JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

UPI FRAUD DETECTION USING MACHINE LEARNING

[1]Dr C Nadhamuni Reddy, [2]Mr E D Pavan Kumar, [3]S Karishma, [4]Y Prashanthi,

[5]M Varshini, [6]D Shafi Qur Rehaman

[1]Professor, [2] Assistant Professor,[3456]Student

[1]Department of Mechanical,[23456]Department of Artificial Intelligence & Data Science

[123456]Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh – 517520 India

***Abstract*: As digital transactions have become more common, UPI (Unified Payments Interface) fraud has increased, making strong detection methods necessary. In order to detect fraudulent activity, this project offers a machine learning-based UPI fraud detection system that examines transaction patterns. Transaction information including amount, merchant category, frequency, and location anomalies make up the dataset. We handle missing values, encode category variables, and normalise numerical features as part of our preprocessing steps. A number of machine learning models are trained and assessed, such as Random Forest, Logistic Regression, Gradient Boosting, and XGBoost. The highest level of fraud detection accuracy is guaranteed by feature importance analysis. The top-performing model successfully separates fraudulent transactions from authentic ones by achieving high precision and recall. By reducing financial risks associated with digital payments and offering real-time fraud detection, this technology improves financial security.**

***Keywords*— Data preprocessing, feature engineering, random forest, xgboost, real-time detection, cybersecurity, risk mitigation, machine learning, digital payments, transaction analysis, anomaly detection, fraud prevention, financial security,UPI fraud detection.**

I. INTRODUCTION

In many areas, the Unified Payments Interface (UPI) has become the primary means of conducting financial transactions due to the quick uptake of digital payment systems. Although UPI provides quick and easy money transfers, its rising popularity has also resulted in a rise in fraud, putting consumers' and financial institutions' security at significant risk. Via phishing, social engineering, and illegal transactions, fraudsters take advantage of system flaws to cause large financial losses. An advanced fraud detection system that can proactively identify and neutralise fraudulent transactions in real time is therefore desperately needed.

The goal of this project is to create a machine learning-based UPI fraud detection system that analyses transactional data to identify suspicious activity and anomalies. Based on important transaction characteristics including amount, frequency, and user behaviour, the system uses the Random Forest and XGBoost algorithms to categorise transactions as either authentic or fraudulent. The model minimises false positives while ensuring high accuracy in detecting fraudulent patterns through the use of feature engineering and data preparation approaches. Including real-time detection tools improves security and assists users in preventing financial losses before they happen.

Through the provision of an effective fraud detection framework that continuously learns and adjusts to new fraud patterns, the proposed system seeks to improve cybersecurity in digital payments. Financial institutions and payment service providers can enhance trust in UPI-based transactions and proactively prevent unauthorised transactions by employing machine learning techniques. By using AI-driven risk assessment models for more thorough fraud detection and prevention tactics, this initiative will not only help prevent fraud but also open the door for future developments in financial security.

II.LITERATURE SURVEY

Research on financial transaction fraud detection has been crucial, and machine learning has emerged as a potent instrument for spotting fraudulent activity. In order to improve the precision and effectiveness of fraud detection systems, numerous studies have investigated various algorithms and approaches. In order to prevent fraud in digital payments, Ramachandran [1] looked at the function of dynamic risk-scoring models, highlighting the necessity of real-time anomaly detection. In a similar vein, Nagaraju et al. [2] suggested a fraud detection model based on Long Short-Term Memory (LSTM) networks that recognises anomalous activity in UPI transactions by learning patterns from transactional data. Their study showed that deep learning methods could detect fraud more effectively than conventional rule-based systems.

To enhance the fraud detection process, another strategy concentrates on feature selection and data preprocessing. The influence of feature engineering strategies was examined by Tressa et al. [3], who demonstrated that choosing pertinent transaction attributes greatly enhances model performance. With findings relevant to UPI fraud detection, Sabbani [4] investigated the use of artificial intelligence (AI) in identifying credit card transaction fraud. Furthermore, Dahiphale et al. [5] highlighted the expanding relevance of AI in financial security by proposing a machine learning framework that makes use of Large Language Models (LLMs) to analyse transaction descriptions and identify fraudulent tendencies.

