IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Fraud Detection In UPI Transactions Using Ensemble Learning

[1]Ms.Viha Dave, [2]Mr. Dhaval Chudasama

[1]PG Student, [2]Assistant Professor

[1]Department of Computer Engineering,

[2]Department of Cyber Security,

[1]Gandhinagar University, Gandhinagar, India,

[2]Gandhinagar University, Gandhinagar, India

Abstract: Digital payments have been transformed by the quick expansion of Unified Payment Interface (UPI) transactions, but this has also made them more susceptible to fraud. Due to the dataset's extreme imbalance and the fact that fraudulent transactions make up a very small percentage of all transactions, fraud detection in UPI transactions poses difficulties. This study suggests a strong framework for detecting fraud that makes use of ensemble learning techniques, such as XGBoost, LightGBM, and neural networks, to increase prediction accuracy and manage data imbalance. The use of sophisticated ensemble techniques to handle class imbalances such as oversampling, under sampling, and synthetic data generation—as well as the integration of feature engineering to detect anomalous patterns are among the major advances. Numerous tests show that the suggested models can minimize false positives while achieving high detection rates. The findings imply that ensemble learning considerably improves UPI fraud detection systems' effectiveness, offering a scalable and practical solution for practical uses.

Index Terms **- Machine learning, UPI, Fraud detection, Ensemble learning, boosting, XGboost, LightGBM, neural network**

I. INTRODUCTION

A key component of digital payments, the Unified Payment Interface (UPI), allows for smooth, immediate transactions and is transforming the way that financial transactions are carried out. Millions of users and businesses now favor UPI due to its broad adoption, which has accelerated the transition to a cashless economy. Digital payment systems have revolutionized financial transactions in recent years by providing users all around the world with accessibility, speed, and convenience. The Unified Payment Interface (UPI), which was first implemented in India, is one example of an inventive payment system that has completely changed the digital payments scene by making it possible for quick and easy money transfers across bank accounts. [2] But this quick uptake has also made UPI systems vulnerable to fraud, which puts user confidence and financial security at serious risk.

We rely heavily on online payment methods like credit cards, debit cards, and UPI in the twenty-first century. For online transactions, more than 93% of retailers accept mobile websites, mobile apps, or both. Support for mobile wallets can help boost the use of mobile payments in general. Mobile proximity payments, such NFC (NEAR FIELD COMMUNICATION) and QR (QUICK RESPONSES) codes, are growing quickly, and mobile payments now reach $218 billion in 2021. Ovum forecasts that 939.10 million of the 1.09 billion mobile convenience payment customers who will exist between now and 2019 will be NFC. [3]

The rapid growth of online banking services has made it simpler for criminals to exploit flaws, endangering the security and integrity of financial systems. Additionally, the onset of the COVID-19 pandemic has functioned as a catalyst, hastening the transition to remote operations and increasing the likelihood of online fraud. Therefore, considering the epidemic, it is more crucial than ever to develop trustworthy fraud detection technologies, underscoring the need for financial institutions and consumers to fortify their anti-fraud defenses. [6]

However, UPI is a major target for fraudulent activities due to its popularity and widespread use, necessitating creative solutions to address these changing risks. The goal of this research is to create a dynamic fraud detection system designed especially for UPI transactions. Conventional fraud detection techniques sometimes depend on static rules or historical data, which might not be flexible enough to keep up with the quickly changing fraudulent activity scene. [8] Due to the extremely unbalanced structure of transaction data—fraudulent cases make up a very small portion of the whole dataset—detecting fraud in such systems is a difficult undertaking. Under these circumstances, traditional machine learning models frequently fall short of producing precise predictions, either overfitting the majority class or failing to generalize effectively to hidden fraud patterns. This research investigates the use of neural networks and contemporary ensemble learning techniques for fraud detection in UPI transactions to overcome these issues. By integrating the predictive capabilities of several base learners, ensemble approaches—like XGBoost and LightGBM—have demonstrated remarkable efficacy in handling unbalanced datasets, providing greater accuracy and resilience than conventional machine learning algorithms. Neural networks improve the ability to identify fraudulent activity with little assistance from humans by learning intricate patterns and relationships in high-dimensional data. To produce more accurate and dependable findings than conventional methods, the main objective of this study is to design and implement a fraud detection framework that makes use of the advantages of contemporary machine learning techniques.

