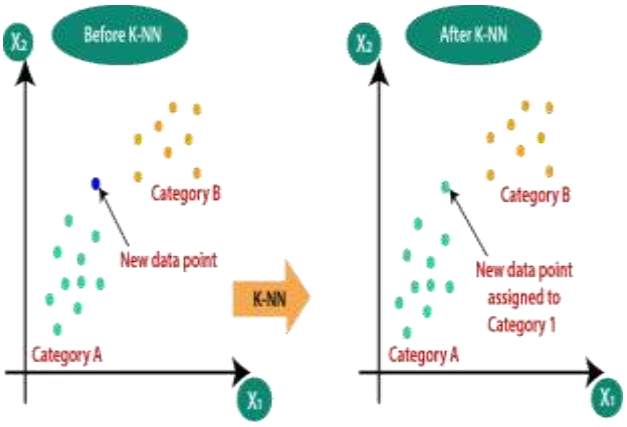
8. Fraud Detection System Integration: A comprehensive fraud detection system was built using the top-performing model. After receiving transaction data as input, the system uses the trained model to evaluate it and determines if a transaction is fraudulent or valid.
Purpose: To offer a comprehensive system that can be implemented in a real-world setting to monitor UPI transactions and automate fraud detection.

9. Mechanism of Alert: An alert mechanism is triggered by the system when it detects a transaction that may be fraudulent. Sending an email, creating a log record, or raising a flag in the system dashboard for human review could all be part of this.
Purpose: To guarantee prompt attention to questionable transactions so that security teams or account holders can take prompt action. Every stage in this process was intended to make a significant contribution to the development of a precise and successful fraud detection system.

IV. ALGORITHMS

4.1 KNN (K-Nearest Neighbors)

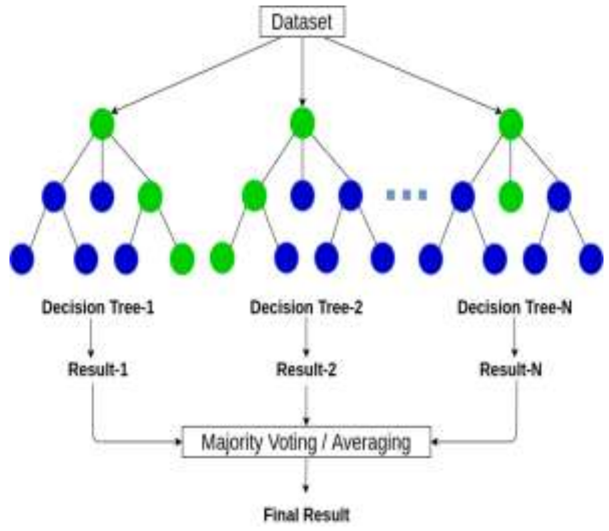
K-Nearest Neighbors (KNN) is an effective and straightforward machine learning algorithm used for both classification and regression process. It functions based on the idea of similarity, where a data point is categorized by determining the predominant class among its K nearest neighbors within the feature space. As a non-parametric method, KNN does not assume any particular data distribution, which allows it to effectively manage intricate and nonlinear relationships.



The algorithm computes the distances between the data point in question and all other points in the training dataset, subsequently identifying the K closest neighbors. Its straightforward nature and ease of implementation, combined with its various types across various usage, have contributed to its widespread use in fields such as pattern recognition, image processing, and recommendation systems.

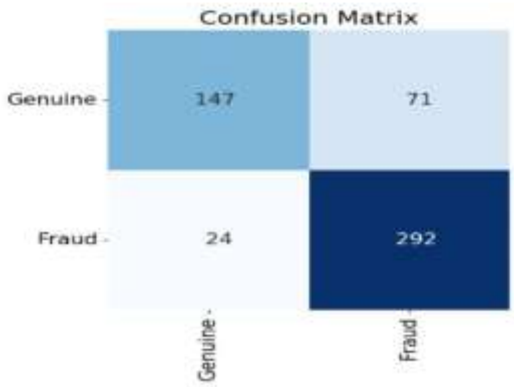
Nonetheless, the performance of KNN can be influenced by the choice of K and may occur significant computational costs when added to large datasets.

