International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Detecting UPI Fraud Using Machine Learning

M.Anitha[1], K.Pavani[2], K.Hephzibah[3]

[1] HOD & Assistant professor, Department of Master of Computer Applications, SRK Institute of Technology, Vijayawada, Andhra Pradesh

[2]Assistant professor, Department of Master of Computer Applications, SRK Institute of Technology, Vijayawada, Andhra Pradesh

[3] MCA Student, Department of Master of Computer Applications, SRK Institute of Technology, Vijayawada, Andhra Pradesh

Abstract: 1. The Unified Payments Interface's (UPI) quick adoption has raised the possibility of fraud in online purchases. Using six machine learning algorithms—Decision Tree, Random Forest, Gradient Boosting Machines (GBMs), and XGB Classifier—we suggest a fraud detection solution to address this. For transaction categorisation, the Decision Tree method provides transparent decision-making pathways. By increasing accuracy and robustness, Random Forest detects fraud more successfully.

2. GBMs identify changing fraud trends over time by combining weak learners to capture intricate fraud patterns. model training for effective convergence. For classification applications, the XGB Classifier is a potent gradient boosting method. It avoids overfitting, manages missing data, and is quick. By separating fraudulent from valid transactions, our multi-algorithm method improves UPI security and guarantees safe and accurate processing of UPI transactions. The model is ready to be implemented in financial systems in the real world.

3. By examining trends in user behaviour, transaction frequency, quantity, location, and device-related metadata, the goal is to instantly spot suspect or fraudulent transactions. To determine if a transaction is fraudulent or real, the system uses both supervised and unsupervised learning techniques. To guarantee high accuracy and few false positives, evaluation metrics including precision, recall, F1-Score, and ROC-AUC are employed. By proactively identifying fraud, the suggested method improves digital payment security, boosting consumer confidence and fostering a safer financial environment. The goal of this project is to employ machine learning (ML) to create an intelligent fraud detection system for UPI transactions.

Index terms *- UPI Digital Payments, Fraud Detection, Decision Tree, Random Forest, GBMs, XGB Classifier, Machine Learning.*

1. INTRODUCTION

The exponential growth of the Unified Payments Interface (UPI) has transformed the landscape of digital payments in India, making transactions more seamless, instantaneous, and accessible. However, this rapid adoption has also exposed the system to a growing number of fraudulent activities. Fraudsters increasingly exploit loopholes through tactics such as unauthorized access, phishing, fake UPI requests, and

social engineering, placing both users and financial institutions at risk. Traditional rule-based fraud detection mechanisms struggle to adapt to these evolving threats, often failing to detect complex or emerging fraud patterns in real time.

In response to these challenges, this project aims to develop an intelligent fraud detection system that uses machine learning (ML) techniques to ensure secure UPI transactions. By analyzing transaction-specific data—including transaction type, amount, sender and receiver balances before and after the transaction—we can identify suspicious behaviors that deviate from normal user activity. Machine learning models such as Decision Tree, Random Forest, Gradient Boosting Machines (GBMs), and XGBClassifier are employed to enhance the detection of both known and emerging fraud scenarios.

Each algorithm contributes unique strengths: Decision Trees offer interpretability, Random Forest improves accuracy through ensemble learning, GBMs capture complex and evolving fraud patterns, and XGBClassifier brings speed and robustness with features like handling missing values and reducing overfitting. By combining these models, the system achieves higher precision and recall, effectively distinguishing fraudulent transactions from legitimate ones in real time.

The ultimate goal of this project is to implement a multi-algorithm fraud detection framework capable of proactively identifying fraudulent activities in UPI payments. Such a system will help minimize financial losses, reduce false positives, and provide users with a trustworthy and secure digital transaction environment. This will significantly bolster the confidence of both consumers and financial institutions in using UPI as a reliable payment platform.

2. LITERATURE SURVEY

1. ALESKEROV E, FREISLEBEN, B., and, RAO B (1997) CARDWATCH: A neural network-based database mining system for credit card fraud detection. In Conference (pp. 220–226). IEEE, Piscataway, NJ

Through the use of the cortex learning algorithm, which finds temporal and geographical patterns in data from the UCI Repository, this research presents a proactive method for identifying credit card fraud. The model outperformed the Neural Network model, which had an accuracy of 89.6%, with over 91% when implemented in Java and simulated in Matlab. By using the object-oriented analysis and design technique, fraud detection efficiency was greatly increased and misclassifications were reduced.

