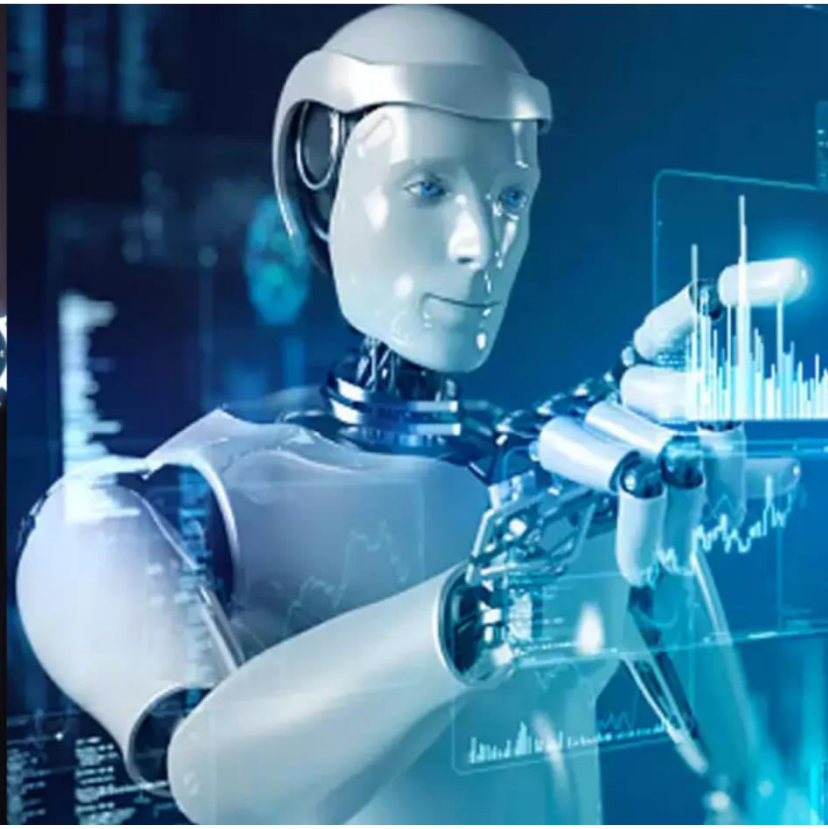
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

UPI Fraud Detection: An Innovative ML Algorithm

Dr. G. Kameswari[1], J. Varshini Priya[2], SK. Sameer[3], K. Sai Hemanth[4], T. Harshitha[5]

Associate Professor, Dept. Of ECE, NBKR Institute of Science and Technology, Vidyanagar, Tirupati district, Andhra Pradesh, India[1]

UG Students, Dept. Of ECE, NBKR Institute of Science and Technology, Vidyanagar, Tirupati district, Andhra Pradesh, India[2345]

ABSTRACT: With Unified Payments Interface (UPI) more gaining grounds with digital transactions, the more risk of fraudulent activities it has brought along with it. Thus in this paper, we propose a sophisticated and innovative technique for the detection of frauds within UPI based on the various parameters of transactions such as the name of a bank book, a transaction ID, and a transaction amount. This method utilizes three K-nearest neighbors (KNN) algorithms and decision trees, at least characterize the step Random Forest. Classifier offers accuracy and is resistant to overfitting, thus proving to be a viable candidate in this application. It operates on the transaction details that were entered to classify the outcome of the transaction as either Transaction Failed: Incorrect Details Entered or Transaction Successful: Details Verified and Processed. KNN has a simple approach to classification depending on finding look-alikes in terms of transaction details from previously labeled transaction details. Decision trees provide great transparency as to how decisions are made with a tree-like structure.

This strategy should help in curtailing fraudulent transactions while also allowing a clear pathway for processing legitimate transactions. Underlining the objective of the model is a growing interest in safeguarding UPI transactions by providing an additional deterrent against unintended practices. Preliminary runs suggest that algorithms have some potential to discriminate between real and false transactions-a very strong prospect for acceptance in financial systems of reality.

KEYWORDS: UPI-Digital Payments, Random Forest Algorithm, K-Nearest Neighbors, Decision Tree, Machine Learning.