By putting its suggested future improvements into practice, this study expands on the work done on the foundation paper "UPI Fraud Detection Using Machine Learning" by Harshith Kumar S. and Dr. H.R. Divakar. It uses cutting-edge machine learning models like Neural Networks, XGBoost, and Gradient Boosting to increase the precision and versatility of fraud detection. Additionally, by using strategies to deal with the disproportionate representation of fraudulent transactions, this study tackles the problem of dataset imbalance, a major constraint in fraud detection systems.

II. PROBLEM STATEMENT

Fraudulent activity has increased because of UPI's growing usage. The dynamic and complex nature of contemporary fraud schemes frequently makes traditional fraud detection techniques insufficient. To protect the integrity of the UPI ecosystem, this research attempts to provide a reliable and flexible fraud detection framework that uses ensemble learning approaches to increase the precision and effectiveness of detecting fraudulent UPI transactions.

Creating efficient fraud detection algorithms is made extremely difficult by the unbalanced structure of transactional data, where fraudulent cases are much less common than valid ones. To rectify this imbalance and enhance the precision of fraud detection in UPI transactions, this study suggests an ensemble learning-based strategy, guaranteeing a safe and dependable digital payment system.

To avoid monetary losses and safeguard user interests, real-time fraud detection in UPI transactions is essential. To provide a safe and effective UPI ecosystem, this project attempts to create a real-time fraud detection system that uses ensemble learning techniques to precisely identify and mitigate fraudulent activity.

III. REVIEW OF LITERATURE

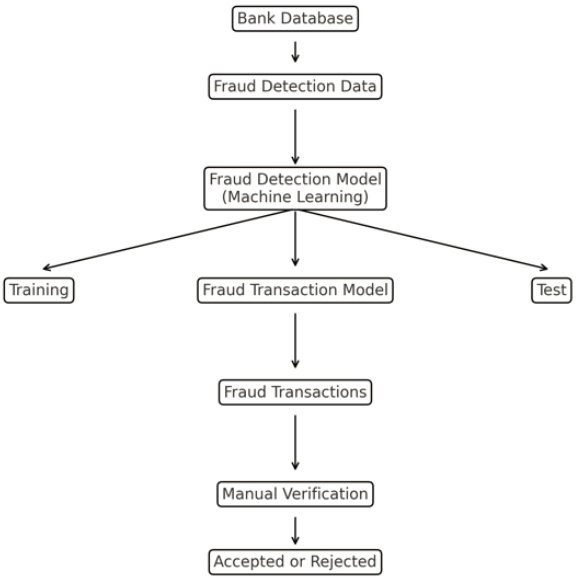

Figure 1Flowchart on Fraud Detection System [3][11]

Using the information acquired from the bank database, a fraud detection system (Fig. 1) trains and learns to create a model that best reflects the characteristics of the transaction data. Figure 1: The flow of the fraud system [3][11]. The model is then used to evaluate trades and determine whether they can be accepted as legitimate transactions or rejected as fraudulent ones. Executing and then adding a transaction that has been approved to the database will enhance the model. If a transaction is rejected, it will instead be reviewed manually. If the rejected transaction is checked and found to be normal, the transaction is executed and the data is added to the bank's database; if not, the transaction is rejected. A key component of the fraud detection and prevention process is training and learning from transaction data to identify future frauds [3][11]. Because fraud can be quickly detected and prevented, it is imperative to develop a model using the best data mining and machine learning algorithms. In addition to accurately identifying frauds, a well-designed model would be able to predict the likelihood of fraud.