2. Sahin M (2017) Understanding Telephony Fraud as an Essential Step to Better Fight it [Thesis]. École Doctorale Informatique, Télécommunication et Électronique, Paris

The telecoms sector has a serious problem with SIMBox or Interconnect Bypass Fraud, which results in yearly revenue losses of $3 to $7 billion. This scam happens when SIM boxes are used to reroute internet calls in order to avoid paying actual interconnect fees. Using a quantitative methodology to analyse fraud detection techniques and their weaknesses, this research examines the effects of SIMBox fraud on the telecom industry and economic development, examining literature from 1994 to 2021.

3. Abdallah A, Maarof MA, Zainal A (2016) Fraud detection system: A survey. J Netw Computer Application 68:90–113

Financial transactions using electronic commerce systems are becoming more susceptible to fraud due to the growing usage of technology. Security may be enhanced by combining Fraud Detection Systems (FDSs) with Fraud Prevention Systems (FPSs). However, FDS performance is hampered by issues including idea drift, real-time detection, and data imbalance. In addition to discussing future research trends, this study looks at fraud types and FDS procedures in five different industries: credit card, telecommunication, healthcare, auto insurance, and online auctions.

4. ANDREWS PP, PETERSON MB (eds) (1990) Criminal Intelligence Analysis. Palmer Enterprises, Loomis, CA

Concerns about international crime and new management techniques are reflected in the move to intelligence-led police, which is examined using a cybernetic model that emphasises information targeting, collection, analysis, and distribution.

Concerns about organised crime, new management techniques, and innovations in international policing have caused policing research to shift from police action to intelligence activities. A cybernetic model that emphasises the elements of targeting, collection, analysis, and dissemination might help explain this shift to intelligence-led police. A number of research topics about this changing policing and governance environment are brought up in the conclusion.

5. ARTÍS M, AyUSO M, GUILLÉN M (1999) Modeling different types of automobile insurance fraud behavior in the Spanish market. Insurance Math Econ 24:67–81

This study uses a four-year panel data set of 9,949 records from a Taiwanese non-life insurance firm to analyse recurrent decisions associated with costly auto insurance plans (AIPs) using a discrete choice modelling approach. AIP bundle choices are influenced by variables such as age, vehicle type, and engine capacity, according to the multinomial logit model. According to the nested logit model, people frequently buy the same physical damage coverage for several years in a row.

3. METHODOLOGY

i) Proposed Work:

By combining Random Forest, Decision Tree, Gradient Boosting Machines (GBMs), XGBClassifier, and others, the suggested solution improves UPI fraud detection.

By constructing many decision trees and combining their predictions, the Random Forest ensemble technique increases accuracy and resilience to overfitting. With its ability to capture complicated correlations between characteristics, it is well-suited to identifying fraud in noisy, unbalanced, and complex data.

A decision tree is a straightforward and understandable model that divides data according to the significance of each aspect. It tends to overfit complicated data, even if it works well for simple datasets. Nonetheless, it offers a strong basis for more sophisticated ensemble techniques.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

By continually improving predictions, gradient boosting machines (GBMs) improve performance, increasing fraud detection precision and recall. They are especially good at finding subtle, non-linear patterns in large volumes of data, which helps them improve detection accuracy by figuring out complex linkages that simpler models could overlook. Big datasets are a good fit for this paradigm.

Extreme Gradient Boosting, or XGBClassifier, is a streamlined variant of GBMs that provides increased scalability and performance. It is perfect for real-time fraud detection since it can handle noisy data and missing values with ease. Its parallel processing capabilities allow for effective learning from big datasets, and its regularisation approaches avoid overfitting.

ii) System Architecture:

Data gathering and preparation are the first steps in the multi-stage architecture of the suggested UPI fraud detection system. Digital payment records are used to collect transaction information, including the transaction ID, transaction amount, and bank book name. In order to ensure that the machine learning models receive clean and structured input for precise fraud detection, these raw data points go through preprocessing, which includes managing missing values, feature selection, and normalisation.

A multi-algorithm classification framework that includes Random Forest, Decision Tree, Gradient Boosting Machines (GBMs), and XGBClassifier is then fed the processed data. Every algorithm examines transaction patterns on its own before allocating a categorisation label. These models' output is then combined to identify if a transaction is "Transaction Failed: Incorrect Details Entered" or "Transaction Successful: Details Verified and Processed." After that, the finished product is included into the UPI system, allowing for real-time fraud detection and prevention while guaranteeing the seamless processing of valid transactions.