To improve the accuracy of fraud detection, hybrid models that combine many machine learning methods have also been investigated. In order to obtain high precision in identifying fraudulent transactions, Rani et al. [6] looked into an ensemble-based fraud detection model that combines Random Forest and Gradient Boosting classifiers. Devi and Indoria [7] examined how consumers view UPI security and emphasised the importance of user awareness in preventing fraud. Additionally, a study by Mubarokah et al. [8] on QR code-based payments identified certain weaknesses that scammers could take advantage of. All of these research demonstrate how important machine learning is to enhancing fraud detection systems and protecting online transactions.

Inference of the Literature Survey

The literature review emphasises the importance of machine learning in identifying UPI fraud, highlighting the efficiency of feature selection methods [3], deep learning models such as LSTMs [2], and hybrid ensemble approaches [6] in raising the accuracy of fraud detection. Research shows that by dynamically examining transaction patterns and spotting irregularities instantly, AI-driven systems perform better than conventional rule-based techniques [1]. Additionally, studies show that thorough fraud protection requires resolving weaknesses in QR code-based payments [8] and raising user security awareness [7]. According to recent studies [5], combining AI with transactional data analysis improves fraud detection systems and increases their ability to adjust to changing fraudulent strategies.

III.PROPOSED METHODOLOGY

1.Gathering and Preparing Data: Gathering transactional data from UPI payment systems, including attributes such transaction amount, sender and recipient details, transaction time, and device information, is the first stage in the suggested process. Next, missing values are handled, duplicate records are eliminated, and numerical features are normalised as part of the preprocessing of the gathered data. To make them appropriate for machine learning models, categorical data like transaction category and merchant type are also included. To extract valuable insights, such as transaction frequency and departure from typical transaction behaviour, feature engineering is also carried out.

2.Engineering and Feature Selection: To improve the accuracy of the model, pertinent characteristics are chosen using statistical techniques and domain expertise following preprocessing. To find the most important predictors of fraudulent transactions, methods like Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE) are used. By generating new features like transaction velocity, transaction location consistency, and peer-to-peer transaction frequency, feature engineering enhances model performance even more. By guaranteeing that the model is trained on the most instructive data, this stage lowers computational complexity and noise.

3.Selection and Training of Machine Learning Models: To identify fraud, supervised and unsupervised machine learning techniques are used in conjunction. To categorise transactions as either fraudulent or valid, supervised models like Random Forest, Gradient Boosting, and Support Vector Machines (SVM) are trained on labelled datasets. Furthermore, abnormalities in real-time transactions without previous labels are found using unsupervised models such as Autoencoders and Isolation Forests. To maximise performance, hyperparameter adjustment is done after the models have been trained using historical data. Each model's efficacy is evaluated using a variety of metrics, such as precision, recall, F1-score, and AUC-ROC.

4. Implementation of a Real-Time Fraud Detection System: A real-time fraud detection system that continuously scans transactions for questionable trends using the trained models. To identify high-risk transactions and enable prompt response, an alert system is incorporated. To reduce false positives and increase decision-making accuracy, machine learning predictions are paired with a rule-based filtering system. In order to ensure adaptability to new fraud patterns, a feedback loop is also included, in which analysts evaluate flagged transactions and utilise the results to retrain and improve the model on a regular basis.

5. Development of Interfaces : To enable real-time fraud detection and user involvement, an intuitive user interface is created. The

interface offers fraud alerts, real-time transaction monitoring, and a user-friendly dashboard for examining transactions that have been detected. To guarantee smooth functioning, the system is connected with UPI payment infrastructures through APIs. For transactions that are flagged, security elements like biometric verification and OTP reauthorisation are implemented. In order to support ongoing model refinement, a user reporting system is also introduced, enabling clients to flag questionable activities. To assist users in identifying and avoiding fraud efforts, educational pop-ups and user awareness campaigns are also included.