According to study in [1][6], the necessity for strong fraud detection systems has increased due to the COVID-19 pandemic's acceleration of the spread of digital transactions and online banking. One noteworthy study investigates the use of sophisticated machine learning methods to detect fraudulent Unified Payments Interface (UPI) transactions, including Convolutional Neural Networks (CNNs), Decision Trees, Naive Bayes, and Logistic Regression using L1 and L2 regularization. While Decision Trees offer efficiency and interpretability, CNNs are excellent at extracting hierarchical features to identify intricate fraud patterns. While Logistic Regression tackles multicollinearity and improves model interpretability, Naive Bayes is praised for its ease of use when managing independent features. Through the integration of various strategies, the study offers a thorough framework for preventing UPI fraud and provides important insights into the real-world application of machine learning in dynamic, high-risk financial settings.

As per studies in [2], by using the output of earlier phases as input for later ones, recurrent neural networks (RNNs) have become a specialized kind of neural network that can handle sequential data. RNNs do exceptionally well in tasks where context and sequence are important, like predicting the next word in a phrase, in contrast to standard neural networks, which presume independence between inputs and outputs. RNNs are distinguished by their hidden or "memory" mode, which allows the network to efficiently model dependencies in the data by storing information from prior inputs. Compared to other neural networks, RNNs greatly minimize parameter complexity by using the same parameters for all inputs and hidden layers, which not only preserves processing consistency. RNNs are especially useful for jobs involving time series, natural language processing, and other sequential data issues because of their capacity to retain and comprehend sequential information.

According to a survey conducted in [7], financial institutions face serious risks from credit default, which is defined as a borrower's inability to repay a loan according to the terms of the agreement. This is especially true for non-performing loans (NPLs). Depending on the type of loan, nonpayment within 90 to 180 days results in these classifications, necessitating proactive measures by institutions to mitigate fraud risks. Guidelines for categorizing and reporting frauds, establishing provisioning requirements, and putting risk mitigation strategies like Red Flagged Accounts (RFA) in place for loans over INR 50 crore have all been adopted by the Reserve Bank of India (RBI). To enable prompt fraud identification and reporting, RFAs

seek to discover Early Warning Signals (EWS) and any red flags. Machine learning has become a powerful tool for fraud detection in the face of mounting worries about delayed detection and a lack of timely information exchange. Methods like Decision Trees, Random Forest, Linear Regression, and Gradient Boosting Methods show great promise for more accurately and quickly detecting and forecasting loan fraud. This research emphasizes how machine learning may improve fraud detection systems and guarantee proactive risk management in banking systems.

[8] says that traditional approaches to fraud detection primarily rely on historical data or static rules, which frequently can't adjust to new fraudulent trends. On the other hand, proactive and flexible solutions are provided by dynamic fraud detection techniques, such those used in UPI transactions. These systems may continually learn and update their detection policies based on real-time transactional data thanks to sophisticated approaches like Deep Reinforcement Learning (DRL). Dynamic systems can automatically modify their detection tactics in response to shifting patterns and abnormalities, strengthening their defenses against scammers. This method improves the general security and integrity of UPI transactions, which makes it a viable way to detect fraud in real time.

Studies in [5] say that effective fraud detection requires a thorough understanding of the data flow within the UPI ecosystem since it makes it possible to distinguish between fraudulent and valid transactions as well as between typical and suspicious user behavior. Evaluating current security measures and their shortcomings to identify any holes that require attention is a crucial component of dynamic fraud detection. Researchers can find key characteristics that are most suggestive of fraudulent activity by examining these components. Furthermore, choosing the right machine learning algorithms—like Support Vector Machine, Random Forest, and Decision Tree—becomes essential for creating efficient fraud detection models. The use of these algorithms is crucial for precisely detecting fraudulent transactions in the UPI ecosystem since they provide a variety of classification techniques.