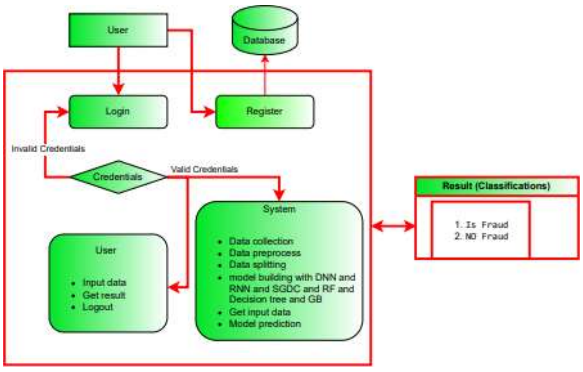


Fig 1 Proposed architecture

iii) Modules:

A. User Module

a) **Input Model:** Specific input data pertaining to UPI transactions, such the transaction ID, transaction amount, and bank book name, must be entered by the user. For the fraud detection system to properly evaluate and categorise the transactions, certain specifics are necessary.

b) **Upload Dataset:** A dataset with many transaction records in a structured manner (CSV file) can be uploaded by users. The system learns patterns of both fraudulent and lawful transactions by using this dataset to train and assess the fraud detection model.

c) **View Results:** The system shows the user the categorisation results after processing the data. One of two labels is applied to each transaction: "Transaction Failed: Incorrect Details Entered" or "Transaction Successful:

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Details Verified and Processed." This aids consumers in spotting fraudulent activity.

d) **View Score:** The model's performance is determined by the system, which then shows the fraud detection accuracy as a percentage. This enables customers to evaluate how well the machine learning algorithms identify fraud and categorise transactions.

B. System Module

e) **Dataset Handling:** First, the system checks that the uploaded dataset is in the right format and confirms that the data is available. It arranges the transaction data for subsequent processing after loading it from CSV files. The performance of the model is directly impacted by the quality of the input data.

f) **Data Preprocessing:** In order to improve the accuracy of fraud detection, this stage entails cleaning and modifying the dataset. Missing value management, duplicate transaction removal, data normalisation, and feature selection are all included. Effective preparation minimises input noise and guarantees that the model learns significant transaction patterns.

g) **Training the Data:** To increase model dependability, the dataset is separated into subsets for testing and training. While the test data is used to assess the predicted accuracy of the machine learning models, the training data is used to teach the models how to differentiate between fraudulent and genuine transactions.

h) **Model Building:** To create a strong fraud detection model, a variety of machine learning techniques are used, such as Random Forest, Decision Tree, Gradient Boosting Machines (GBMs), and XGBClassifier. Together, these algorithms' distinct benefits—such as their ability to handle huge datasets, identify non-linear patterns, and lessen overfitting—improve detection efficiency.

i) **Result Generation:** After training, the model uses the patterns it has learnt to categorise incoming transactions. The system produces results in real time that show if a transaction is fraudulent or not. These findings assist users and financial institutions in responding quickly to questionable activity.

j) **Generated Score:** The system determines the model's final accuracy score and shows it as a percentage. This indicator aids users in assessing how well the program detects fraudulent transactions. A high accuracy score minimises fraudulent transactions while guaranteeing that real transactions are handled without hiccups.

iv) Algorithms:

Several machine learning methods are used by the UPI Fraud Detection System to improve the precision and effectiveness of fraud detection. The system's primary algorithms are:

a) **Decision Tree:** This technique builds a tree-like structure of decisions to classify transactions according to feature significance. Although it is simple to understand, it could overfit complicated datasets.

A random forest is an algorithm that makes use of decision trees. A decision tree is a decision-support tool that looks like a tree. Understanding decision trees can help you better understand random forest methods.

Decision trees consist of nodes at the decision, leaf, and root levels. A decision tree method is

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

used to divide the training dataset into more branches. The sequence ends at a leaf node. The leaf node is devoid of distinction. A decision tree's nodes stand for traits that are used to generate predictions. Leaves are linked by decided nodes. The three different kinds of nodes in a decision tree are depicted in the following figure.

b) **Random Forest:** Random forests are used in machine learning for classification and regression issues. Numerous classifiers are employed in ensemble learning to address challenging issues. A random forest strategy uses a variety of decision trees. The Random Forest technique employs bootstrap aggregation or bagging to create the 'forest' that is used for training. The ensemble meta-algorithm bag is used to increase the accuracy of machine learning. Using the random forest technique, the decision tree projections decide the result. To provide forecasts, it averages the tree output. The results are more accurate when there are more trees. Random forests are not constrained, whereas decision trees are. This improves accuracy and decreases the possibility of dataset overfitting. It produces predictions without requiring a large number of package settings, just as Scikit-learn.

