IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14215

A Detection Model for Suspicious Mobile Money Transactions

Jessica Predise Bai[1], Victor Thomas Emmah[2], Onate Egerton Taylor[3]

Department of Computer Science, Rivers State University, Port Harcourt, Nigeria[1,2,3]

Abstract: Suspicious transactions in mobile money systems have become a growing concern due to the increasing volume of digital transactions and the sophistication of fraudulent activities. Mobile money platforms, widely used for quick and secure financial transfers, are vulnerable to various types of fraud, such as identity theft, unauthorized access, and transaction manipulation. Detecting fraudulent transactions in real-time is a challenge due to the vast amounts of data and the dynamic nature of fraudulent behaviors. Existing systems often struggle with high false-positive rates or fail to catch advanced fraud patterns, leading to financial loss and security breaches. This paper proposes a secure model for mobile money applications, incorporating two layers of authentication that include passwords, One-Time Passwords (OTP), and a machine learning-based approach. Specifically, the Random Forest classifier is employed to accurately detect suspicious mobile money transactions. Results show that the system ensures a robust and scalable solution to efficiently identify fraudulent transactions with minimal user intervention, achieving 100% training accuracy and 99% testing accuracy, enhancing financial security. This innovation plays a crucial role in safeguarding mobile money platforms globally.

Keywords: Mobile money, One-Time Passwords, Random Forests, Suspicious Transactions

I. INTRODUCTION

Mobile money has become one of the primary methods of financial transactions, especially in developing countries where access to traditional banking services is limited. Services such as M-Pesa, Airtel Money, and MTN Mobile Money have made it easier for people to transfer, save, and withdraw money using their mobile phones. However, the ubiquity of mobile money services has also made them a target for fraudsters and criminals engaging in illegal activities, including money laundering and identity theft.Through mobile money, financial technologies (FinTechs) have revolutionized financial services in the fourth industrial revolution (4IR) in developed and developing countries, which arose as the prospective mobile payment platform.

[1] define mobile money as a service that requires the use of mobile phones to gain access to financial services by either dialing unstructured supplementary service data (USSD) codes or using mobile money applications. Today, mobile money subscribers perform mobile money services using a dedicated mobile money application installed on a smartphone or USSD, but the latter is frequently used [2]. Mobile money applications have become a critical part of financial systems, enabling users to perform transactions conveniently. However, with their growing usage, security vulnerabilities have emerged, particularly in the form of unauthorized access, fraudulent activities, and identity theft. Traditional authentication methods, such as passwords or PINs, are inadequate for ensuring the security of mobile transactions as they are prone to phishing attacks, password reuse, and interception.

Fraudsters often exploit weaknesses in these systems by initiating suspicious transactions from foreign locations or manipulating transaction amounts, leading to financial losses for both users and service providers. Additionally, the increasing sophistication of cyber-attacks demands more robust and adaptive authentication systems. Without effective security measures, users are left vulnerable to these threats, which erodes trust in mobile money platforms.

Given the challenges, there is a critical need for a secure authentication model that incorporates advanced machine learning techniques to detect suspicious transactions and mitigate fraudulent activities in real time. The challenge lies in developing a solution that not only strengthens authentication but also identifies and responds to fraudulent behaviour based on transactional data patterns, geographical anomalies, and user behaviours.

II. RELATED REVIEWS

Fraud detection in mobile money systems is a growing area of research that combines various machine learning, statistical, and anomaly detection techniques. The need for efficient fraud detection models is especially pressing given the rise in mobile payment applications, which provide both accessibility and convenience but also create opportunities for fraudsters.

[3] developed a secure multi-factor authentication (MFA) algorithm for mobile money applications. It uses personal identification numbers, one-time passwords, biometric fingerprints, and quick response codes to authenticate and authorize mobile money subscribers. Secure hash algorithm-256, Rivest-Shamir-Adleman encryption, and Fernet encryption were used to secure the authentication factors, confidential financial information and data before transmission to the remote databases. The results of the review grouped the threat models into attacks against privacy, authentication, confidentiality, integrity, and availability. The survey identified authentication attacks, identity theft, phishing attacks, and PIN sharing as the key mobile money systems' security issues.

[4] proposed a framework that combines multi-factor authentication and machine learning to increase the safety of online financial transactions. Their methodology is based on using two layers of security. The first layer incorporates two factors to authenticate users. The second layer utilizes a machine learning component, which is triggered when the system detects a potential fraud. This machine learning layer employs facial recognition as a decisive authentication factor for further protection. To build the machine learning model, four supervised classifiers were tested: logistic regression, decision trees, random forest, and naive Bayes. The results showed that the accuracy of each classifier was 97.938%, 97.881%, 96.717%, and 92.354%, respectively.

[5] proposed a secure Internet Financial transactions using Multifactor Authentication and Machine Learning which offers a unique system that integrates machine learning (ML) with multifactor authentication (MFA). Their system uses two levels of protection. The first layer uses two authentication factors, and the second layer is an embedded layer that asks for facial recognition from the user to successfully continue the purchase process if the ML model determines that the present transaction is fraudulent. To select the best classifier for constructing the ML model, four supervised ML classifiers were put into practice. After testing many classifiers, including Random Forest (RF), Decision Trees (DT), Logistic Regression (LR), and Naïve Bayes (NB), the accuracy of each was 96.717%, 97.881%, 97.938%, and 92.354%, respectively.