4.2 Random Forest



The popular ensemble learning algorithm Random Forest (RF) is well-known for its performance in both regression and classification tasks. Using a technique known as bootstrap aggregating or bagging, it builds many decision trees using randomly chosen subsets of data and attributes. The majority vote (in classification) or average (in regression) of all the trees is used to make the final forecast, greatly lowering the possibility of overfitting that single decision trees frequently encounter. Because of its capacity to manage huge, intricate, and unbalanced datasets, Random Forest is very useful in the context of UPI transaction fraud detection. It has the ability to simulate non-linear correlations between characteristics including transaction frequency, timing, and amount all of which are important markers of fraudulent behavior.
Its capacity to quantify feature importance, which aids analysts in determining which elements are most crucial in spotting fraud, is one of its main advantages. Random Forest's resilience to missing data and outliers is another benefit, which makes it dependable for real-world applications where data quality may differ. Additionally, it is easily parallelizable and scales well to huge datasets, both of which are advantageous when handling enormous amounts of transaction records. Random Forest is a great option for developing safe and dependable fraud detection systems in digital payment settings like UPI because it provides a good mix between accuracy, interpretability, and computational efficiency.

V. RESULT



The project's main goal was to improve the security of UPI (Unified Payments Interface) transactions by creating an effective machine learning-based fraud detection system. In order to accomplish this,

the project used two important algorithms: K-Nearest Neighbors (KNN) and Random Forest. These algorithms were selected because to their versatility and resilience in classification tasks, particularly when dealing with complicated and non-linear data structures. 2,666 records with transaction details, including time, date, UPI numbers, amount, and a label indicating whether the transaction was fraudulent or authentic, made up the dataset utilized for testing and validation. A comprehensive preparation step was performed on the dataset, which included dimensionality reduction using Principal Component Analysis (PCA), feature scaling, and addressing missing values. This enhanced the model's capacity to identify minute patterns that might point to fraudulent activity. The dataset was divided into training and testing sets following preprocessing. The testing set was used to evaluate the machine learning models' efficacy after they had been trained on the training data. To assess the models' performance, evaluation metrics like Precision, Recall, F1 Score, and Support were computed: As it indicates the percentage of transactions reported as fraudulent that were in fact fraudulent,

Precision is essential to fraud detection. Less false alerts are indicated by a high precision score, which is essential for preserving user confidence and preventing needless account limits.

Recall (or Sensitivity) quantifies the model's capacity to identify every instance of fraud. A high recall guarantees that the majority of fraudulent transactions are discovered before they cause harm.

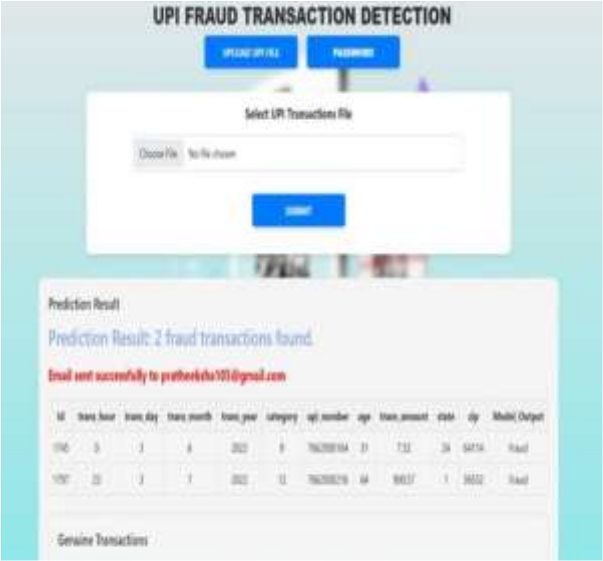
F1 Score, which is the harmonic mean of accuracy and recall. This is particularly helpful in datasets that are unbalanced, such as fraud detection, where there are far fewer fraudulent transactions than valid ones.

Support provides information about the dataset's distribution by indicating the quantity of real cases in each type (fraudulent and legitimate).

The outcomes showed that while both the Random Forest and KNN models did well, Random Forest's ensemble nature and capacity to minimize overfitting allowed it to show somewhat higher stability and accuracy. The models' ability to consistently identify anomalies in the transaction data was validated by the validation metrics. Additionally, to help stakeholders better grasp the advantages and disadvantages of each strategy, graphical plots of classification accuracy and error rates were created to show model performance.

The creation of an integrated fraud detection framework that can be used in UPI systems to track transactions and identify questionable activity was one of the project's main results. Although real-time detection was not used, the system is made to process transactions in batches and detect possible frauds later, which is useful for security assessments and post-transaction audits. When high-risk transactions are identified, the system's alert notification module can notify relevant parties (such bank representatives or system administrators).

This innovation also makes the system more sensitive, allowing for quicker responses to fraud and reducing possible losses. To sum up, the project's outcome demonstrates the feasibility of applying machine learning algorithms to UPI system fraud detection. The suggested system provides a workable way to increase the security of digital payments and is accurate, scalable, and efficient. Future improvements, such adding deep learning models or putting the system in real-time settings for even more effective fraud protection, are made possible by the encouraging findings.



Prediction Result

Prediction Result: 2 fraud transactions found.

