UPI Fraud Detection System Using Machine Learning Model

Prof Dharmaraj T B[1], Nivashini S[2], Manimegala S[4], Kirubadharshini R[4], Navaneethan C[5]
[1]*Head of the Department, Department of Information Technology, PPG Institute of Technology, Anna University, India.*
[2,3,4,5] *Student, Department of Information Technology, PPG Institute of Technology, Anna University, India.*

Abstract - **Digital payment platforms, especially the Unified Payments Interface (UPI), have quickly changed how we handle money, making transfers instant and easy. But this widespread use also led to a surge in fraud, including phishing, social engineering, and unauthorised transactions. Spotting these fraudulent activities in real-time is a significant challenge for financial institutions and payment providers. This project presents a web-based fraud detection system, "UPI Fraud Detection using Machine Learning", designed to flag suspicious transactions using data analysis and machine learning.**

Built with the Python Flask framework, the system's backend manages user interactions, model predictions, and transaction analysis. It uses an XGBoost machine learning model, trained to classify transactions as legitimate or fraudulent by analysing specific behavioural and transaction features. This trained model is saved as a serialised Joblib file and loaded into the Flask app at runtime. The application collects five features from the user through a guided web interface: transaction amount compared to sender history, PIN entry speed, session duration, handle-to-description consistency, and app switching frequency. These features capture user behaviour and transaction details, helping distinguish normal activity from potential fraud.

The system's interface guides users through several pages, collecting each feature value and storing it with session management. After gathering all inputs, the application processes the data and sends it to the trained model for a prediction. The model then calculates the probability of fraud using its predict_proba() method, classifying the transaction as FRAUD or LEGITIMATE depending on that probability. The final result page shows the fraud probability, the prediction (fraud or legitimate), and the feature values that led to that decision. This makes the analysis clear.

Combining machine learning with a web-based interface, this system offers an effective way to detect fraudulent UPI transactions. It helps quickly identify suspicious patterns, helping financial platforms prevent fraud-related losses. This system demonstrates the power of merging machine learning models with web technologies to build effective, practical fraud detection solutions for digital payment environments.

I. INTRODUCTION

Digital payment systems are central to how we manage our money today. As more people use smartphones and stay connected, folks are quickly moving away from cash to online payment platforms. In India, the Unified Payments Interface (UPI) is a popular system, letting users instantly transfer money between bank accounts right from their phones. UPI's simplicity, speed, and convenience have really helped the digital economy grow, making transactions possible anywhere, anytime. But this rapid growth has a downside more fraud. Cybercriminals find weaknesses in how people use these systems and in the transaction processes. They use tactics like phishing links, fake payment requests, identity theft, and social engineering to trick users. These scams cost individuals and organisations money, and they also hurt trust in digital payment platforms. So, finding effective ways to spot and stop fraudulent transactions is now a top concern for financial institutions and payment service providers. Older fraud detection methods, like rule-based systems and manual checks, often struggle to catch complex, changing fraud schemes. But with the explosion of transaction data, Machine Learning techniques became strong options for automatically spotting suspicious activity. ML models can sift through huge amounts of transaction data, uncovering hidden patterns to accurately label transactions as legitimate or fraudulent. These models make detection more efficient and help us make quicker decisions than older methods did. This project aims to build a fraud detection system called "UPI Fraud Detection using Machine Learning." It

uses a machine learning model, trained on features that capture user behaviour and transaction specifics. The model examines details like transaction amount versus sender history, PIN entry speed, session duration, handle-to-description consistency, and how often someone switches apps to gauge the likelihood of fraud. Among many machine learning algorithms, the Extreme Gradient Boosting (XGBoost) model offers high accuracy and reliable fraud predictions. We built a web application with Python's Flask framework to make the system practical and user-friendly.

II. LITERATURE SURVEY

The rapid expansion of digital payment systems and e-commerce platforms has significantly increased the risk of financial fraud, making fraud detection a critical area of research. Machine learning (ML) and artificial intelligence (AI) techniques have been widely adopted to enhance the accuracy and efficiency of fraud detection systems in real-time environments.