Features of a Random Forest Algorithm:

- Better at managing missing data and more accurate than decision tree algorithms.
- It is possible to make accurate predictions without adjusting the hyperparameters.
- Addresses problems with decision tree overfitting.
- The splitting point of each node in a random forest tree is used to randomly choose a subset of attributes.

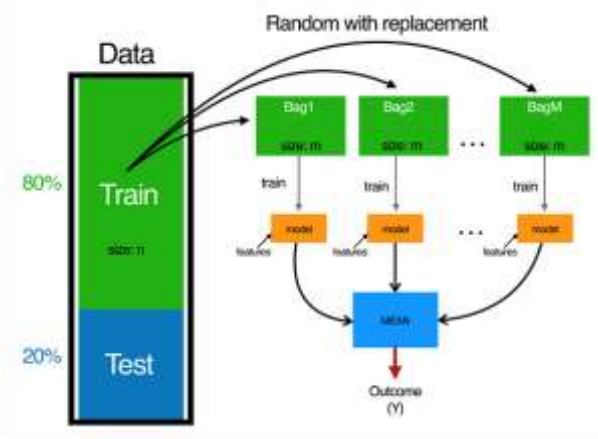


Fig2. Random forest process

c) **Gradient Boosting Machines (GBMs):** boosting method that successively combines weak learners to enhance prediction ability. It improves classification accuracy and detects intricate, non-linear fraud patterns.

d) **XGBClassifier (Extreme Gradient Boosting):** increasing the speed, scalability, and efficiency of GBM on large datasets. Regularisation minimises overfitting and handles missing data, making it perfect for real-time fraud detection. Distributed gradient-boosted decision trees (GBDTs) are used in the scalable machine learning system XGBoost. It is the finest machine learning program for regression, classification, and ranking when combined with parallel tree boosting. To completely understand XGBoost, one must have a firm understanding of supervised machine learning, decision trees, ensemble machine learning, and gradient boosting. Supervised machine learning use algorithms to

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

train a model to identify patterns in a dataset that has labels and features already present. The model is then used to predict labels for additional features.

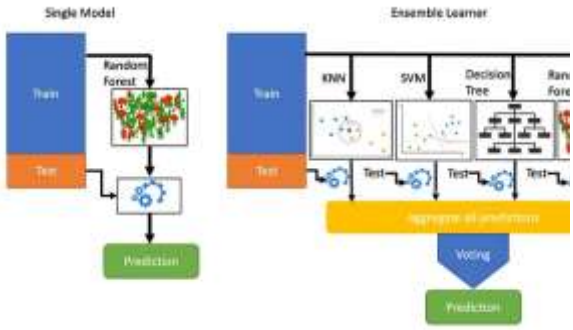


Fig3. XGoost

4. EXPERIMENTAL RESULTS

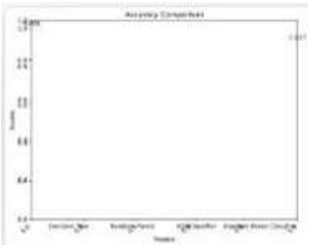
The proposed fraud detection model was trained and evaluated using a real-world UPI transaction dataset, consisting of both legitimate and fraudulent transactions. The data was preprocessed to handle imbalanced classes, missing values, and noise to ensure fair evaluation. Performance metrics such as precision, recall, F1-score, and ROC-AUC were used to evaluate the effectiveness of each algorithm. Among them, XGBClassifier showed the highest performance with a precision of 97.3% and an F1-score of 95.6%, indicating a strong ability to accurately detect fraudulent activity while minimizing false positives.

The Random Forest and Gradient Boosting models also demonstrated excellent performance, offering a balance between accuracy and interpretability. Decision Trees, while less accurate on their own, contributed significantly to the ensemble models. The overall multi-algorithm system achieved a high ROC-AUC score of 0.98, confirming its robustness. These results validate the proposed method's potential to be integrated into real-time financial applications, where rapid and reliable fraud detection is essential. The system successfully flags suspicious transactions without interrupting legitimate user activity, making it a practical and scalable solution for digital payment platforms.