[6] proposed a system to predict mobile money transaction fraud using machine learning algorithms which aims to utilize machine learning classifiers to predict transactions flagged as a fraud in mobile money transfers. Logistic regression was used as the baseline model and compared with ensemble and gradient descent models. The results indicate that the logistic regression model still showed reasonable performance while not performing as well as the other models. Among all the measures, the random forest classifier exhibited outstanding performance because it achieved high precision (0.96), recall (0.80), and F1-score (0.87). The amount of money transferred emerged as the top feature for predicting money laundering transactions in mobile money transfers.

[7] analysed the security of the online banking system and proposed a new anomaly-based fraud detection method to overcome phishing and SIM swap fraud attacks. The login attributes like IP address, device, cookie, operating system, and browser were used to generate and update the user's profile. The primary user profile contains the most recently used login attributes, and the second profile contains the most frequently used login attributes. If the current login attributes match either the primary or secondary user profile, the user can access their account. Otherwise, additional security mechanisms like OTP with QR code or biometric authentication or both are used to identify the suspicious behavior of the user. Their proposed method reduces the login burden of the user and provides better security for the online mobile banking system.

[8] proposed an XGBoost-based fraud detection framework while considering the financial consequences of fraud detection systems. The framework was empirically validated on a large dataset of more than 6 million mobile transactions. To demonstrate the effectiveness of their proposed framework, they conducted a comparative evaluation of existing machine learning methods designed for modeling imbalanced data and outlier detection. The results suggest that in terms of standard classification measures, the proposed semi-supervised ensemble model integrating multiple unsupervised outlier detection algorithms and an XGBoost classifier achieves the best results, while the highest cost savings can be achieved by combining random under-sampling and XGBoost methods.

[9] used techniques such as SMOTE (Synthetic Minority Over-sampling Technique) to handle class imbalance in fraud detection tasks. Their study showed that SMOTE can create synthetic samples of the minority class, which in the case of fraud detection, is typically the fraudulent transactions. This helps balance the training dataset and improves the performance of machine learning models.

The rapid adoption of mobile money systems, especially in emerging markets, has resulted in new types of fraud. [10] conducted research on fraud detection in mobile payments, highlighting the challenges of mobile-specific threats such as device spoofing, SIM card fraud, and unauthorized access to mobile wallets. The authors proposed hybrid models combining rule-based and machine learning techniques, achieving promising results in detecting fraudulent mobile transactions.

DOI: 10.17148/IJARCCE.2025.14215

[11] introduced a feature-engineered machine learning-based model for detecting transaction fraud. By processing as much data as it can, the algorithm can gain experience, strengthen its stability, and increase its performance. The effort to detect online fraud transactions can use these algorithms. In their study, a dataset of specific online transactions was obtained. Then, with the aid of machine learning algorithms, unusual or distinctive data patterns that will be helpful in identifying any transactions that are fraudulent are discovered. The XGBoost algorithm is a cluster of decision trees, which was utilized in order to achieve the best outcomes. Comparing this approach to other ML algorithms reveals that it is faster and more accurate.

III. ANALYSIS OF THE PROPOSED SYSTEM

The proposed system operates by integrating machine learning algorithms with a robust user interface to detect and flag suspicious mobile money transactions in real-time. Initially, mobile money transaction data is collected, including critical attributes such as transaction amounts, user authentication status, transaction locations, and timestamps. The system employs the Random Forest classifier, trained on a balanced dataset using techniques like Synthetic Minority Oversampling Technique (SMOTE) to address class imbalance, ensuring that both normal and suspicious transactions are adequately represented. When a new transaction is initiated, the system automatically evaluates it against the trained model. It analyzes the transaction's features and determines the likelihood of it being fraudulent based on patterns learned during training. If a transaction is flagged as suspicious, it is highlighted for further investigation.

a. Architectural Design of the Proposed System

The proposed system architecture in Figure 1 shows the architecture of a suspicious mobile money detection System that involves several processes related to authentication, transaction initiation, and security monitoring. Each component plays a critical role in ensuring a secure and seamless transaction flow.