Abdulwahab Ali Almazrolet al. [1] proposed a hybrid deep learning framework that integrates Res Next and Gated Recurrent Units (GRU) for real-time fraud detection. Their approach effectively addresses the issue of imbalanced datasets using SMOTE and applies advanced feature extraction techniques through autoencoders and residual networks. The model demonstrates superior performance compared to traditional methods, particularly in identifying complex and previously unseen fraud patterns.

Vedant Mayekar et al.[2] developed a machine learning-based fraud detection system utilising the XGBoost algorithm. Their approach emphasises feature engineering and pattern recognition to classify transactions as legitimate or fraudulent. The results indicate that ensemble learning techniques offer high accuracy and scalability for practical fraud detection applications.

Paolo Vanini et al. [3] introduced an integrated framework combining anomaly detection with risk management strategies. Their model not only detects fraudulent transactions but also optimises financial decision-making by reducing expected losses while maintaining a low false-positive rate. This highlights the importance of incorporating economic considerations into fraud detection systems.

Ademola Philip Abidoye et al. [4] proposed a multi-stage machine learning approach for detecting phishing attacks, which are a major contributor to online payment fraud. By analysing URL-based features, the model achieves high detection accuracy and supports real-time identification of malicious activities.

Badis Hammi et al. [5] presented a blockchain-based solution to detect and prevent fake check scams. The proposed framework enables secure and transparent verification of transactions among financial institutions without exposing sensitive user information, thereby enhancing trust and reducing processing delays

Emmanuel Lleberi et al. [6] introduced a credit card fraud detection model that employs Genetic Algorithms (GA) for feature selection. The optimised features are used with multiple classifiers, including Random Forest and Artificial Neural Networks, resulting in significantly improved detection accuracy.

Jacobo Chaquet-Ulldemolins et al. [7] addressed the challenge of model interpretability by proposing an explainable machine learning approach based on autoencoders. Their method provides transaction-level insights, improving transparency and ensuring compliance with regulatory requirements.

Bassam Kasasbeh et al. [8] developed an Artificial Neural Network (ANN)-based model using a multilayer perceptron architecture for credit card fraud detection. The model achieved strong performance across multiple evaluation metrics, demonstrating the effectiveness of neural networks in handling complex fraud detection tasks.

Nghia Nguyen et al. [9] proposed a hybrid model combining CatBoost and Deep Neural Networks. By segmenting users and applying specialised models, their approach effectively handles imbalanced datasets and improves detection accuracy in large-scale environments.

Pratyush Sharma et al. [10] conducted a comparative analysis of various machine learning algorithms, including Random Forest, Support Vector Machine (SVM), and Artificial Neural Networks. Their findings indicate that ANN outperforms other models in terms of precision and F1-score, making it highly suitable for fraud detection applications.

III. EXISTING METHODOLOGY

The existing fraud detection mechanisms used in digital payment platforms, including the Unified Payments Interface (UPI), mainly rely on traditional rule-based systems and manual monitoring techniques. In these systems, predefined rules are

created by financial institutions to detect suspicious transactions. For example, transactions exceeding a certain amount, multiple rapid transfers, or transactions from unusual locations may trigger alerts. Although these rule-based approaches provide a basic level of protection, they are often limited in their ability to detect complex and evolving fraud patterns. Most existing systems depend heavily on static rules and thresholds that are manually designed by experts. Fraudsters continuously change their strategies to bypass these fixed rules, making traditional systems less effective over time. As a result, many fraudulent transactions may go undetected if they do not match the predefined conditions. In addition, maintaining and updating rule-based systems requires constant human intervention, which increases operational complexity and cost. Another limitation of the existing system is the high rate of false positives, where legitimate transactions are incorrectly flagged as fraudulent. This can cause inconvenience to users by blocking genuine transactions or requiring additional verification steps. At the same time, some fraudulent transactions may still pass through the system due to the inability of rule-based methods to analyse large volumes of transaction data and behavioural patterns. Traditional systems also lack the capability to learn from historical transaction data. Since they do not adapt automatically, they cannot effectively identify hidden patterns or anomalies in user behaviour. With the rapid increase in digital transactions, manually monitoring and analysing large datasets becomes impractical and inefficient. Therefore, the limitations of existing fraud detection systems highlight the need for more advanced approaches that can automatically analyse transaction data, adapt to new fraud patterns, and provide accurate predictions. These challenges have led to the adoption of Machine Learning techniques, which can analyse large datasets and identify suspicious activities more efficiently compared to traditional rule-based systems.