I. INTRODUCTION

The rise of digital payments has brought convenience but also increased vulnerability, particularly with the growing popularity of the Unified Payments Interface (UPI). The frequency of transaction-related frauds has risen alongside UPI's widespread adoption, prompting urgent attention to its associated risks [2, 3]. To mitigate these issues, fraud detection in UPI systems is proposed through comprehensive analysis of transaction data, such as the account holder's name, transaction ID, and transaction amount [2, 5]. This study applies three prominent machine learning algorithms—Random Forest, K-Nearest Neighbors (KNN), and Decision Tree—to detect and classify fraudulent activities. Among them, Random Forest emerges as the most effective due to its high accuracy and resistance to overfitting, making it suitable for real-time fraud detection in dynamic transaction environments [2, 5].

KNN is used for its simplicity and mathematical basis in classifying observations based on distance, which helps detect anomalies in transaction behaviour [3]. Decision Trees add value by offering an interpretable structure, allowing easier understanding and decision-making in fraud analysis [5,8]. All three models are employed to classify transactions into two outcomes: either "Transaction Failed: Incorrect Details Entered" or "Transaction Successful: Details Verified and Processed," thereby enhancing clarity in fraud assessment [1,2]. The integration of these machine learning models is expected to improve the overall security of UPI systems, ensuring that genuine transactions proceed unhindered while fraudulent attempts are detected and mitigated effectively [6, 9 and 12].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

OBJECTIVE

Most of all, it is developing a truancy detection system for UPI transactions by employing important pieces of data during transaction processing, including the bank book name, transaction ID, and transaction amount. It includes the designing of a complete framework where machine learning algorithms Random Forest, K- Nearest Neighbors (KNN), and Decision Trees may be incorporated for classification of transactions as otherwise Transaction Failed: Incorrect Details Entered or Transaction Successful: Details Verified and Processed. The proposed model aims to empower its forecasting capability to detect fraudulent transactions while avoiding the detection of innocent ones through effective use of these algorithms. This would not only secure UPI digital payments but, at the same time, provide a better, seamless user experience. Eventually, we envision deploying the model proposed by us in the real system, thereby providing a safety net for users against unauthorized activities and boosting the confidence of such users in digital transactions.

MOTIVATION

The rapid increasing UPI development is as strong as possible towards cashless transactions as fast and easy. But along with this convenience has come fast-rising alarming frauds that risk users and financial institutions. The project's motivation clearly states that it would be an effective fraud detection system to protect UPI transactions. Using Random Forest, K-Nearest Neighbors (KNN), and Decision Tree with machine learning techniques, the system attempted to analyze original bank book name, transaction ID, and amount in the transaction details to accurately classify transactions as legitimate or fraudulent. Although the Random Forest classifier is not very sensitive to overfitting, which enhances the accuracy of results, KNN offers a fairly simple classification by seeing how close it is to past transactions. Decision Trees are intuitively easy to follow and are probably useful for every person concerned with decision making. Thus, this multi-algorithm approach intends to secure UPI transactions so that people using it feel secured and have faith in digital payments.

SCOPE

The system for fraud detection in UPI (Unified Payments Interface) transactions is the main aim of the study. In order to secure such detection, this study aims to analyze various transaction details such as bank book name, transaction ID, and transaction amount, for which three machine learning algorithms, Random Forest (RF), K-Nearest Neighbors (KNN), and Decision Tree (DT), will be used. The various algorithms will be compared in their ability to classify transactions as either Transaction Failed: Incorrect Details Entered or Transaction Successful; that is, verified details have been processed. The application of the models is intended to strengthen the security of UPI transactions, offering a reliable fraud prevention mechanism to users while ensuring the smooth processing of legitimate transactions. The project will thus become a comparative case study regarding the performances of these classifiers in order to identify the best for real-life applications in financial systems, thus enhancing user trust and safety in many digital payments.

II. LITERATURE REVIEW

1. In [1], Gupta et al. (2024) proposed a deep learning-based framework for detecting financial fraud in UPI (Unified Payments Interface) transactions. The authors utilized transaction datasets, incorporating both temporal and behavioural features, and experimented with multiple deep learning architectures such as LSTM and CNN to capture sequential transaction patterns and anomalies. The model achieved notable accuracy and precision, indicating its effectiveness in distinguishing between legitimate and fraudulent activity. However, the study also highlighted limitations such as challenges with imbalanced datasets and the need for real-time deployment optimization.