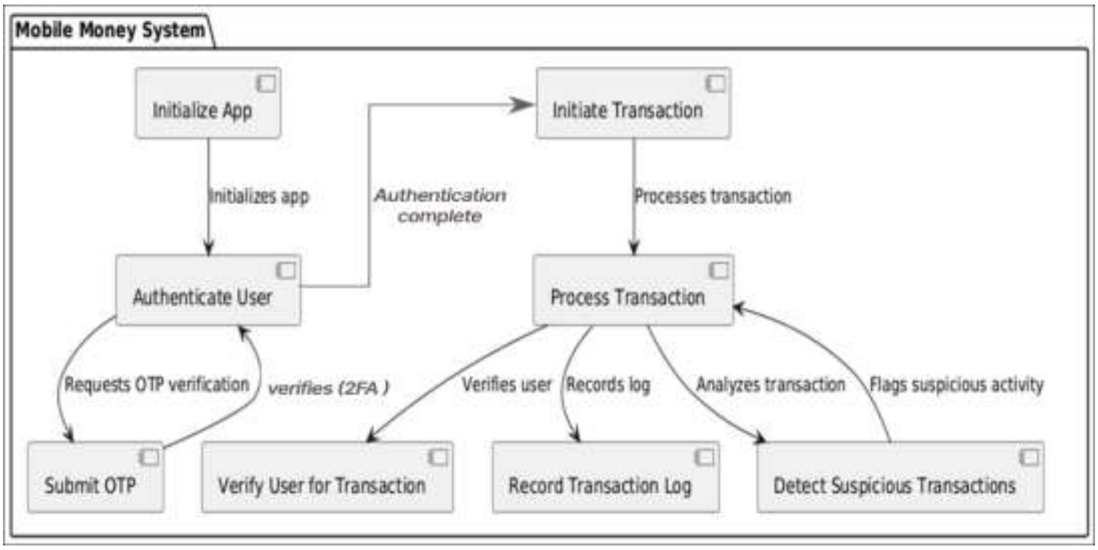


Fig. 1: Architecture of the Suspicious Mobile Money Dectection System

The components of the architecture is as follows:

1. Initialize App: This is the first step in the process, where the mobile money application is initialized. When a user launches the app, it sets up the necessary environment for further actions. This may include loading user settings, checking for app updates, and preparing the app for authentication or transaction activities.

2. Authenticate User: After initializing the app, the user needs to be authenticated to ensure secure access. The system requests OTP (One-Time Password) verification and leverages 2FA (Two-Factor Authentication) to verify the user's identity. Authentication usually involves:

Submit OTP: The user submits a one-time password sent to their registered mobile number or email address for validation.

i. **Verify User for Transaction**: This step checks if the OTP and other authentication factors (like biometric or password) match the information on file, ensuring the user is legitimate and authorized to initiate transactions.

3. Initiate Transaction: Once the user is authenticated, they can proceed to initiate a transaction. This step typically includes selecting the type of transaction (e.g., money transfer, bill payments), entering recipient details, and specifying the transaction amount. The system now prepares to process the transaction, validating the details provided.

4. Process Transaction: This is the core functionality of the mobile money system, where the transaction is executed. After verifying the user's credentials and ensuring the request aligns with system rules, the transaction proceeds. This step includes:

i. **Verify User**: Ensures that the authenticated user has the proper permissions and account balance to proceed with the transaction.
ii. **Record Transaction Log**: The system records all details related to the transaction (e.g., date, time, amount, and recipient) in a log. This serves as a reference for both the user and the system for audit purposes and for tracking transactions.
iii. **Detect Suspicious Transactions**: The system monitors transactions for any suspicious behaviour. This involves analysing transaction patterns and flagging potentially fraudulent activities. The system could raise alarms if a transaction appears anomalous, such as large transfers to unfamiliar accounts or transfers from a new location.

5. Submit OTP: As part of the user authentication process, this block is responsible for handling the input of the One-Time Password (OTP). After the system sends an OTP to the user's registered device, the user enters this code into the app, which the system checks against the sent code for verification. This adds an additional layer of security to the system.

6. Verify User for Transaction: In this step, the system confirms the user's identity, ensuring the two-factor authentication (2FA) mechanisms, such as biometric data, passwords, or OTP, match. If the user passes this verification, they are allowed to proceed to the transaction phase. This verification ensures that even if someone else gains access to the user's phone or credentials, the transaction cannot proceed without a correct OTP or other verification methods.

7. Record Transaction Log: This block plays a vital role in auditing and keeping a track of all system activities. Every transaction initiated and completed is recorded into a transaction log. The data logged includes transaction details such as date, time, amount, and any other relevant metadata. This log is essential for reviewing transaction history, auditing, and in case of disputes.

8. Detect Suspicious Transactions: An important security feature of the system, this block is responsible for identifying and flagging any unusual or potentially fraudulent activity. It continuously analyzes transactions against known patterns or rules and alerts the system or the user if something suspicious is detected. This may include large, unusual transactions, transfers to unknown or flagged accounts, or a series of rapid transactions in a short period.

9. Flag Suspicious Activity: In conjunction with the suspicious transaction detection process, this block flags the detected irregularities. If a transaction is marked as suspicious, it may trigger further actions such as blocking the transaction, notifying the user, or alerting the system administrators to take preventive measures.

Algorithm 1: Suspicious transactions detection Algorithm on mobile money

```
Start
Input: TransactionData (collection of mobile money transactions)
Output: Normal Transaction, Fraudulent Transaction
    1. Preprocess TransactionData to extract relevant features (e.g., TransactionID, Amount, Location, TimeOfDay,
       Authentication Status)
    2. Split the preprocessed data into training and testing datasets
    3. Initialize the RandomForestClassifier model for fraud detection
    4. Train the model using historical transaction data
    5. Set a threshold for fraud detection based on model output
    6. For each transaction in the test set:
            1. prediction = model.predict(transaction_features)
```

```
        2. If prediction == 1 (Fraudulent), flag the transaction for review
        3. Else, mark the transaction as normal
7. Return the result for each transaction:
        o If flagged, return "Fraudulent Transaction detected"
        o Else, return "Normal Transaction"
8. End
```