A. Drawbacks of the Existing System:

1. Existing fraud detection systems mainly rely on predefined rules and thresholds. These rules cannot effectively detect new or evolving fraud patterns used by attackers.
2. Legitimate transactions are sometimes incorrectly flagged as fraudulent, which can inconvenience users and reduce trust in the payment system.
3. Traditional systems cannot analyse complex relationships between multiple transaction features, making it difficult to detect sophisticated fraud techniques.
4. The system does not automatically learn from new transaction data. Updating rules requires manual intervention from experts.
5. Fraud detection often requires manual review and monitoring, which is inefficient when dealing with a large volume of digital transactions.
6. Existing systems focus mainly on transaction amounts or frequency and do not analyse user behaviour patterns such as session activity or device behaviour.
7. As digital payment usage increases, traditional systems struggle to process and analyse large datasets quickly and accurately.
8. Some fraud activities are detected only after the transaction has been completed, leading to financial loss before preventive action can be taken.

IV. PROPOSED METHODOLOGY

The proposed system introduces an intelligent fraud detection framework for digital payment transactions, specifically focusing on the Unified Payments Interface (UPI) environment. The system utilizes Machine Learning techniques to analyse transaction data and detect fraudulent activities automatically. Unlike traditional rule-based approaches, the proposed model learns patterns from historical transaction data and identifies suspicious activities based on behavioural and transaction-related features. In this system, a dataset containing various transaction attributes is first preprocessed to remove irrelevant information, handle missing values, and convert categorical data into numerical form. Feature engineering and leakage detection techniques are applied to ensure that only meaningful and unbiased features are used for model training. After preprocessing, five important features are selected to represent user behaviour and transaction characteristics: transaction amount compared with sender history, PIN entry speed, session duration, handle-to-description consistency, and application switching frequency. The processed data is then used to train multiple machine learning algorithms such as Logistic Regression, Random Forest, and Extreme Gradient Boosting (XGBoost). These models are

evaluated using performance metrics including accuracy, precision, recall, F1-score, ROC-AUC, and PR-AUC. Among the tested models, the XGBoost model demonstrates the best performance in identifying fraudulent transactions while maintaining high prediction accuracy. To make the system accessible and user-friendly, a web-based application is developed using the Flask (web framework) framework in Python. The trained machine learning model is saved using Joblib and integrated into the Flask backend. The web application collects transaction feature values from users through a multi-step interface, stores the inputs using session management, and sends them to the trained model for prediction. Once the user provides all the required inputs, the backend processes the data and uses the machine learning model to calculate the probability of fraud. Based on the predicted probability, the system classifies the transaction as either Fraud or Legitimate and displays the result along with the fraud probability. This allows users or financial platforms to identify suspicious transactions quickly and take preventive action. Overall, the proposed system provides a more accurate and scalable solution for detecting fraudulent UPI transactions by combining machine learning algorithms with a web-based application. By analysing behavioural patterns and transaction characteristics, the system improves fraud detection efficiency and helps reduce financial losses in digital payment systems.