2. In [2], Gupta, Saxena, and Kumar (2024) developed a hybrid fraud detection system for UPI transactions by integrating traditional rule-based approaches with machine learning models. They utilized anomaly detection algorithms to identify unusual transaction patterns, focusing on both transactional and behavioral features. The proposed system demonstrated effective real-time detection capabilities, enhancing the security of digital payments. However, the study acknowledged challenges such as the need for continuous model updates and the handling of evolving fraud tactics.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

3. In [3], Jagadeesan et al. (2024) proposed a machine learning-based framework for detecting fraudulent activities in UPI transactions. The authors employed a combination of supervised and unsupervised learning techniques, including Random Forest and anomaly detection algorithms, to identify unusual transaction patterns indicative of fraud. Their approach demonstrated significant improvements in detection accuracy and real-time responsiveness. However, the study acknowledged challenges such as the need for continuous model updates and the integration of evolving fraud tactics.

4. In [5], Kamble et al. (n.d.) proposed a novel approach to UPI fraud detection by employing stacked generalization, an ensemble learning technique that combines multiple base models to improve predictive performance. Their methodology demonstrated enhanced accuracy in identifying fraudulent transactions, addressing challenges such as class imbalance and model overfitting. The study highlighted the effectiveness of stacked generalization in leveraging diverse model strengths to achieve robust fraud detection.

5. In [6], Karthick et al. (2024) proposed an advanced fraud detection system for Unified Payments Interface (UPI) transactions by integrating deep learning techniques with artificial neural networks (ANN). Their approach aimed to identify and mitigate fraudulent activities, enhancing the security of digital payment systems. The study demonstrated the effectiveness of combining deep learning models with ANN in detecting complex fraud patterns in real-time UPI transactions. However, the paper also acknowledged challenges such as the need for large, labeled datasets and the computational complexity associated with training deep learning models.

6. In [7], Kumar et al. (2025) proposed an advanced fraud detection system for Unified Payments Interface (UPI) transactions by integrating XGBoost and Long Short-Term Memory (LSTM) networks. The XGBoost algorithm effectively handled complex data relationships, while the LSTM model captured sequential patterns in user behaviour. The hybrid model demonstrated improved accuracy in identifying fraudulent transactions, addressing challenges such as class imbalance and evolving fraud tactics. The study emphasized the importance of continuous learning and real-time monitoring to adapt to new fraud patterns. Additionally, the integration of industry tools like two-factor authentication was highlighted as a means to enhance security.

III. EXISTING SYSTEM

K-Nearest Neighbors (KNN) is a simple, non-parametric algorithm used for both classification and regression tasks. It operates by finding the 'k' closest data points (neighbors) to a query point and making predictions based on the majority class (for classification) or average value (for regression) of these neighbors. The algorithm is intuitive and easy to implement but can computationally expensive, especially with large datasets, because it requires calculating the distance between the query point and all other points in the dataset. Additionally, KNN's performance can be heavily influenced by the choice of 'k' and the distance metric used, and it is sensitive to irrelevant or noisy features, which can mislead the distance calculations and reduce its accuracy. Despite these limitations, KNN is widely used due to its simplicity and effectiveness in certain scenarios.

Disadvantages:

- **Data Sensitivity:** Existing systems may struggle with noisy or irrelevant features, which can lead to inaccurate predictions and decreased performance.
- **Scalability Issues:** Algorithms like KNN can become computationally expensive with large datasets, resulting in slower response times and inefficiencies in real-time applications.
- **Overfitting Risk:** While Random Forest is robust, decision trees can easily overfit to training data, leading to poor generalization on unseen transactions**.**
- **Limited Interpretability:** Although Decision Trees provide some level of interpretability, ensemble methods like Random Forest can be less transparent, making it harder for users to understand the decision-making process.
- **Imbalanced Data:** Fraud detection systems often deal with imbalanced datasets, leading to biased predictions favouring legitimate transactions over fraudulent ones.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