Table 1Comparative Study of literature survey

Name of the study	**Methodologies**	**Findings**	**Strengths**	**Limitations**
Yarramreddy Chandrasena Reddy, Polavarapu Nagendra Babu, Venkata Sai Pavan Ravipati, Velpula Chaitanya. (2024). UPI Fraud Detection Using Convolutional Neural Networks (CNN). Research Square. https://doi.org/10.21203/rs.3.rs-4088962/v1	CNN, Decision Trees, Naïve Bayes, Logistic Regression (L1, L2 Regularization)	Decision trees offer efficiency and interpretability, while CNNs are excellent at extracting hierarchical features. Multicollinearity is addressed by logistic regression.	Thorough ML strategy incorporates several techniques.	CNN computational complexity: Naïve Bayes implies feature independence.
[2] Mr. R. Ramakrishnan, S. Vanisri, D. Yuvalakshmi. (2024). Unified Payment Interface Seamless Transaction Using RNN Model. INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS), 04(05), 1279-1283. https://www.doi.org/10.58257/IJPREMS34325	Recurrent Neural Networks (RNNs)	RNNs are appropriate for time-series fraud detection because of their ability to handle sequential data efficiently.	Effective for time-dependent fraud patterns, memory retention occurs in consecutive transactions.	Diminishing gradient problem; high computing expense.
[3] Manav Mangukiya, Meet Savani, Anuj Vaghani, Aryan Khunt. (2023). Financial Fraud Detection Approaches Using Machine Learning. Gujarat Technological	Methods for detecting fraud based on machine	Highlights how crucial it is to improve fraud	Demonstrates how ML is used in adaptive	Lacks detailed implementation information for the

University, PAPER ID: PCP386.	learning	detection by learning from previous fraudulent transactions.	fraud detection.	algorithm.
[4] Sayalee S. Bodade, P.P. Pawade. (2023). Review Paper on UPI Fraud Detection Using Machine Learning. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 11(12). https://doi.org/10.22214/ijraset.2023.57551	General Machine Learning techniques for UPI fraud detection	Examines various machine learning models and emphasizes how they can be used to detect fraud.	Offers a comprehensive viewpoint on fraud detection using machine learning.	Doesn't offer any empirical support.
[5] Harshith Kumar S, Dr. H.R. Divakar. (2024). UPI Fraud Detection Using Machine Learning. International Research Journal of Modernization in Engineering Technology and Science, 06(08). https://www.doi.org/10.56726/IRJMETS60849	Support Vector Machine, Random Forest, Decision Trees	ML models have the potential to differentiate between authentic and fraudulent transactions.	Highlights salient characteristics of fraud; effective classification.	Real-time fraud detection has not received much attention.
[6] J. Kavitha, G. Indira, A. Anil kumar, A. Shrinita, D. Bappan. (2024). Fraud Detection in UPI Transactions Using ML. *EPRA International Journal of Research and Development (IJRD), 09(04). https://doi.org/10.36713/epra16459	Machine Learning techniques for UPI fraud detection	Draws attention to fraud trends and the need for robust fraud detection systems.	Provides a methodical methodology for preventing UPI fraud.	Does not specify certain methods of implementation.
[7] M. ValavanAnita B. Desai, Dr. Ravindra Deshmukh and S. Rita. (2022). Predictive-Analysis-based Machine Learning Model for Fraud Detection with Boosting Classifiers. 10.32604/csse.2023.026508	Boosting Classifiers (Gradient Boosting, Random Forest, Decision Trees)	ML techniques improve risk reduction and credit fraud detection approaches.	Adaptive learning works well with unbalanced datasets.	The cost of computation must be adjusted.
[8] L.SaiSampanPatrudu, D.Noorisha, E.Sidharatha, V.SaiRagaSudha, DrK.V.Satyanarayana. (2024). DynamicFraud Detection in UPI Transactions. Industrial Engineering Journal, 53(04).	Deep Reinforcement Learning (DRL)	Emerging fraud patterns can be dynamically adjusted by DRL-based fraud detection systems.	Adaptive learning and real-time fraud detection.	Computationally costly; a large amount of training data is needed.
[9] K. Krithiga Lakshmi, Himanshu Gupta, Jayanthi Ranjan. (2019). UPI Based Mobile Banking Applications – Security Analysis and Enhancements. IEEE	An examination of UPI mobile banking apps' security	Finds and recommends improvements for security flaws in UPI transactions.	Offers workable security solutions to reduce fraud.	Restricted to topics of theoretical security.
[10] Dr. S. Jamuna, Dr. J.R.Gaur, Anshu Singh, Dharam Barot. (2023). A REVIEW RESEARCH ON ONLINE FINANCIAL	Online financial fraud	Investigates the patterns of financial fraud	Overview of India's efforts to	Does not focus on ML-