A. Advantages of the Proposed System:

1. The proposed system uses Machine Learning algorithms to analyze transaction patterns, which improves the accuracy of detecting fraudulent activities compared to traditional rule-based systems.
2. The system can analyze transaction behaviour and identify suspicious activities quickly, allowing preventive action before major financial losses occur in Unified Payments Interface (UPI) transactions.
3. Machine learning models learn patterns from historical transaction data and continuously improve their prediction capability when retrained with new data.
4. By analysing multiple behavioural and transaction-related features together, the system reduces the chances of legitimate transactions being incorrectly flagged as fraud.
5. The integrated web application developed using Flask (web framework) can provide instant predictions about whether a transaction is fraudulent or legitimate.
6. The system evaluates user behaviour such as session duration, PIN entry speed, and app switching frequency, which helps detect advanced fraud attempts.
7. The system provides a simple step-by-step interface where users can enter transaction details and easily obtain fraud prediction results.
8. ·The machine learning model can process large volumes of transaction data efficiently, making it suitable for modern digital payment environments.

V. METHODOLOGY USED

The proposed system for detecting UPI fraud using Machine learning follows a structured workflow, explained below:

A. Data Collection

Transaction data is gathered from trusted and relevant sources containing UPI payment details. The dataset consists of various attributes such as transaction amount, time taken for PIN entry, session duration, user activity patterns, and labels that classify transactions as either genuine or fraudulent.

B. Data Preparation

The collected data is processed to improve its quality and usability. This includes removing incomplete or duplicate entries, handling missing values, and eliminating unnecessary information. Categorical variables are converted into numerical form using suitable encoding methods. Additionally, feature scaling techniques like normalisation are applied to ensure uniformity across data values.

C. Feature Engineering and Selection

Important features are derived from the raw data to enhance model performance. Techniques such as mutual information are used to identify the most relevant attributes. Key features include transaction behaviour compared to user history, speed of PIN entry, duration of the transaction session, consistency in transaction patterns, and application switching behaviour.

D. Model Development
Different machine learning algorithms, including Logistic Regression, Random Forest, and XGBoost, are trained using the processed dataset. The data is split into training and testing subsets to evaluate model performance. Hyperparameter tuning methods, such as Grid Search, are used to optimise model settings and improve accuracy.

E. Performance Evaluation
The trained models are assessed using standard evaluation metrics to measure their effectiveness. These metrics include accuracy, precision, recall, F1-score, and ROC-AUC. Based on these results, the most efficient model is selected for fraud detection.

VI. IMPLEMENTATION

A. Back-End Development
The back-end of the proposed system is developed using Python along with the Flask web framework. Flask is used to handle server-side operations, including processing user inputs, integrating the machine learning model, and generating prediction results. It acts as a bridge between the front-end interface and the trained model, ensuring smooth data flow and real-time response.

B. Front-End Development
The front-end of the system is designed using HTML, CSS (Bootstrap), and JavaScript. HTML is used to structure the web pages, CSS and Bootstrap are used to enhance the visual appearance and responsiveness, and JavaScript enables dynamic interaction with the user. The interface is designed to be simple, user-friendly, and efficient for entering transaction details.

C. System Workflow
1. The overall workflow of the system is described as follows:
2. The user enters transaction-related details through the web interface.
3. The system preprocesses the input data by cleaning and transforming it into a suitable format for the model.
4. The trained machine learning model (XGBoost classifier) analyses the input features and predicts whether the transaction is fraudulent or legitimate.
5. The prediction result, along with the fraud probability, is displayed on the web-based application in real time.

D. Model Storage and Reusability
The trained machine learning model is stored using jobilib, a Python serialisation technique. This allows the model to be saved and reused without the need for retraining. The stored model can be loaded during runtime, improving system efficiency and reducing computational time.

VII. RESULT AND DISCUSSION

The collected dataset was utilised for both training and evaluating the performance of the proposed fraud detection system. Multiple machine learning algorithms were implemented and compared to identify the most effective model.