IV. PROPOSED SYSTEM

A potent contender for UPI fraud detection is the Random Forest, a kind of machine-learning algorithm. It trains decision trees using basically, you have multiple samples with numerous decision trees making a decision on every record, with an aggregation of their outputs to form a decision. The ensemble style therefore ensures more accuracy and reduces the risks of overfittings, thus making it suitable for any task involving frauds since the data are often full of noises, imbalance, and involve elaborate feature-interrelationship patterns. In the case of UPI frauds, Random Forest is capable of looking into many transaction attributes such as bank book name, transaction ID, amount, etc. and these are can be shown in fig-1 as , to detect patterns distinguishing genuine and fraudulent transactions. Random Forest is, amenably, able, with strength, to unleash detection using the synergy between its trees for capturing those faint traits of frauds, which many a time go unnoticed by simplistic models.

In Fig-1, the system workflow begins with data collection, followed by pre-processing and splitting of the data. The processed data is then used for model building and prediction before the user is logged out. On the user side, Fig-1 illustrates a sequence starting from registration and login, followed by inputting credentials, submitting input data, and finally receiving the result. This integrated flow ensures seamless interaction between the user and the predictive model system.

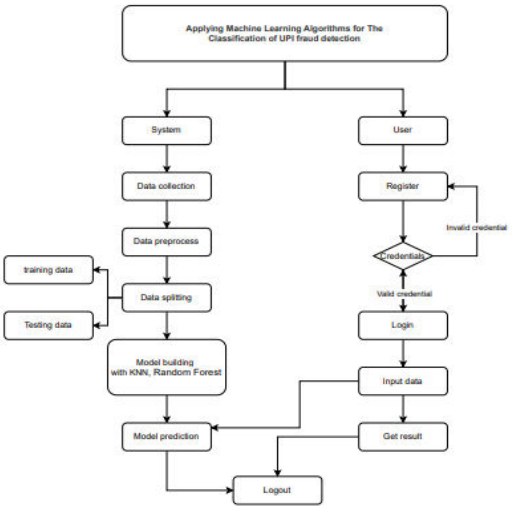


Fig-1: Block diagram for proposed system

Advantages:

- **Increased Accuracy:** The individual high accuracies of Random Forest, KNN, and Decision Tree are combined by this hybrid classification approach, increasing actual performance while reducing false positives and false negatives.
- **Reduced Overfitting:** Random Forest achieves this through its ensemble nature, making the system robust against noisy and imbalanced transaction data.
- **Interpretability:** Decision trees lay out the entire decision process clearly, allowing for understanding of how the classification decision was derived, which increases trust in the financial system.
- **Real-Time Detection:** The system investigates transaction details in real-time to allow prompt detection and prevention of fraud.
- **Flexibility:** The methodologies can be retrained for new data as fraud patterns change, ensuring they will remain relevant for active detection.
- **User Protection:** The system increases user confidence and secures transactions over the Internet by differentiating between real and fraudulent transactions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

V. METHODOLOGY

The methodology of this project seeks to detect and classify UPI transactions as fraudulent or legitimate by analyzing transaction attributes using machine learning algorithms. This methodology is sorted into a well-defined process or analysis pipeline, consisting of the following phases which can be shown in above fig-1:

1. Data Collection: The collected data consist of transactional data fields such as Information about bank book name, transaction ID, amount transacted, and whether the transaction was fraudulent or legitimate. With the labeling of such a dataset, it supports supervised learning processes, where the output may classify the statements saying. Transaction Failed: Incorrect Details Entered, or Transaction Successful: Details Verified and Processed.

2. Data Pre-processing: Handling of Missing Values: Complete or incomplete null entries in fields such as the transaction amount-II or transaction ID are either filled in with statistical methods mean/median-imputation or dropped depending on their importance.

Feature Selection: Emerging of redundantornonkey features (e.g. user identifiers that have been hashed-out) are ruled out in favor of more meaningful predictors like the amount and transaction pattern. Label Encoding: The output labels are encoded into binary values — 0 representing the successful transaction while 1 stands for failed transactions (these could also be potential fraud). Class Imbalance Handling: Since fraud cases are rare, SMOTE (Synthetic Minority Oversampling Technique) is being used in boosting balance in the dataset by generating some of these minority class examples in a synthetic way.