IV. Workflow

1.Information Gathering and Preservation : Obtaining transactional data from banks, financial institutions, and UPI payment gateways is the initial stage. Real-time transaction logs, past transaction records, and user reviews of fraudulent transactions are examples of data sources. A structured database is used to safely store the gathered data, guaranteeing data integrity and adherence to privacy laws. To enable real-time fraud detection, a data pipeline is set up to continuously add new transactions to the database.

2. Pattern Recognition and Data Analysis: To find patterns and irregularities in transaction behaviour, exploratory data analysis, or EDA, is carried out after the data has been gathered. Common fraud tendencies, like abnormally large transaction amounts, abrupt transaction bursts, and location irregularities, are identified using statistical techniques and visualisation tools. By classifying transactions into normal and suspect classifications, clustering techniques assist identify anomalies in user behaviour and improve fraud detection tactics.

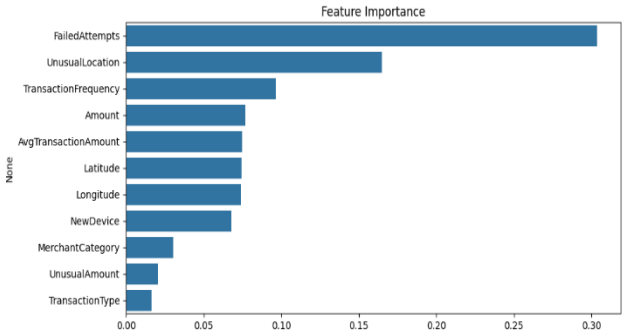
3. Implementation of Fraud Detection Models: Machine learning models built on historical data are used to categorise fresh transactions if pertinent fraud tendencies have been found. The models continuously scan incoming transactions for unusual activity while operating in real-time. Every transaction is given a fraud risk score by the system based on a number of criteria, and transactions that over a predetermined threshold are marked for additional examination. To keep up with changing fraud strategies, the model is routinely retrained using fresh data.

V.DATA ACQUISTION

1. **User information and transactional data:** TransactionID, UserID, Amount, Timestamp, and MerchantCategory are among the crucial details that are recorded in this collection of UPI transactions. Because each transaction is uniquely identifiable and associated with a particular user, it is feasible to monitor their spending patterns. The information helps analyse consumer spending trends by classifying transactions into merchant categories including retail, restaurants, and travel. We can spot odd activity, such high-value transactions or excessive frequency, that can point to fraudulent activity by looking at transaction trends. Models for risk assessment and fraud detection can benefit from the dataset's comprehensive picture of financial transactions.

2. **Tracking Devices and Locations:** DeviceID, IPAddress, Latitude, and Longitude are among the device and network-related parameters included in the information, which makes it possible to identify fraudulent activity based on device usage and geographic location. In order to help identify possible fraud, the UnusualLocation feature highlights transactions done from places that are noticeably different from the user's usual behaviours. While DeviceID guarantees that the transaction comes from a recognised device, monitoring IPAddress changes can show unauthorised access attempts. Additional security checks may be triggered to stop fraudulent activity and unauthorised access to user accounts if a transaction is completed from an unusual device or location.

3. **Behavioural Characteristics and Transaction Patterns:** This dataset contains features like AvgTransactionAmount, TransactionFrequency, and UnusualAmount, which are important behavioural patterns in fraud detection. While TransactionFrequency offers information on how frequently a user makes transactions (e.g., 5/day or 3/day), the AvgTransactionAmount field aids in identifying the individual's normal spending patterns. Whether a transaction is noticeably larger than the user's typical spending pattern is indicated by the UnusualAmount flag. By examining these trends, anomalies can be found and marked as possibly fraudulent activity, enabling fraud detection systems to decide on transaction legality and security threats in real time.