FRAUDS IN INDIA. The American Journal of Management and Economics Innovations, 05(01), 1-7. https://doi.org/10.37547/tajmei/Volume05Issue01-01	detection techniques	in India.	detect online fraud.	based fraud detection.
[11] Anita B. Desai, Dr. Ravindra Deshmukh. (2013). Data mining techniques for Fraud Detection. International Journal of Computer Science and Information Technologies, 4(1), 1-4.	Data Mining Techniques	Draw attention to how data mining can be used to uncover fraud.	Preliminary research on data mining for fraud detection.	Lacks contemporary machine learning techniques.
[12] Akshayapatra Lakshmi Harshini. (2021). A COMPARATIVE STUDY OF UPI AND TRADITIONAL PAYMENT METHODS: EFFICIENCY, ACCESSIBILITY, AND USER ADOPTION. International Journal of Computer Science and Engineering Research and Development (IJCSERD), 1, 10-16	A comparison between UPI and conventional payment methods	Assesses the effectiveness, usability, and uptake of UPI payments.	Gives information about the trends of UPI use.	Does not concentrate on detecting fraud.

IV. IMPLEMENTATION

4.1Existing System

The existing system for UPI fraud detection, as discussed in the base paper by Harshith Kumar S and Dr. H.R. Divakar, provides a foundational framework for understanding and addressing the vulnerabilities in the UPI transaction ecosystem. The system begins with a comprehensive analysis of the UPI transaction processes, focusing on the data flow within the ecosystem. This includes mapping the lifecycle of transactions, from initiation to completion, to identify points of potential exploitation by fraudsters.

A critical part of the existing system involves distinguishing between legitimate and fraudulent transactions. This distinction is achieved by examining the inherent characteristics and behavioral patterns associated with each type of transaction. Legitimate transactions often follow predictable patterns, while fraudulent transactions exhibit anomalies or irregularities in parameters such as frequency, transaction amount, and user location. By analyzing these patterns, the system seeks to identify and flag suspicious activities effectively.

The existing system also evaluates the current security measures within the UPI ecosystem, identifying their strengths and limitations. While these measures provide a baseline level of security, they often rely on static rules or predefined thresholds, making them less effective against evolving and sophisticated fraud techniques. This limitation highlights the need for adaptive, data-driven methods to enhance detection capabilities. [13]

To address these challenges, the existing system utilizes machine learning algorithms such as Decision Tree, Random Forest, and Support Vector Machine (SVM). These algorithms are employed to identify key features indicative of fraudulent activities and to build predictive models capable of distinguishing between legitimate and fraudulent transactions. Decision Trees offer simplicity and interpretability, Random Forests enhance robustness and accuracy through ensemble learning, and SVMs provide high precision in detecting complex patterns within data.

Through this detailed examination and application of machine learning techniques, the existing system lays the groundwork for developing more advanced fraud detection frameworks that can adapt to the dynamic and ever-evolving nature of fraudulent activities in UPI transactions.[14]

4.2 Proposed System

As described in their paper UPI Fraud Detection Using Machine Learning, Harshith Kumar S. and Dr. H.R. Divakar laid the groundwork for the suggested approach. It specifically tackles the future scope that was emphasized in their work, with an emphasis on improving the accuracy of fraud detection, integrating real-time adaptation. By incorporating Gradient Boosting, XGBoost, and Neural Networks into the fraud detection framework, the suggested system carries out the future enhancement described in the base study. These models were used because they can handle intricate patterns and increase the precision of detection.