The algorithm works by analyzing mobile money transactions to identify potential fraudulent activities. Initially, the transaction data is preprocessed to extract key features such as transaction amount, location, time of day, and authentication status. The data is then split into training and testing sets, and a Random Forest classifier is trained on historical transaction data. The classifier learns patterns of normal and fraudulent behaviour during training. For each new transaction, the model predicts whether it is normal or fraudulent based on the learned patterns. Transactions flagged as fraudulent are highlighted for further review, while normal transactions proceed without interruption. The use of Random Forest ensures robust and accurate detection, leveraging its ability to handle complex decision-making through multiple decision trees.

b. Exploratory Data Analysis (EDA)

The Exploratory Data Analysis (EDA) process is a crucial first step in understanding the dataset for mobile money transactions. The dataset Paysim1 consists of 7,000 records with mobile money transactions which were generated with PaySim simulator. The simulation was based on a sample of real transactions gathered by a company who is the provider of the mobile financial service which is currently running in more than 14 countries all around the world. The data is a set of one-month financial logs from a mobile money service implemented in an African country. The mobile money transactions, each labelled as either "suspicious" or "normal" based on factors such as transaction amount, authentication status, and transaction location serve as the target variable, where 1 denotes a suspicious transaction, and 0 denotes a normal transaction. The primary goal of EDA is to uncover patterns in the data and to identify any potential issues before proceeding with model training.

i. Distribution of Suspicious vs. Normal Transactions

The first EDA step involved examining the distribution of suspicious and normal transactions as shown in Figure 2. A count plot was generated to visualize this distribution. From the plot, it is evident that suspicious transactions represent a minority of the total, indicating class imbalance in the dataset. This imbalance may affect the model's performance, as it may lead to the model predicting the majority class more frequently. To solve the problem of class imbalance, SMOTE technique was employed to balance the data. The distribution of the balance data can be seen in Figure 3

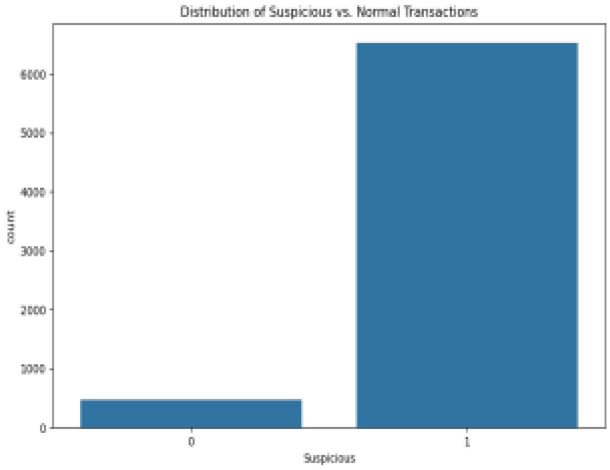


Fig. 2: Distribution of normal transactions vs suspicious transactions (Imbalanced data)

DOI: 10.17148/IJARCCE.2025.14215

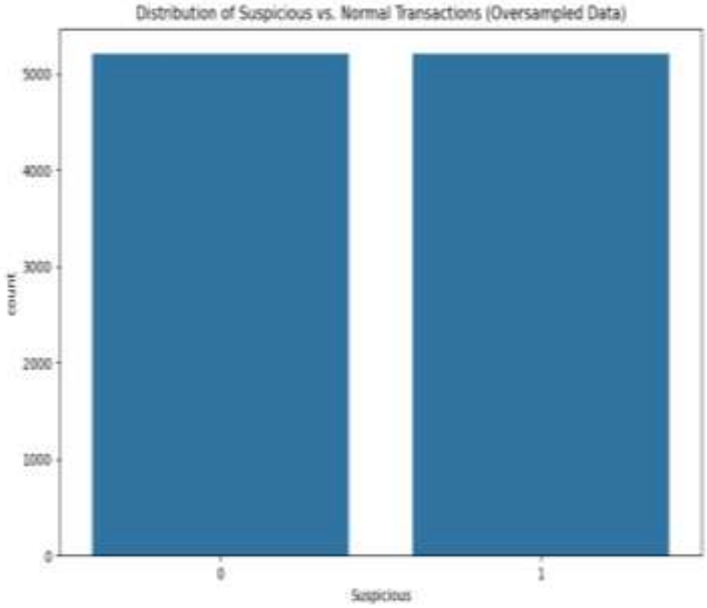


Fig. 3: Distribution of normal transactions vs suspicious transactions (Balanced data)

Transaction Amounts by Suspicious Label

A box plot (Figure 4) was generated to analyse the relationship between transaction amounts and the "suspicious" label. The box plot illustrates that suspicious transactions tend to involve higher amounts compared to normal transactions, though there is a wide range of amounts for both classes. This suggests that the transaction amount is a key feature for detecting suspicious behaviour.