3. Model Development: Three classifiers have been developed and tested against each model- Random Forest, K-Nearest Neighbors (KNN), and Decision Tree. They all were trained using our pre-processed dataset and further evaluated based on their capability of fraud detection.

4. Model Evaluation: Accuracy: Overall correctness of the predictions. Precision, Recall, F1 Score: This gives insight into how well the model detects fraud (recall) without misclassifying legitimate transactions (precision). Confusion Matrix: Visualization of how true/false positives and true/false negatives are performing.

5. Model Optimization: Hyperparameters for each model are being tuned by either grid search or random search in order to maximize true positive detection and minimize false positives. For example, in KNN Both LDA and QDA work well for generating values to predict the class of an object that has to be classified.

6. Results Visualization: Bar charts visualize the model performance, comparing accuracy. Confusion matrices illustrate detection efficiency. Together, this informs the decision as to which model would be best suited for real-time deployment in UPI systems.

VI. ALGORITHM IMPLEMENTATION

This section outlines the implementation of various ML algorithms employed to predict and classify air quality categories, such as Good**,** Satisfactory**,** and Poor. Below is a detailed description of each algorithm used in this study:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

1. Random Forest Classifier

```
Accuracy Score of RandomForest=  0.656752176707766
======================================================
f1 score score fo RandomForest = 0.655645444952515
======================================================
precision_score of RandomForest is= 0.65376746361138
======================================================
recall_score of RandomForest is = 0.6575342465753424
======================================================
coonfusion matrxi of RandomForest =
 [[11294  5923]
 [ 5825 11184]]
======================================================
```

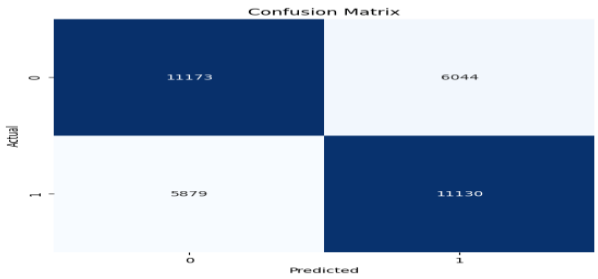


Fig.2: Performance Analysis of Random Forest Classifier on UPI Transaction dataset

The above fig.2 is one of the implementations of the Random Forest Classifier () from the sklearn.ensemble module. This model builds ensembles from various Decision Trees and aggregates their predictions, thereby aiding in generalization and overfitting. Results observed are as follows- Accuracy - 65.67% F1 Score - 65.56% Precision - 65.37 Recall - 65.75%.

2. Decision Tree Classifier

Accuracy: 0.6076

Classification Report:

	precision	recall	f1-score	support
0	0.61	0.60	0.61	17217
1	0.60	0.62	0.61	17009
accuracy			0.61	34226
macro avg	0.61	0.61	0.61	34226
weighted avg	0.61	0.61	0.61	34226

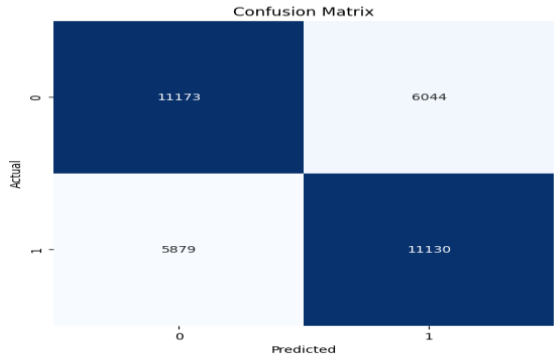


Fig-3: Performance Analysis of Decision Tree Classifier on UPI Transaction dataset

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

In the above fig.3 is the Decision Trees classifier from sklearn.tree library is a model favoured for simplicity and easy interpretation, as it splits the data based on individual feature thresholds to build a decision structure. Performance Results-Accuracy: 60.76% Precision (Class 0/1): 0.61 / 0.60 Recall (Class 0/1): 0.60 / 0.62 F1-Score (Class 0/1): 0.61 / 0.61.