The following primary goals are highlighted by the suggested system:

1. **Detection in Real Time**
   Dynamic Model Implementation: To adjust to changing fraud strategies, the system will use machine learning models that can be updated continuously with fresh data.
   Real-Time Analysis: By processing and analyzing transactions in real-time, the technology makes it possible to spot suspicious activity right away.
   Reduced Response Time: The system can drastically cut down on the amount of time needed to start preventive actions by quickly identifying and flagging fraudulent transactions.
2. **Managing Unbalanced Data**
   Ensemble Learning: When working with unbalanced datasets, combining many machine learning models, such as XGBoost, LightGBM, and neural networks, can enhance the system's overall performance.
3. **Enhanced Precision**
   Advanced Algorithms for Machine Learning:
   i) **XGBoost:** A potent gradient boosting method renowned for its great accuracy and effectiveness is called XGBoost.
   ii) **LightGBM:** A more rapid and effective gradient boosting method that works well with big datasets.
   iii) **Neural Networks:** Deep learning models that can identify elaborate fraud schemes by extracting complex patterns from data.

   Reduced False Positives: The system will be adjusted to reduce the quantity of valid transactions that are mistakenly reported as fraudulent, cutting down on pointless enquiries and enhancing user experience.
4. **Adaptability in Dynamic**
   Self-Learning Mechanisms: To continuously learn from fresh data and enhance its decision-making skills, the system will use reinforcement learning techniques.
   Adapting to Changing Fraud Patterns: By automatically updating its models and modifying its detection thresholds, the system will be able to respond to new fraud strategies.

IV. RESULTS AND DISCUSSION

According to different studies, it is observed that ensemble learning outperforms as compared to other conventional techniques.

The studies infer the fact that the real-time situations in which the UPI transactions falling under the category of fraudulent are very less as compared to non-fraudulent transactions which have immensely increased in this advanced era. This actually results in the overall imbalancing of the dataset which contain both fraudulent and non-fraudulent UPI transactions.

Due to the imbalanced nature, most of the conventional ML techniques are likely to overfit and results may not be accurate enough to imply the correct prediction about the fraudulent UPI transactions which are already observed to be very less while analysing the non-fraudlent ones. This implies the actual demand of using more sophisticated models for better performance resulting into predictions which can accurately categorise the fraudulent transactions.

Also, depending completely on a model's working and predictions can actually result into a shallow analysis of the overall nature of the dataset because a model can only focus on the properties identified according to its internal working on which it is based. But in detecting the patterens of the fraudulent UPI transactions, we need more detailed and precise working models which can deeply penetrate into every single trait and can come to the conclusion by considering all the possibilities. This again signifies that using more advanced ML techniques like neural networks and ensemble learning can not only give the accurate results but can also identify the precise properties of the fraudulent transactions.

As we know that neural networks are supposed to penetrate deep inside the dataset and extract all the required information needed to come to a conclusion but using ensemble learning can also help in incurring best results from the combination of outcomes obtained from different techniques altogether. This can have a more convincing effect on the analyst's mind to be more assured of the results obtained.

Studies from [9], [10] and [12] focus more on the cause of the problem but does not really infer the ways of detecting the actual traits of increasing frauds. [1] and [2] determines the need to use neural networks instead of the methods which may not analyze the properties of the data elements deeply. As shown in [2],

the recurrent neural networks can identify and analyze the sequential patterens in the data efficiently and can give the results more clearly. Comparing the studies done in [5] and [6], [3] proves the point of using latest ML techniques and gives more analysis by using some better ML algorithms but again it is likely to be lacking in detailed implementation. [7] seems to be good at choosing the technique which can focus not only on the patterens of the overall dataset but also made to believe that learning from the previous states can result in more filtered and precised outputs.