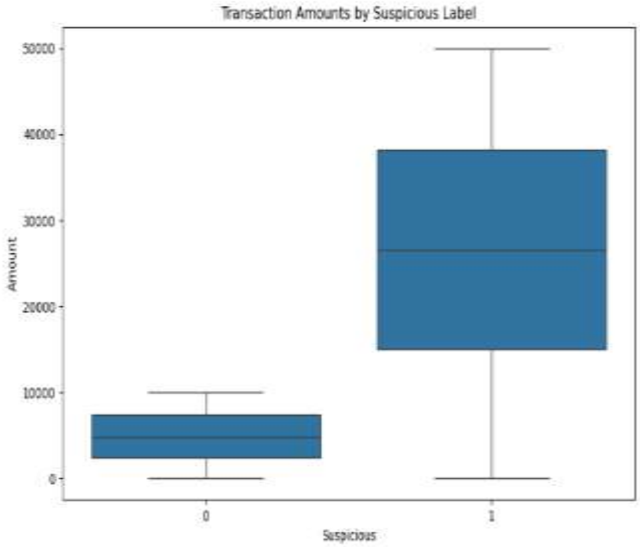


Fig. 4: Outlier detection using box plot

ii. Suspicious Transactions by Location

The locations where the transactions occurred were analyzed as shown in Figure 5. A count plot was created to display the number of suspicious and normal transactions based on the transaction location (i.e., whether it was in the user's common cities or a foreign city). The plot reveals that a higher proportion of suspicious transactions occur in foreign cities, reinforcing the idea that location is a significant indicator of potentially fraudulent activity.

DOI: 10.17148/IJARCCE.2025.14215

These visualizations provide key insights into the characteristics of suspicious transactions, which are essential for guiding the feature engineering and model training phases.

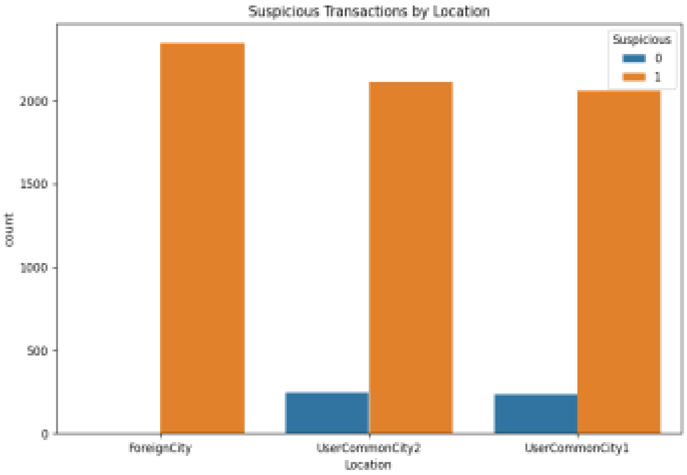


Fig. 5: Distribution of locations with highest number of suspicious mobile money transactions and normal transactions.

IV. MODEL TRAINING

After performing EDA, the next step was to train a machine learning model to detect suspicious mobile money transactions. The **Random Forest** algorithm was selected for this task due to its ability to handle both categorical and numerical data and its robustness in classification tasks.

a. Data Preparation

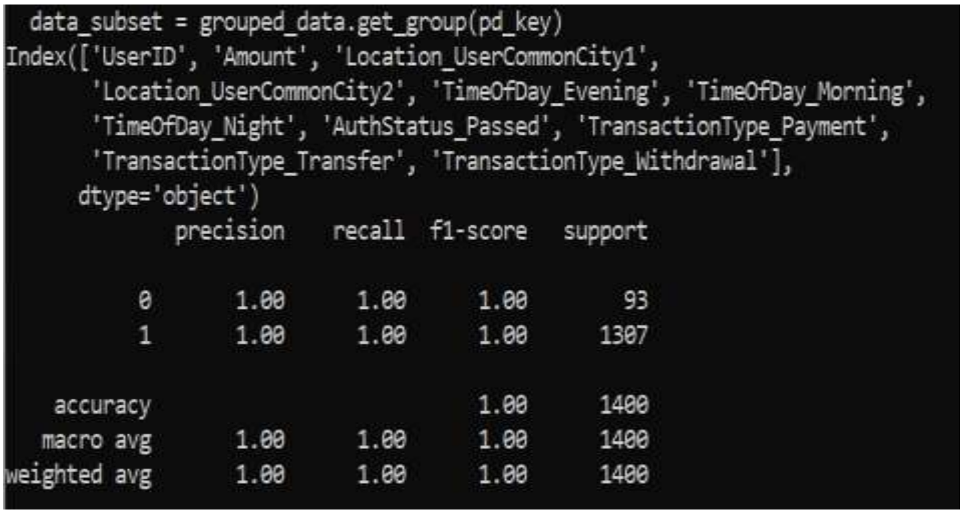
The data was first split into feature variables (X) and the target label (y). The features include UserID, Amount, Location, TimeOfDay, AuthStatus, and TransactionType, while the target variable, Suspicious, indicated whether a transaction was suspicious (1) or normal (0). Since the dataset contained categorical variables such as Location and AuthStatus, these were converted into numerical representations using one-hot encoding to ensure compatibility with the Random Forest model.