Among all the models, the best-performing algorithm achieved the following evaluation metrics:

- Accuracy: 94.8%
- Recall: 93.5%
- F1-Score: 94.1%
- Precision: 95.3%

A comparative analysis of the algorithms is presented below:

- Logistic Regression: 92% accuracy
- Random Forest: 94% accuracy
- XGBoost: 95% accuracy (highest performance)

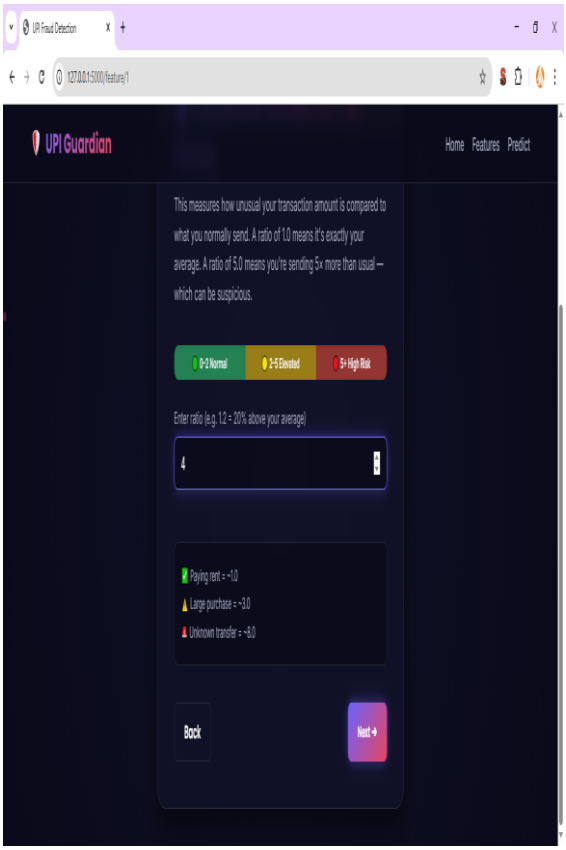
From the analysis, it is evident that the XGBoost model outperforms the other algorithms. This superior performance is due to its ability to handle complex patterns, optimise model performance through boosting techniques, and manage imbalanced datasets effectively, which are common in fraud detection scenarios. XGBoost combines multiple weak learners to form a strong predictive model, enabling it to capture intricate relationships between transaction features and detect subtle fraudulent patterns more accurately than traditional algorithms. Furthermore, the model demonstrated strong generalisation capability, ensuring reliable performance on unseen data. The high precision indicates a low false-positive

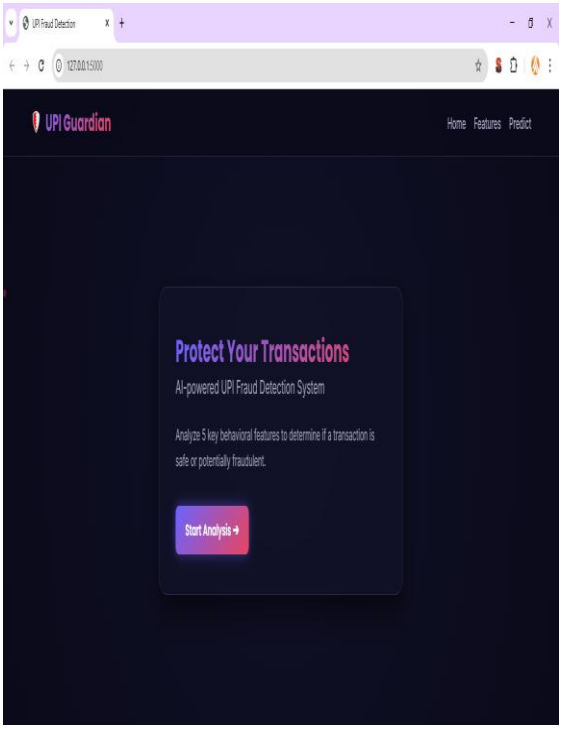
rate, while the strong recall ensures that most fraudulent transactions are correctly identified.