4. **Indicators for Fraud Detection:** Fraud detection indicators such as FraudFlag, FailedAttempts, and NewDevice are included in the collection. A transaction from a previously unseen device may suggest an attempt at account takeover if NewDevice is declared TRUE. The number of unsuccessful transaction attempts, which frequently indicate fraudulent

access attempts, is recorded in the FailedAttempts field. An essential element for machine learning model training is the FraudFlag label, which shows if a transaction has been flagged as fraudulent. These indicators can be used to train fraud detection algorithms to identify fraudulent transaction patterns and enhance real-time fraud protection strategies.

SYSTEM ARCHITECTURE:

The UPI Fraud Detection system's architecture is made to process transaction data effectively and spot fraudulent activity instantly. The User Interface (UI), where users enter transaction details, is the first of the architecture's many essential parts. The Preprocessing Module receives this data after it has been cleaned, normalised, and organised for additional analysis. Key transaction attributes such transaction amount, frequency, location, and device usage are extracted by the Feature Engineering Module following preprocessing. These characteristics are essential for spotting odd behaviours and suspicious patterns linked to fraudulent transactions.

The Machine Learning Model evaluates the processed data after feature extraction is finished and categorises transactions as either authentic or fraudulent. The Transaction Dataset's historical transaction data is used to train this model, enabling it to identify trends in fraudulent activity. For effective predictions in real-time applications, the trained model is stored in a Fraud Detection Model File. The user can then take the appropriate action when the User Interface shows them the fraud detection results. This architecture improves the security of UPI transactions by guaranteeing a scalable, precise, and automated fraud detection mechanism.

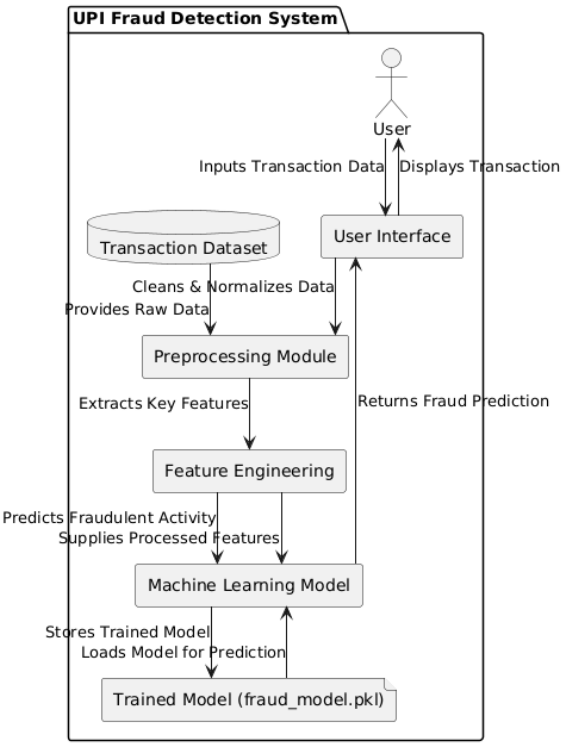
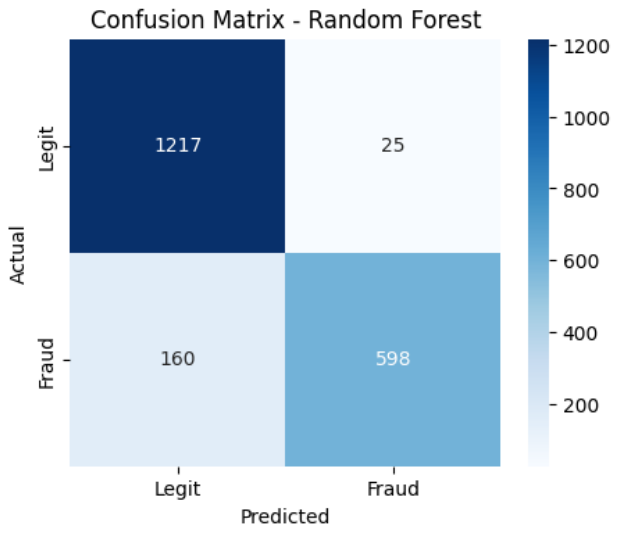