Hereby, observing all the implemented studies, it is concluded that using more sophisticated ML techniques like neural networks and ensemble learning techniques, we can have better and precised results.

V. CONCLUSION

In conclusion, the suggested system's uniqueness is in its capacity to learn, change dynamically, and examine transactions from a variety of angles. The limits of conventional systems are greatly enhanced by the combination of ensemble learning, reinforcement learning, geolocation checks, and behavioral analysis, which results in a strong and all-encompassing fraud detection mechanism. High detection accuracy and flexibility in response to the constantly changing nature of fraudulent activity within the UPI ecosystem are guaranteed by this multifaceted approach.

REFERENCES

[1] Yarramreddy Chandrasena Reddy, Polavarapu Nagendra Babu, Venkata Sai Pavan Ravipati, Velpula Chaitanya. (2024). UPI Fraud Detection Using Convolutional Neural Networks(CNN). Research Square. https://doi.org/10.21203/rs.3.rs-4088962/v1

[2] Mr. R. Ramakrishnan, S. Vanisri, D. Yuvalakshmi. (2024). Unified Payment Interface Seamless Transaction Using RNN Model. INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS) , 04(05), 1279-1283. https://www.doi.org/10.58257/IJPREMS34325

[3] Manav Mangukiya, Meet Savani, Anuj Vaghani, Aryan Khunt. (2023). Financial Fraud Detection Approaches Using Machine Learning. Gujarat Technological University, PAPER ID: PCP386.

[4] Sayalee S. Bodade, P.P. Pawade. (2023). Review Paper on UPI Fraud Detection Using Machine Learning. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 11(12). https://doi.org/10.22214/ijraset.2023.57551

[5] Harshith Kumar S, Dr. H.R. Divakar. (2024). UPI Fraud Detection Using Machine Learning. International Research Journal of Modernization in Engineering Technology and Science, 06(08). https://www.doi.org/10.56726/IRJMETS60849

[6] J. Kavitha, G. Indira, A. Anil kumar, A. Shrinita, D. Bappan. (2024). Fraud Detection In UPI Transactions Using ML. *EPRA International Journal of Research and Development (IJRD), 09(04). https://doi.org/10.36713/epra16459

[7] M. ValavanAnita B. Desai, Dr. Ravindra Deshmukh and S. Rita. (2022). Predictive-Analysis-based Machine Learning Model for Fraud Detection with Boosting Classifiers. 10.32604/csse.2023.026508

[8] L.SaiSampanPatrudu, D.Noorisha, E.Sidharatha, V.SaiRagaSudha, DrK.V.Satyanarayana. (2024). DynamicFraud Detection in UPI Transactions. Industrial Engineering Journal, 53(04).

[9] K. Krithiga Lakshmi, Himanshu Gupta, Jayanthi Ranjan. (2019). UPI Based Mobile Banking Applications – Security Analysis and Enhancements. IEEE

[10] Dr. S. Jamuna, Dr. J.R.Gaur, Anshu Singh, Dharam Barot. (2023). A REVIEW RESEARCH ON ONLINE FINANCIAL FRAUDS IN INDIA. The American Journal of Management and Economics Innovations, 05(01), 1-7. https://doi.org/10.37547/tajmei/Volume05Issue01-01

[11] Anita B. Desai, Dr. Ravindra Deshmukh. (2013). Data mining techniques for Fraud Detection. International Journal of Computer Science and Information Technologies, 4(1), 1-4.

[12] Akshayapatra Lakshmi Harshini. (2021). A COMPARATIVE STUDY OF UPI AND TRADITIONAL PAYMENT METHODS: EFFICIENCY, ACCESSIBILITY, AND USER ADOPTION. International Journal of Computer Science and Engineering Research and Development (IJCSERD), 1, 10-16