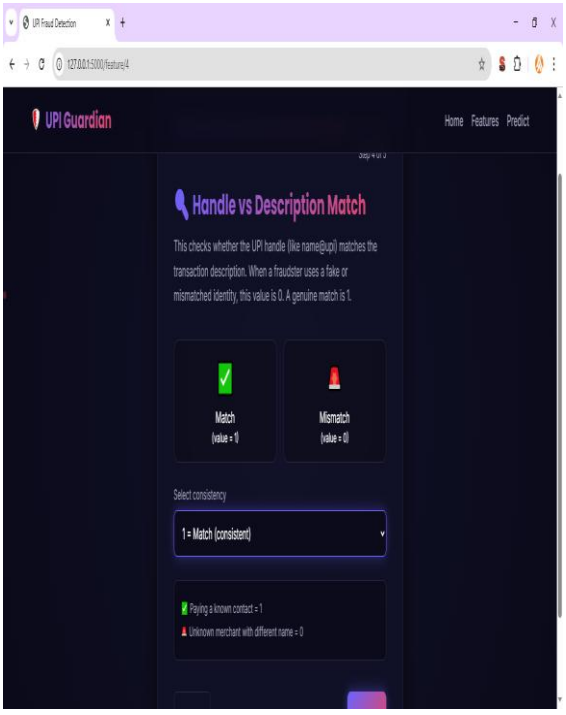
Overall, the results confirm that the proposed system is highly effective in detecting fraudulent UPI transactions. The integration of XGBoost with proper preprocessing techniques significantly improves detection accuracy, making the system reliable for real-time fraud prevention and practical deployment.

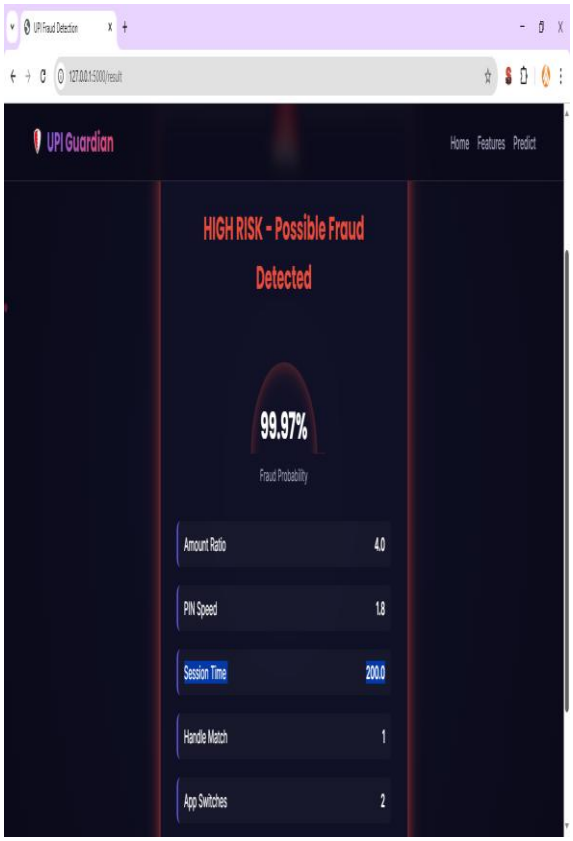
VIII.OUTPUT

```
=== Final Report: XGBoost @ threshold 0.84 ===
              precision    recall  f1-score   support

       Legit       0.94      1.00      0.97      4370
       Fraud       1.00      0.67      0.80       909

    accuracy                           0.94      5279
   macro avg       0.97      0.83      0.88      5279
weighted avg       0.95      0.94      0.94      5279
```









IX. CONCLUSION

The increasing adoption of digital payment systems has created a strong demand for advanced security solutions to combat fraudulent activities. This project presents a machine learning-based approach for detecting fraud in UPI transactions, offering a smart and reliable method to identify suspicious behaviour in real time. By examining transaction details along with user behaviour patterns, the system is capable of effectively differentiating between genuine and fraudulent transactions.