Fig 1 System Architecture

VI . RESULTS AND DISCUSSION

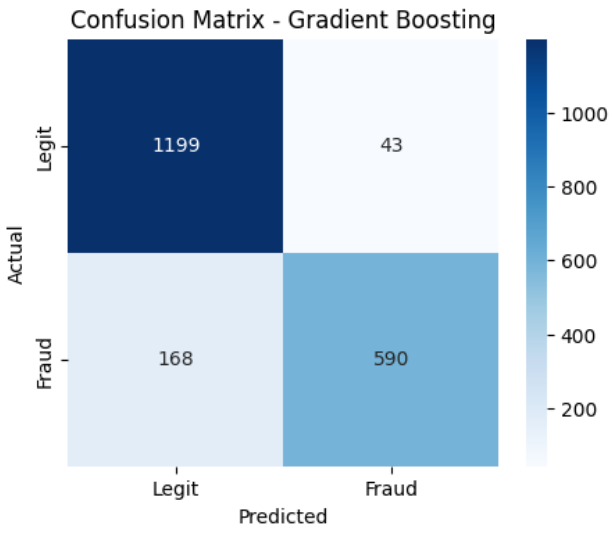
According to the results, Random Forest was the best model for identifying fraudulent UPI transactions, with the greatest accuracy of 90.75%. Additionally, it had the best memory and precision balance, especially when it came to spotting fraudulent transactions. LightGBM and Gradient Boosting came in second and third, respectively, with accuracy scores of 89.35% and 89.45%. These models also showed a high degree of accuracy in identifying fraudulent activity, while having somewhat lower recall values. The accuracy values of XGBoost and CatBoost were 89% and 88%, respectively, indicating comparable performance. With an accuracy of 83.90%, Logistic Regression was the least accurate, especially when it came to fraud detection recall.

RANDOM FOREST:



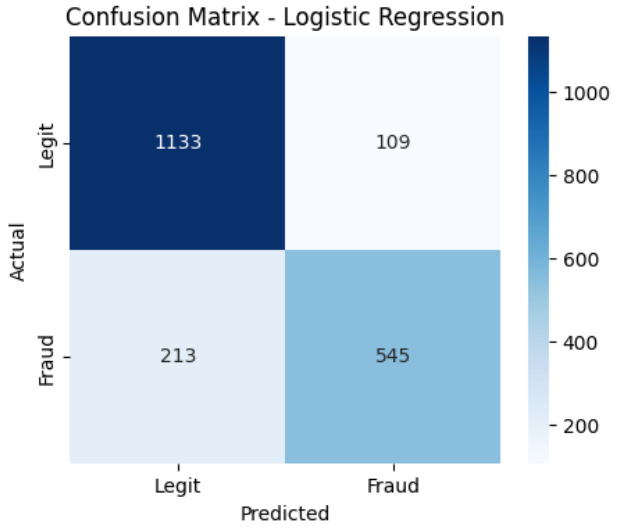
Metric	False (Legit)	True (Fraud)	Macro Avg	Weighted Avg
Precision	0.88	0.96	0.92	0.91
Recall	0.98	0.79	0.88	0.91
F1-Score	0.93	0.87	0.90	0.91
Support	1242	758	-	2000
Accuracy	**0.9075**	-	-	-

GRADIENT BOOSTING RESULTS:



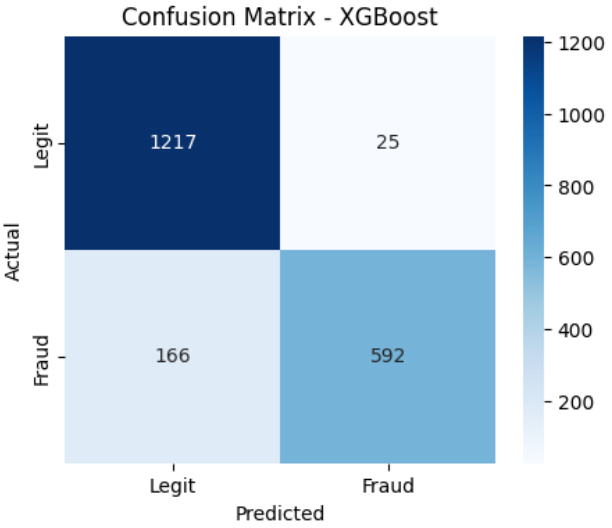
Metric	False (Legit)	True (Fraud)	Macro Avg	Weighted Avg
Precision	0.88	0.93	0.90	0.90
Recall	0.97	0.78	0.87	0.89
F1-Score	0.92	0.85	0.88	0.89
Support	1242	758	-	2000
Accuracy	**0.8945**	-	-	-