3. K-Nearest Neighbors (KNN) Classifier

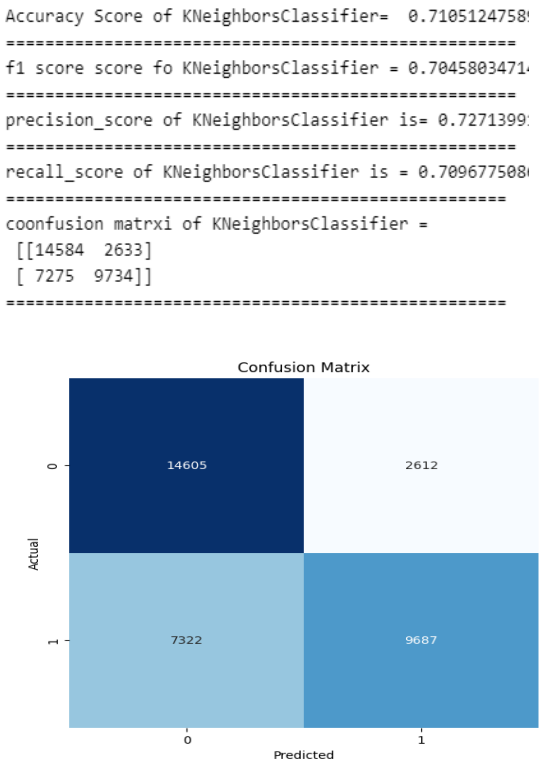


Fig-4: Performance Analysis of K-nearest neighbors Classifier on UPI Transaction dataset

The above fig.4 is the K-nearest neighbors classifier is a distance-base model where classification is accomplished through the scikit-learn function K Neighbors Classifier (). The classification of the sample is done based on which class among the k-nearest neighbors is in majority. The performance metrics obtained are as follows: Accuracy: 71.05%F1: 70.45%Precision: 72.71%Recall: 70.07%.

COMPARISON OF ALL MODELS

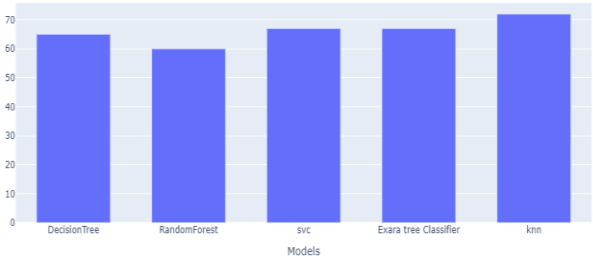


Fig-5: Comparison of Models

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

The fig-5 is the chart compares the accuracy figures the horizontal bar graph shows different machine learning models concerning one classification task. Each bar represents one of the individual models: Decision Trees, Random Forest, Support Vector Classifier (SVC), Extra Tree Classifier, and K-Nearest Neighbors (KNN). The height of each bar represents the accuracy of each model, where all models exhibited similar performance levels within the ballpark of 60-70%. This shows that these algorithms worked well for the dataset under consideration, and perhaps some tuning or ensemble methods could improve performance. All in all, this demonstrates a clear visual representation of the models' comparative accuracies.

VII. RESULTS AND DISCUSSIONS

Best Performance Model: K-Nearest Neighbors (KNN) : Of the three models assessed, K-Nearest Neighbors had the best performance, with an accuracy of 71.05%, precision of 72.71%, and an F1-score of 70.45%. KNN proved most effective in distinguishing legitimate from fraudulent transactions based on nearest-neighbor similarity. KNN compares new transactions to transactions seen in the past and assigns them to the class with the highest similarity. This approach came to work particularly well in this case due to its extremely high sensitivity, which is important in fraud detection.
Moderate Performance: Random Forest Classifier : The Random Forest model can be said to have delivered some balance between results-a little inconsistency here and there-with correctness at 65.67%, recall at 65.75%, and F1-score at 65.56%. Random Forest is an ensemble method employed in developing classifiers where the predictions of individual decision trees are aggregated to enhance accuracy and lessen variance, Overfitting. Though not as good as KNN, it is still a method that gives relatively stable results across all inputs examined. One strong point of Random Forest is that it captures complex patterns and interactions that may take place among attributes related to transactions: transaction ID, amount, and account name.