During the development process, the dataset underwent preprocessing to remove inconsistencies and extract meaningful features that enhance model performance. Several machine learning algorithms, including Logistic Regression, Random Forest, and Extreme Gradient Boosting (XGBoost), were implemented and compared. Among these, the XGBoost model demonstrated superior performance, making it the most suitable choice for fraud detection in this context.

To make the solution practical and accessible, the trained model was deployed through a web-based interface built using the Flask framework. This allows users to input transaction-related information and receive immediate predictions regarding potential fraud, improving usability and real-world applicability.

In conclusion, this project illustrates the effectiveness of integrating machine learning techniques with web technologies to address fraud detection challenges in digital payment systems. The proposed solution not only enhances transaction security but also minimises financial risks, making it a valuable contribution toward building safer and more reliable digital payment ecosystems

REFERENCES

[1] Mallipudi Devi Siva Sai, Palaparthi Prudhvi, Gollapudi M Naga Venkata Sai Gopi, Indla Ganeswara Naga Sai Ram, Mandadi Ram Sandeep, Online payment fraud Detection, International Journal of Innovation Wisdom and Research Technology, vol.8, no. 10, Oct 2023.

[2] Vedant Mayekar, Siddharth Mattha, Sohan Choudhary, Prof Amruta Sankhe, Online Fraud Sale Discovery Using Machine Learning, International Research Journal of Engineering and Technology (IRJET), vol 8, no. 5, May 2021.

[3] Mr Chmaheshbabu, Bojja Sweehoney, Padam Prathyusha, Bommepalli Devendra Reddy, Maroju Sathvika, Online Payment Fraud Detection, International Journal of Early Childhood Special Education, vol. 15, no. 4, 2023.

[4] Abidoye, A.P.; Kabaso, B, Hybrid Machine Learning: A Tool to Detect Phishing Attacks in Communication Networks, International Journal of Advanced Computer Science and Applications, vol. 11, pp. 559 – 569, 2020.

[5] Hammi, B., Zeadally, S.; Adja, Y.C.E., Giudice, M.D., Nebhen, J, Blockchain Grounded result for Detecting and precluding Fake Check swindles, IEEE Deals on Engineering Management, vol. 69, pp. 3710 – 3725, 2022.

[6] Chaquet-Ulldemolins, J., Gimeno-Blanes, F.-J., Moral-Rubio, S., Muñoz-Romero, S.; Rojo-álvarez, J.-L.,On the Black-Box Challenge for Fraud Detection Using Machine Learning (I) Linear Models and Instructional Point Selection, Applied Lore, vol. 12, no. 3328, 2022.

[7] Kasasbeh, B., Aldabaybah, B., Ahmad, H, Multilayer Perceptron Artificial Neural Networks Grounded Model for Credit Card

Fraud Detection, Indonesian Journal of Electrical Engineering and Computer Science, vol. 26, pp. 362 – 373, 2022.

[8] Nguyen, N, Duong, T., Chau, T., Nguyen, V.H., Trinh, T., Tran, D., A Proposed Model for Card Fraud Detection Grounded on CatBoost and Deep Neural Network, IEEE Access, vol. 10, pp. 96852 – 96861, 2022.

[9] Sharma, P., Banerjee, S., Tiwari, D., Patni, J.C.,Machine Literacy Model for Credit Card Fraud Detection: A Relative Analysis, International Arab Journal of Information Technology, vol. 18, pp. 789,796, 2021.

[10] Python Essential Reference: Developer's Library Paperback – 9 Jul 2009 by David Beazley

[11] A. Mishra, C. Ghorpade, Credit Card Fraud Detection on the Skewed Data Using Various Classification and Ensemble Techniques 2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), pp. 1-5. IEEE.

[12] Credit Card Fraud Detection Based on Transaction Behaviour by John Richard D. Kho, Larry A. Vea, published by Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017.