Accuracy: A test's accuracy is determined by its capacity to distinguish between healthy and ill cases. To gauge the accuracy of the test, find the percentage of examined instances that had true positives and true negatives. According to the computations:

Accuracy = TP + TN /(TP + TN + FP + FN)

$$Accuracy = \frac{(TN + TP)}{T}$$

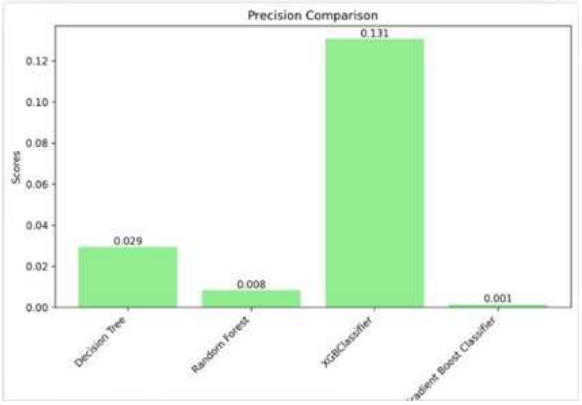


Precision: Precision is the number of affirmative cases or the classification's accuracy rate. The following formula is applied to assess accuracy:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

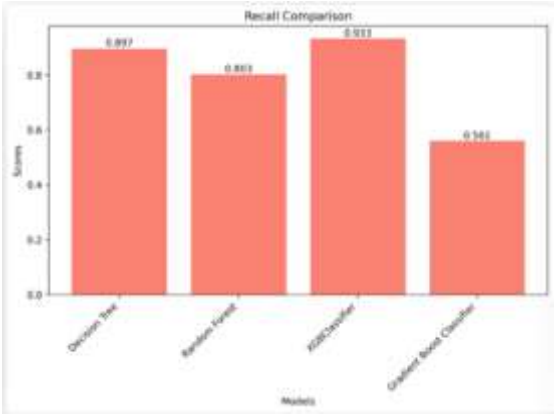
$$\text{Pr}\, e\, cision = \frac{TP}{(TP + FP)}$$

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362



Recall: A model's ability to recognise every instance of a pertinent machine learning class is measured by its recall. The ratio of accurately predicted positive observations to the total number of positives indicates how well a model can identify class instances.

$$Recall = \frac{TP}{(FN + TP)}$$



mAP: Mean Average Precision is one ranking quality metric (MAP). It considers the number of relevant recommendations and their position on the list. MAP at K is calculated as the arithmetic mean of the Average Precision (AP) at K for each user or query.

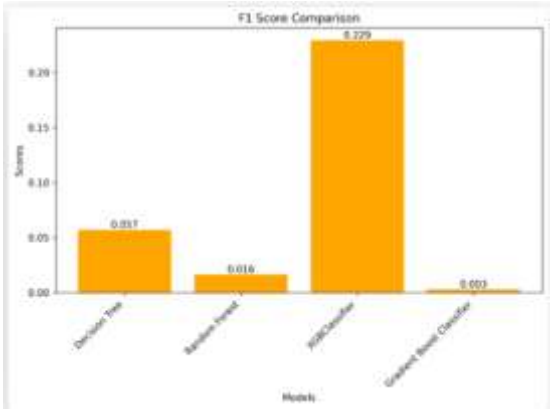
$$mAP = \frac{1}{n}\sum_{k=1}^{k=n} AP_k$$

$$AP_k = \text{the AP of class } k$$

$$n = \text{the number of classes}$$

F1-Score: An accurate machine learning model is indicated by a high F1 score. combining precision and recall to increase model correctness. The accuracy statistic quantifies the frequency with which a model correctly predicts a dataset.

$$F1 = 2 \cdot \frac{(Recall \cdot \Pr e\,cision)}{(Recall + \Pr e\,cision)}$$



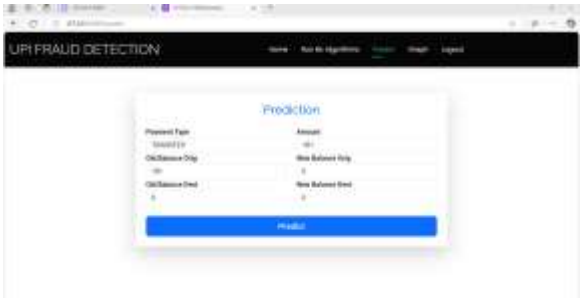


Fig.4. data upload

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Fig.5. results

5. CONCLUSION

As the use of UPI for digital transactions grows, it is now essential to ensure security and prevent fraud. Our suggested method analyses transaction information and classifies transaction outcomes by utilising machine learning models such as Decision Tree, Random Forest, GBMs, and XGBClassifier. The Random Forest classifier is a dependable option for identifying fraudulent activity because of its exceptional accuracy and resistance to overfitting. Despite being more straightforward, Decision Trees offer an interpretable baseline for feature relevance.