LOGISTIC REGRESSION RESULTS:



Metric	False (Legit)	True (Fraud)	Macro Avg	Weighted Avg
Precision	0.84	0.83	0.84	0.84
Recall	0.91	0.72	0.82	0.84
F1-Score	0.88	0.77	0.82	0.84
Support	1242	758	-	2000
Accuracy	**0.8390**	-	-	-

XGBOOST RESULTS:



Metric	False (Legit)	True (Fraud)	Macro Avg	Weighted Avg
Precision	0.89	0.88	0.89	0.89
Recall	0.93	0.81	0.87	0.89
F1-Score	0.91	0.84	0.88	0.88
Support	1242	758	-	2000
Accuracy	**0.8900**	-	-	-

CATABOOST RESULTS:

Metric	False (Legit)	True (Fraud)	Macro Avg	Weighted Avg
Precision	0.88	0.92	0.90	0.90
Recall	0.96	0.79	0.87	0.89
F1-Score	0.92	0.85	0.88	0.89
Support	1242	758	-	2000
Accuracy	**0.8935**	-	-	-

LIGHT BGM RESULTS:

Metric	False (Legit)	True (Fraud)	Macro Avg	Weighted Avg
Precision	0.88	0.92	0.90	0.90
Recall	0.96	0.79	0.87	0.89
F1-Score	0.92	0.85	0.88	0.89
Support	1242	758	-	2000
Accuracy	**0.8935**	-	-	-

With the highest recall for fraudulent transactions (79%), Random Forest outperformed all other models in identifying the majority of fraud incidents while reducing false negatives. Nevertheless, alternative models with marginally lower recall values, such as Gradient Boosting and XGBoost, also shown dependable detection skills. Because it performed the worst, logistic regression is not appropriate for situations involving high stakes fraud detection. Because of their capacity to successfully capture intricate transaction patterns, ensemble-based models like as Random Forest, Gradient Boosting, and LightGBM ultimately turned out to be the best options for fraud detection in UPI transactions.

VII CONCLUSION

Using a variety of machine learning models, this study successfully created a fraud detection system for UPI transactions. With an accuracy of 90.75%, Random Forest proved to be the most successful model. Strong performance was also shown by ensemble learning models like Gradient Boosting, LightGBM, and XGBoost, which made them suitable substitutes for fraud detection. The findings demonstrate how crucial precision and recall balance are to reducing false negatives and correctly detecting fraudulent transactions. To increase detection accuracy and flexibility to changing fraud trends, future improvements might incorporate deep learning techniques, real-time fraud detection, and adaptive learning processes.

VIII . REFERENCES

International Journal of Engineering Research & Technology, vol. 12, no. 3, May 2024, doi: 10.17577/IJERTCONV12IS03071.
[1] Rani, R., Alam, A., & Javed, A., "Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions," 2024 2nd International Conference on Disruptive Technologies (ICDT), pp. 924-928, 2024.Google Scholar

[2] Nagaraju, M., "Detection of Fraudulent Activities in Unified Payments Interface using Machine Learning-LSTM Networks," 2024 International Conference on Circuit Power and Computing Technologies (ICCPCT), 2024.Google Scholar

[3] Melam Nagaraju, V.C., Reddy, Y.C., & Babu, P.N., "UPI Fraud Detection Using Convolutional Neural Networks (CNN)," 2024. Google Scholar