Lower Performance: Decision Tree Classifier: With a performance of merely 60.76% accuracy and a macro F1- score of merely 0.61, the Decision Tree classifier is the worst performer among all the classifiers evaluated. It is simple and has reasonable interpretability; however, its predictive performance and robustness, compared to other methods based on ensembles or on distance, are questionable. This underperformance is likely as a result of overfitting, which means that the model adapted itself too well to training data and was unable to generalize on the test data. This indicates a definite requirement for pruning or regularization in the application of decision trees to fraud detection.

Discussion:
According to experimental results, K-Nearest Neighbors exhibits maximal efficiency with regard to the overall classification metrics, and, therefore, remains a strong candidate for all UPI fraud detection tasks. It is an effective measure against the detection of activities that are anomalous and consequently of interest since it allows comparisons of new transactions against similar historical instances; however, it is computationally expensive during inference and may need to be optimized before larger-scale deployment.

Random forests are a rather balanced option, since they are the most consistent and constitute somewhat of a complex learning apparatus, permitting the tuning of parameters to refine performance. Being an ensemble The varied decision trees of a Random Forest inhibits overfitting much better than a single decision tree would.

Decision Trees are interpretable and, on the other hand, can most times underfit data, which essentially means they have not been able to capture the relationship that exists within the data. This is really the case when we have imbalanced or noisy data. Standing alone, without combinations of learning methods like pruning or boosting, they do not seem very helpful for high-risk applications as that of fraud detection.

Class imbalance is another issue facing all models. Nevertheless, despite SMOTE-type techniques being employed to balance the classes, the reality is that there is always comparatively much fewer fraudulent transactions than legitimate ones in the field of real-world fraud detection. Such an imbalance has potential in skewing results against a Decision Tree model, being sensitive to dominant classes.

In conclusion, the comparative study indicates that although all three algorithms can detect UPI fraud to some extent, KNN stands out as the best performing model, followed by Random Forest. Decision Tree, on the other hand, requires further tuning and possible integration into ensemble structures for it to be useful in this use case. In the future, a

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

combination of model ensembles and advanced oversampling strategies, as well as continuous learning frameworks with live stream of transactions, should be pursued to improve the detections in real-time systems.

VIII. CONCLUSION

As a result, the growing dependence on Unified Payments Interface (UPI) transactions necessitates strong fraud detection capability in order to protect users from unauthorized activity. The multi-algorithm approach, generated This is carried out using the Random Forest, K-Nearest Neighbors (KNN), and Decision Tree classifiers.

They conduct very effective analysis of the characteristics of transactions to identify them, and speedily process valid transactions. Random forest algorithm is very accurate and immune to overfitting, KNN uses a simple but effective classification technique based on similarity, and Decision trees provide the person with possible pathways to decision that enhance visualization. Initial evaluations show that these algorithms indeed have the potential for a significant increase in UPI transaction security. The financial institution thereby elevates its service potential of consumer confidence while safeguarding assets through the general realization of an ultimately safer digital payment environment. This study adds to the continuous battle against fraud in digital transactions, reassuring the credibility and reliability of UPI as the most preferred mode of payments.

IX. FUTURE ENHANCEMENTS

The next possible step are advanced machine learning techniques like ensemble methods or deep learning for further enhancement in UPI fraud detection model. Real-time data analytics will also improve the model's accuracy to any emerging pattern of fraud. Feature engineering on other transaction extras, such as user's way of transactions and geographical location, will add deeper and wider perspectives about the legitimacy of a transaction.

Integration of model feedback mechanism which always updates with the new information about transactions is an important aspect that would lead to better adaptability of the model to evolving fraud tactics. Collaboration with financial institutions to get different kinds of datasets would further diversify the training data and make the model more robust. Finally, creating a seamless user interface with real-time alert and verifications of transactions would improve user stewardship and security awareness. The proposed modifications are designed to enhance the user's detection ability while simultaneously improving the level of trust associated with UPI systems and thereby facilitate the adoption of safer digital transactions.