Email sent successfully to pratheeksha103@gmail.com

id	trans_hour	trans_day	trans_month	trans_year	category	upi_number	age	trans_amount	state	zip	Model Output
[illegible]	5	3	4	[illegible]	8	[illegible]	31	7.32	34	[illegible]	Fraud
[illegible]	21	3	7	[illegible]	11	[illegible]	44	[illegible]	1	[illegible]	Fraud

Genuine Transactions

VI. CONCLUSION

The financial ecosystem in India and abroad has undergone tremendous change as a result of the quick spread of digital payment systems, especially the Unified Payments Interface (UPI). But this change has also made people more susceptible to fraud and online attacks. The CNN-based model for UPI fraud detection that we suggested in this paper uses deep learning to find intricate patterns and abnormalities in transaction data that point to fraudulent activity. The model demonstrated encouraging outcomes in correctly identifying suspicious transactions, providing a potential remedy to reduce monetary losses and improve the effectiveness of fraud detection systems.

Our approach comprised thorough transactional data preprocessing, labeled dataset training for the model, and performance assessment utilizing important metrics including accuracy, precision, recall, and F1-score. Although the model performed well in a controlled setting, it is yet unknown how well it works in real-time applications and how well it can adjust to changing fraud tactics. There are drawbacks to using static historical data to identify new dangers.

To increase robustness and privacy, future research should concentrate on real-time deployment, continuous learning using adaptive algorithms, and cutting-edge techniques like reinforcement and federated learning. Enhancing model reliability and practical impact will also require partnerships with financial institutions to have access to anonymized real-world data. To sum up, this initiative establishes a strong basis for automated, intelligent fraud detection in the UPI ecosystem. Such systems have the potential to be extremely important in protecting digital transactions and promoting confidence in financial technologies with additional development and real-world integration.

VII. REFERENCE

[1] ALESKEROV E, FREISLEBEN, B., and, RAO B (1997) CARDWATCH: neural network, based database mining system for credit card scam identification. In Conference (pp. 220–226). IEEE, Piscataway, NJ
Sahin M (2017) Understanding Telephony Fraud as an Essential Step to Better Fight it [Thesis]. École Doctorale Informatique, Télécommunication et Électronique, Paris
Abdallah A, Maarof MA, Zainal A (2016) Fraud detection system: A survey. J Netw Comput Appl

68:90–113
ANDREWS PP , PETERSON MB (eds) (1990) Criminal Intelligence Analysis. Palmer Enterprises, Loomis, CA
ARTÍS M, AyUSO M, GUILLÉN M (1999) Modeling different types of automobile insurance fraud behavior in the Spanish market. Insurance Math Econ 24:67–81 BARAO MI, TAWN JA (1999) Extremal analysis of short series with outliers: Sea-levels and athletics records.

[2] Adekunle, I. M., & Ozoh, P. (2023). Fraud detection model for illegitimate transactions. Kabale University Interdisciplinary Research Journal,2(2),21-37 https://doi.org/10.1016/j.future.2015.01.001
Boulieris P, Pavlopoulos J, Xenos, A., & Vassalos, V. (2023). 122.https://doi.org/10.24321/2394.6539.202012
Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023).
https://doi.org/10.1016/j.dss.2010.08.008

[3] Mohammed, Emad, and Behrouz Far.“Supervised Machine Learning Algorithms used for Credit Card scam transaction identification: A Study.” IEEE Annals of the History of Computing, IEEE, 1 July 2018, doi.ieeecomputersociety.org/10.1109/IRI.2018.00025.
Randhawa, Kuldeep, et al. “Credit Card scam identification Using AdaBoost and Majority Voting.” IEEE Access, vol. 6, 2018, pp. 14277–14284., doi:10.1109/access.2018.2806420.
doi:10.1109/colcomcon.2017.8088206.

[4] Omair B, Alturki, A (2020) A organized literature analysis of fraud detection metrics REFERENCES Ayushi Agrawal, Shiv Kumar, Amit Kumar Mishra, "A Novel approach for UPI Fraud Detection", 2nd International Conference, on Computing for feasible Global Development (INDIA.Com), 2018.
N. Sivakumar, R. Balasubramanian, "Cheating identification in Visa Transactions: Classification dangers Also counteractive action Techniques", universal diary for PC science and majority of the data Technologies, vol. 6, no. 2, 2015.

[5] LESKEROV E, FREISLEBEN, B., and, RAO B (1997) CARDWATCH: neural network-based, database mining system for credit card fraud identification. In Conference (pp. 220–226). IEEE, Piscataway, NJ Sahin M (2017) Understanding Telephony Fraud as an Essential Step to Better Fight it [Thesis]. École Doctorale Informatique, Télécommunication et Électronique, Paris Abdallah A, Maarof MA, Zainal A (2016) Fraud detection system: A survey. J Netw Comput Appl 68:90–113