[4] Tressa, N., Asha, V., Padanoor, S., Tabassum, R., Dharmesh, D.V., & Saju, B., "Credit Card Fraud Detection Using Machine Learning," 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), pp. 1-6, 2023.Google Scholar

[5] Ramachandran, K., "Unified Payments Interface (UPI): Transformation of Digital Payment Systems in India," International Journal of Core Engineering & Management, vol. 5, no. 4, pp. 42-48, 2018.Google Scholar

[6] Ramachandran, K., "Implementing Dynamic Risk Scoring Models for Adaptive Fraud Prevention," European Journal of Advances in Engineering and Technology, vol. 11, no. 5, pp. 33-40, 2024.Google Scholar

[7] Sabbani, G., "AI in Credit Card Fraud Detection: Innovations and Future Directions," North American Journal of Engineering Research, vol. 4, no. 1, 2023.Google Scholar

[8] Sabbani, G., "Unified Payments Interface (UPI) – Digital Future of India," European Journal of Advances in Engineering and Technology, vol. 10, no. 11, 2023.Google Scholar

[9] Devi, K., & Indoria, D., "An Analysis on the Consumers Perception Towards UPI (Unified Payments Interface)," International Journal of Aquatic Science, vol. 12, no. 2, pp. 1967-1976, 2021.Google Scholar

[10] Mubarokah, L., Rahmawati, N., & Rizky, R.M., "QR Code-Based Payments Among UPI Management Students Class of 2022: Exploration of Perceptions, Attitudes, and Adoption Intentions," Neraca: Jurnal Ekonomi, Manajemen dan Akuntansi, vol. 2, no. 12, pp. 512-520, 2024.Google Scholar

[11] Dahiphale, D., Madiraju, N., Lin, J., Karve, R., Agrawal, M., Modwal, A., Balakrishnan, R., Shah, S., Kaushal, G., Mandawat, P., Hariramani, P., & Merchant, A., "Enhancing Trust and Safety in Digital Payments: An LLM-Powered Approach," arXiv preprint arXiv:2410.19845, 2024. arXiv

[12] "Data Analysis for Fraud Detection," Wikipedia, 2024. Wikipedia+1Google Scholar+1

[13] Rani, R., Yogi, K.K., & Yadav, S.P., "Tech Innovations & Dataset Analysis to Combat Fake Accounts in Digital Communities," 2024 2nd International Conference on Disruptive Technologies (ICDT), pp. 1679-1684, 2024.Google Scholar

[14] Varshney, S., Rani, R., Gaur, T., & Choudhary, S., "Activity Based Travel Demanding Model Using Apache Kafka and Spark," 2024 2nd International Conference on Disruptive Technologies (ICDT), pp. 1154-1161, 2024.Google Scholar

[15] Rani, R., Yogi, K.K., & Yadav, S.P., "Subjective Evaluation of Clone Attack Detection Using Machine Learning Approach," Transdisciplinary Research and Education Center for Green Technologies, 2024.Google Scholar

[16] Rani, R., Chakraborty, S., & Singh, P., "Oddity Based Botnet Recognition Utilizing AI Model in the Internet of Things Framework," 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2023. Google Scholar

[17] Rani, R., Bisht, D., & Mittal, D., "Driver Snoozing System with Infrared Technology," 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS), 2023.Google Scholar

[18] Jyoti, A., Mishra, R., Rani, R., & Kalra, R., "E-voting Using Blockchain Technology," Advances in Computational Intelligence and Communication Technology, 2022.Google Scholar

[19] Wadkar, P.N., YES's, I., Misal, S., & Mundhe, S., "Analysis of Breast Cancer Dataset and Its Prediction Using Machine Learning," Editorial Board, vol. 15, 2022.Google Scholar

[20] Wadkar, P., & Mundhe, S., "Exploring the Effectiveness of Different Machine Learning Algorithms in Credit Card Fraud Detection: A Comparative Study," Sustainable Smart Technology Businesses in Global Economies, pp. 558-567, 2014.Google Scholar