The dataset exhibited class imbalance, with suspicious transactions being underrepresented. To mitigate this, **SMOTE (Synthetic Minority Oversampling Technique)** was applied. SMOTE oversamples the minority class by generating synthetic samples, thus balancing the class distribution in the training dataset. This step is crucial to ensure the Random Forest model does not become biased toward the majority class (normal transactions).

b. Model Training

The Random Forest classifier was trained using the oversampled training dataset. A total of 100 decision trees were used (n_estimators=100), and the random_state was set to 42 to ensure reproducibility. The model was trained to learn patterns in the data, such as high transaction amounts, failed authentication statuses, and foreign locations, which are more likely to indicate suspicious activity. The performance of the trained Random Forest model was evaluated on the test set, which was not oversampled and represents the real-world data distribution. Two key evaluation metrics were used: The classification report in Figure 6 and Figure 7 shows that the model achieved a good balance between precision and recall for detecting suspicious transactions, indicating that the Random Forest classifier successfully learned the patterns associated with fraudulent behaviour in mobile money transactions. The accuracy score further confirms the model's ability to correctly classify transactions. The model was saved as a .pkl file using the joblib library, making it ready for future use in detecting suspicious transactions in real-world scenarios.

DOI: 10.17148/IJARCCE.2025.14215



```
  data_subset = grouped_data.get_group(pd_key)
Index(['UserID', 'Amount', 'Location_UserCommonCity1',
       'Location_UserCommonCity2', 'TimeOfDay_Evening', 'TimeOfDay_Morning',
       'TimeOfDay_Night', 'AuthStatus_Passed', 'TransactionType_Payment',
       'TransactionType_Transfer', 'TransactionType_Withdrawal'],
      dtype='object')
              precision    recall  f1-score   support

           0       1.00      1.00      1.00        93
           1       1.00      1.00      1.00      1307

    accuracy                           1.00      1400
   macro avg       1.00      1.00      1.00      1400
weighted avg       1.00      1.00      1.00      1400
```

Fig. 6: Classification of the Random Forest model on threats detection

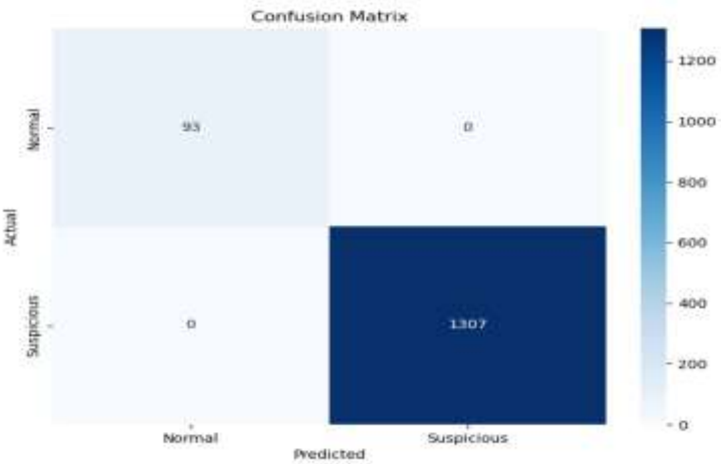
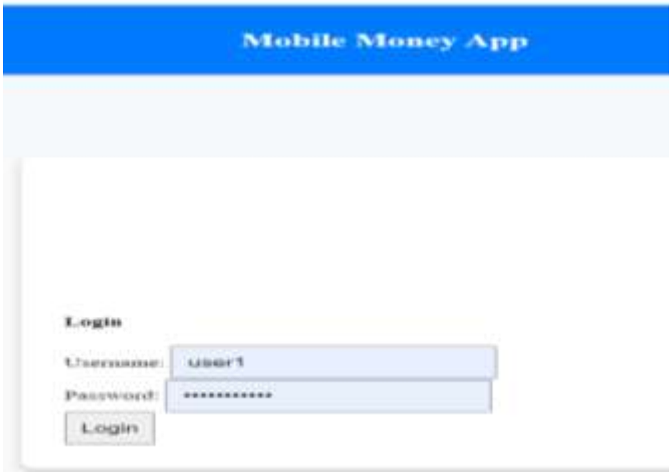


Fig. 7: Confusion matrix of the Random Forest model for threat detection on mobile transactions.

c. Deployment

The implementation of this HTML template creates a responsive dashboard for displaying mobile money transactions, incorporating Bootstrap for design and layout. The page features a sidebar navigation menu with links to different sections, such as Dashboard, Transactions, Reports, and Settings. The sidebar is designed to be hidden on smaller screens and toggled on and off using a button. The main content displays a table of transactions, where each transaction is dynamically generated using Flask’s templating language, showing details like Transaction ID, User ID, Amount, Location, and Status. A threat detection function (detect_threat) is used to highlight suspicious and normal transactions. The page adapts for mobile and desktop views using media queries, ensuring a smooth user experience on different devices. The deployed interface can be seen in Figures 8, 9 and 10.