REFERENCES

1. Gupta, V., Sharma, S., Nimkar, S., & Pathak, S. (2024). UPI Based Financial Fraud Detection Using Deep Learning Approach. 2024 International Conference on Advances in Computing Research on Science Engineering and Technology, ACROSET2024. https://doi.org/10.1109/ACROSET62108.2024.10743663
2. Gupta, Y., Saxena, N., & Kumar, K. (2024). UPI Fraud Detection Using Machine Learning. International Journal of Advances in Engineering and Management (IJAEM), 6, 29–34. https://doi.org/10.35629/5252-06102934
3. Jagadeesan, S., Arjun, K. S., Dhanika, G., Karthikeyan, G., & Deepika, K. (2024). UPI fraud detection using machine learning. Challenges in Information, Communication and Computing Technology, 755–760. https://doi.org/10.1201/9781003559085-130
4. Just a moment... (n.d.), Retrieved April 23, 2025 romhttps://ijerst.org/index.php/ijerst/article/download/446/421?__cf_chl_tk=ITSX48OaCOpCIn0L5svakC5GPewoNZ_sPhrr59diu_w-1745388721-1.0.1.1-78vTTJYKFoULvcIA1KDUSNRNp4urKUffG_HahIr9bYg
5. Kamble, V. B., Pisal, K., Vaidya, P., & Gaikwad, S. (n.d.). Golden Sun-Rise International Journal of Multidisciplinary on Science and Management Enhancing UPI Fraud Detection: A Machine Learning Approach Using Stacked Generalization. https://doi.org/10.71141/30485037/V2I1P108
6. Karthick, N., Leema Roselin, G., Tamilarasan, M., Kalaiselvi, K., Sudha, S., & Jayanthi, J. (2024). Unified Payment Interface Imposture and Scam Detection Using Deep Learning And ANN. 2024 3rd International Conference on Smart Technologies and Systems for Next Generation Computing, ICSTSN 2024. https://doi.org/10.1109/ICSTSN61422.2024.10671346

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405047|

7. Kumar, P., Selvaraj, S., Balamurugan, S., & Ravi, S. A. (2025). UPI Fraud Detection in Mobile Payment Using a Boost Based Framework. AIP Conference Proceedings, 3279(1). https://doi.org/10.1063/5.0263094/3341764
8. Manju Bhargavi, S., Kesava Ram, B., & Author, C. (n.d.). Enhanced UPI Fraud Detection Using CNN: A Comparative Analysis with Machine Learning Models. https://doi.org/10.54660/.IJMRGE.2025.6.2.452-455
9. Naik, S. K. L., Kiran, A., Kumar, V. P., Mannam, S., Kalyani, Y., & Silparaj, M. (2024). Fraud Fighters - How AI and ML are Revolutionizing UPI Security. Proceedings of 2024 International Conference on Science, Technology, Engineering and Management, ICSTEM 2024. https://doi.org/10.1109/ICSTEM61137.2024.10560740
10. Ragavee, U., Raj, M. P., Mithra, J. N., Sudharshan Balaji, S., Ajay Narayanan, L., & Jacob Mahimai Dass, Y. (2025). A Robust UPI Fraud Identification Scheme over Digital Money Transactions using Learning Powered Classification Principles. 3rd International Conference on Electronics and Renewable Systems, ICEARS 2025 - Proceedings, 1551–1558. https://doi.org/10.1109/ICEARS64219.2025.10941576
11. Raju, M. N., Chandrasena Reddy, Y., Babu, P. N., Pavan Ravipati, V. S., & Chaitanya, V. (2024). Detection of Fraudulent Activities in Unified Payments Interface using Machine Learning - LSTM Networks. Proceedings of International Conference on Circuit Power and Computing Technologies, ICCPCT 2024, 769–774. https://doi.org/10.1109/ICCPCT61902.2024.10672890
12. Rani, R., Alam, A., & Javed, A. (2024). Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions. 2024, 2nd International conference on disruptive technologies, ICDT 2024, 924-928.https://doi.org/10.1109/ICDT61202.2024.10489682
13. Becker RA, Volinsky C, Wilks AR (2010) Fraud Detect Telecommunications 52(1):20–33
14. Dorronsoro JR, Ginel F, Sanchez C, Santa Cruz C (1997) Neural fraud detection in credit card operations. IEEE 8:827–834
15. Hand C, Whitrow DJ, Adams C, Juszczak NM, Weston P D (2008) Performance criteria for plastic card fraud detection. JORS 59(7):956–962

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details