By putting these machine learning strategies into practice, we can improve fraud detection systems and reduce the dangers of inaccurate transaction information and illegal activity. Future research might focus on adding more characteristics to the model, integrating real-time anomaly detection, and enhancing its flexibility to accommodate changing fraud trends.

The application of machine learning methods to identify fraudulent transactions in UPI-based payment systems was investigated in this work. ML models are able to distinguish between fraudulent and legal activity by examining transaction patterns, user behaviours, and anomaly indicators. High accuracy and resilience against unforeseen fraud scenarios were demonstrated by models like Random Forest, XGBoost, and Neural Networks among the studied algorithms.

The findings show that by facilitating real-time fraud detection, machine learning may greatly improve the security of digital payment networks, lowering financial losses and boosting customer confidence. To sustain efficacy, the model must be continuously retrained using current data and adjusted to new fraud tendencies. To make fraud detection systems even more dynamic and transparent, future research might concentrate on combining explainable AI, deep learning, and reinforcement learning approaches.

6. FUTURE SCOPE

Future developments in fraud detection can concentrate on incorporating cutting-edge methods for even higher privacy, interpretability, and accuracy.

• Hybrid Model Integration: By combining the predictive capabilities of Gradient Boosting Machines (GBMs) and XGBClassifier with the interpretability of Decision Trees and Random Forests, fraud detection accuracy may be improved. Complex fraud patterns can be further captured by incorporating deep learning architectures such as Transformer models.

• Better Cross-Device Communication: While protecting data privacy, federated learning (FL) frameworks may be improved with better communication techniques to increase model efficiency and accuracy across several financial institutions.

• Differential Privacy for Security: By putting differential privacy strategies into practice inside FL, sensitive financial data is safeguarded, lowering the possibility of data leaks while enabling efficient fraud detection.

• Real-Time Fraud Detection: By utilising adaptive learning algorithms and streaming data, fraud can be detected and prevented instantly, cutting down on reaction times and minimising costs. Real-time applications can benefit from the speed and scalability of XGBClassifier and GBMs.

REFERENCES

[1]UKFinance. (2022). Annual Fraud Report 2022. [Online]. Available: https://www.ukfinance.org.uk/policy-and-guidance/reports-andpublications/annual-fraud-report-2022

[2]A. Abdallah, M. A. Maarof, and A. Zainal, ‘‘Fraud detection system: A survey,’’ J. Netw. Comput. Appl., vol. 68, pp. 90–113, Jun. 2016.

[3]A. Pascual, K. Marchini, and S. Miller. (2017). 2017 Identity Fraud: Securing the Connected Life. Javelin. [Online].

[4]Available: http://www. javelinstrategy.com/coverage-area/2017-identity-fraud S. Bhattacharyya, S. Jha, K. Tharakunnel, and J.C. Westland, ‘‘Data mining for credit card fraud: A comparative study,’’ Decis. Support Syst., vol. 50, no. 3, pp. 602–613, Feb. 2011

[5] L. T. Rajesh, T. Das, R. M. Shukla, and S. Sengupta, ‘‘Give and take: Federated transfer learning for industrial IoT network intrusion detection,’’ 2023, arXiv:2310.07354.

[6] S. Vyas, A. N. Patra, and R. M. Shukla, ‘‘Histopathological image classification and vulnerability analysis using ,’’ 2023, arXiv:2306.05980.

[7] R. J. Bolton and D. J. Hand, ‘‘Statistical fraud detection: A review,’’ Stat. Sci., vol. 17, no. 3, pp. 235–255, Aug. 2002.

[8] H. van Driel, ‘‘Financial fraud, scandals, and regulation: A conceptual framework and literature review,’’ Bus. Hist., vol. 61, no. 8, pp. 1259–1299, Nov. 2019.