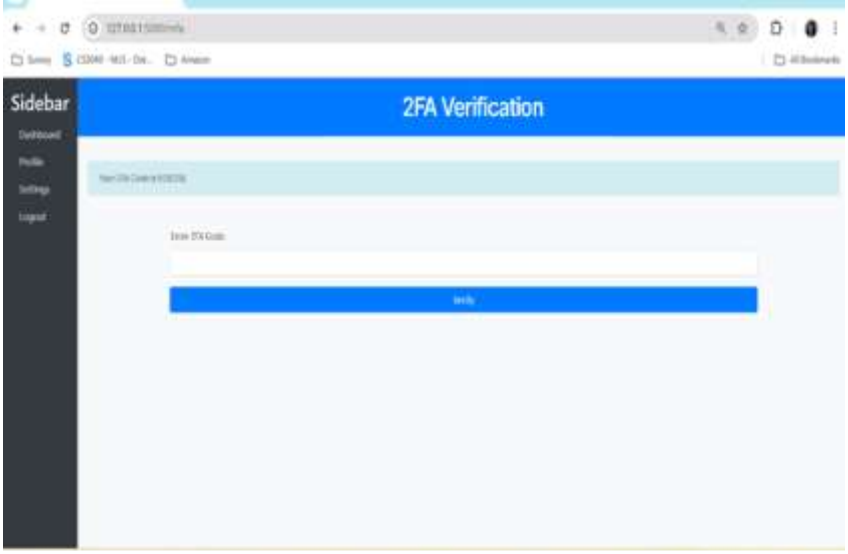
DOI: 10.17148/IJARCCE.2025.14215



Username: user1

Password: ************

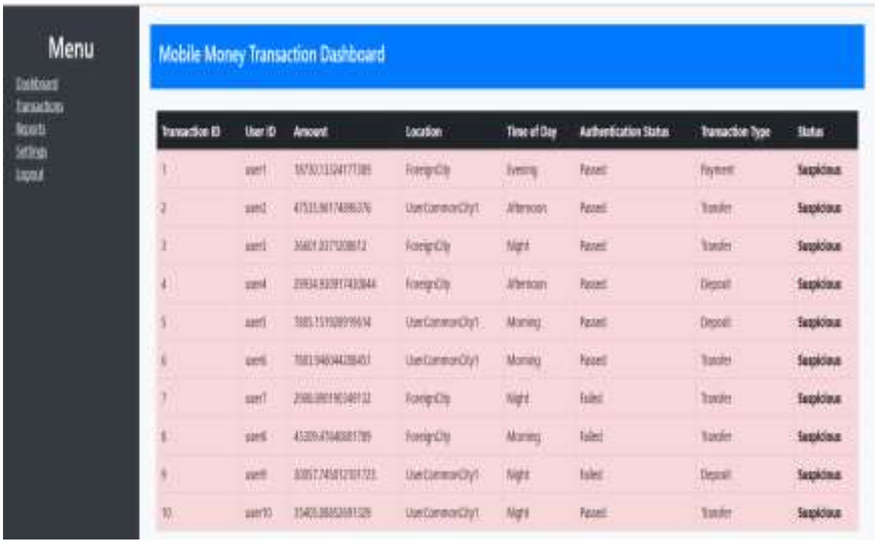
Fig. 8: Login form to authenticate users



Your 2FA Code is [illegible]

Enter 2FA Code:

Fig. 9: OTP authentication to verify users



Mobile Money Transaction Dashboard

Transaction ID	User ID	Amount	Location	Time of Day	Authentication Status	Transaction Type	Status
1	user1	18730.13324177185	ForeignCity	Evening	Passed	Payment	**Suspicious**
2	user2	47535.9617486376	UserCommonCity1	Afternoon	Passed	Transfer	**Suspicious**
3	user3	36601.2071208612	ForeignCity	Night	Passed	Transfer	**Suspicious**
4	user4	29934.93091743844	ForeignCity	Afternoon	Passed	Deposit	**Suspicious**
5	user5	7885.151930899614	UserCommonCity1	Morning	Passed	Deposit	**Suspicious**
6	user6	7083.946044208451	UserCommonCity1	Morning	Passed	Transfer	**Suspicious**
7	user7	2988.080196348132	ForeignCity	Night	Failed	Transfer	**Suspicious**
8	user8	45209.47040881785	ForeignCity	Morning	Failed	Transfer	**Suspicious**
9	user9	30057.74581210723	UserCommonCity1	Night	Failed	Deposit	**Suspicious**
10	user10	35405.38853091528	UserCommonCity1	Night	Passed	Transfer	**Suspicious**

Fig. 10: Suspicious transactions detected by the RF model

DOI: 10.17148/IJARCCE.2025.14215

V. DISCUSSION

Figure 6 presents the classification report from the Random Forest model trained on the mobile money transaction data. The report showcases evaluation metrics like precision, recall, and F1-score for the model's ability to classify suspicious and normal transactions. The performance metrics indicate a good balance between precision (correctly predicting suspicious transactions without too many false positives) and recall (identifying most of the true suspicious transactions). These metrics demonstrate that the Random Forest model has effectively learned the patterns of suspicious activities. Following this report is the confusion matrix shown in Figure 7 which a summary of the model's performance in detecting suspicious transactions. It shows the number of true positives, true negatives, false positives, and false negatives. The matrix helps in understanding how well the model is distinguishing between suspicious and normal transactions. A high number of true positives (correctly identified suspicious transactions) and a low number of false negatives (missed suspicious transactions) are key indicators of the model's success in identifying fraudulent activities.

The model was later deployed to show the performance. Figure 8 depicts the login form used for user authentication in the system. The form is part of the deployed interface, where users must input their credentials to access the system. The login process ensures that only authorized individuals can enter the system, reinforcing security by preventing unauthorized access to sensitive transaction data. In Figure 9, OTP Authentication to Verify Users is displayed. This figure shows the OTP (One-Time Password) authentication process that follows the initial login step. OTP adds an additional layer of security by requiring users to provide a dynamically generated password sent to their mobile devices. This two-factor authentication mechanism strengthens the security of the system by verifying the user's identity through something they possess (their mobile phone). In Figure 10, Suspicious Transactions Detected by the Random Forest Model is clearly indicated. The detected suspicious transactions are highlighted in the interface, as flagged by the Random Forest model. ‘Suspicious transactions’ providing a visual cue for system users to quickly identify and review potentially fraudulent activities. The model's integration into the interface allows for real-time monitoring and threat detection in mobile money transactions.

The proposed system shows a testing accuracy of 99% which underscores the effectiveness of the proposed Random Forest model and SMOTE techniques in detecting suspicious transactions, making the system more reliable and generalizable to real-world scenarios.

VI. CONCLUSION

The main contribution of this research to knowledge lies in the development of an integrated threat detection and two-factor authentication (2FA) model specifically tailored for mobile money transactions, addressing both fraud detection and user authentication in a unified approach. This study combines the Random Forest algorithm for real-time threat detection with SMOTE for handling class imbalance, ensuring a higher accuracy in identifying suspicious transactions. Additionally, the implementation of a secure 2FA system, featuring both password-based login and OTP verification, further strengthens user authentication processes. What sets this work apart is its practical deployment of these models into native mobile money application prototypes, offering a comprehensive, scalable solution that enhances both transaction security and user experience, making it highly adaptable to real-world mobile financial systems.

REFERENCES

[1]. Talom, F. S. G., & Tengeh, R. K. (2019). The impact of mobile money on the financial performance of the SMEs in Douala, Cameroon. *Sustainability*, *12*(1), 183

[2]. El Ayeb, S., Hemery, B., Jeanne, F., & Cherrier, E. (2020). Community detection for mobile money fraud detection. In *2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS)* (pp. 1-6). IEEE

[3]. Guma, A. (2022). Development of a secure multi-factor authentication algorithm for mobile money applications (*Doctoral dissertation*, NM-AIST).

[4]. Aburbeian, A. M., & Fernández-Veiga, M. (2024). Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. *AI*, *5*(1), 177-194.

[5]. Rbeian, A., & Mohamad, A. H. (2024). *Secure Internet Financial Transactions using Multifactor Authentication and Machine Learning* (Doctoral dissertation, AAUP).

[6]. Lokanan, M. E. (2023). Predicting mobile money transaction fraud using machine learning algorithms. *Applied AI Letters*, *4*(2), e85.

[7]. Ajish, S., & Anil Kumar, K. S. (2022). Secure mobile internet banking system using QR code and biometric authentication. In *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021* (pp. 791-807). Singapore: Springer Nature Singapore.

[8]. Hajek, P., Abedin, M. Z., & Sivarajah, U. (2023). Fraud detection in mobile payment systems using an XGBoost-based framework. *Information Systems Frontiers*, *25*(5), 1985-2003.

[9]. Chawla, N. V., Bowyer, K. W., & Hall, L. O. (2002). Kegelmeyer WPJJoair. *SMOTE: synthetic minority over-sampling technique*, *16*, 321-357.

[10]. Hu, M., & Li, X. (2019). Fraud Detection in Mobile Payments Using Machine Learning. *Journal of Financal Technology*. 5(2). 112-130

[11]. Siddaiah, U., Anjaneyulu, P., Haritha, Y., & Ramesh, M. (2023, May). Fraud Detection in Online Payments using Machine Learning Techniques. In *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 268-273). IEEE.

BIOGRAPHY

Ms Predise Jessica Bai obtained her Bachelor of Science Degree from the the Department of Computer Science, Niger Delta University, Bayelsa State, Nigeria. She is a Masters student at the Rivers State University where she is studying Computer Science. Her main research work focuses on Machine Learning, Data Science, and Artificial Intelligence. She has presented at Tech-Expo conferences and contributed to peer-reviewed research in the field.

Dr. Victor. T Emmah obtained his Bachelor of Science degree and Master of Science degree from Department of Computer Science, Rivers State University and University of Port Harcourt respectively. He is currently a senior Lecturer in the Department of Computer Science, Rivers State University. He is a member of the Computer Professional (Registration Council) of Nigeria. His main research work focuses on Machine Learning, Data Science, Deep Learning and Artificial Intelligence.

Dr. O. E. Taylor obtained his B. Sc, M. Sc and Ph. D degrees all in Computer Science from the Rivers State University of Science and Technology, University of Ibadan and University of Port Harcourt, Nigeria respectively. He is currently Senior Lecturer in the Department of Computer science, Rivers State University, Port Harcourt, Nigeria. He is a chartered member of the Computer Professionals (Registration Council) of Nigeria and Nigeria Computer Society. His research focuses on intelligent systems, smart space, context-aware systems, machines learning algorithms and artificial intelligence. He has over ten years of teaching and research experience.