SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I3P110

Volume 11 Issue 3, 96-105, March 2024

Original Article

Enhancing Security in Mobile Wallet Payments: Machine Learning-Based Fraud Detection across Prominent Wallet Platforms

Abdullahi Ahmed Abdirahman[1], Abdirahman Osman Hashi[1], Ubaid Mohamed Dahir[1], Mohamed Abdirahman Elmi[1], Octavio Ernest Romo Rodriguez[2]

[1]*Faculty of Computing, SIMAD University, Mogadishu-Somalia.*
[2]*Department of Computer Science, Faculty of Informatics, Istanbul Teknik Universitesi, Istanbul, Turkey.*

[1]*Corresponding Author : aaayare@simad.edu.so*

Received: 08 January 2024 Revised: 13 February 2024 Accepted: 11 March 2024 Published: 31 March 2024

Abstract *- This paper presents a novel approach to enhancing the security of financial transactions within mobile wallet applications through the implementation of machine learning-based fraud detection models. This study implements four machine learning models: Random Forest, Logistic Regression, Support Vector Machine and Artificial Neural Networks (ANN), and it evaluates the effectiveness of these models in detecting fraudulent activities within four prominent mobile wallet platforms: EVC Plus, Premier Wallet, Dahabshil Wallet, and IBS Wallet. The evaluation encompasses a comprehensive analysis of model performance metrics, including accuracy, precision, and recall, to assess the efficacy of fraud detection across different wallet ecosystems. The results demonstrated that the ANN-based model exhibits promising accuracy and effectiveness in identifying fraudulent transactions by achieving an accuracy of 91.39%, thereby providing users with enhanced security and confidence in their digital financial transactions. By integrating these fraud detection capabilities into mobile wallet applications, users can proactively mitigate fraud risks and safeguard their financial assets, fostering trust and reliability in the digital financial ecosystem. This research contributes valuable insights and solutions to the ongoing efforts to combat fraud in mobile wallet payments, paving the way for more secure and resilient financial transactions in the digital era.*

Keywords *- Fraud detection, Mobile wallet, Machine Learning, Logistic Regression, Support Vector Machine, Random Forest.*

1. Introduction

The combination of Artificial Intelligence (AI) and big data has emerged as a revolutionary force across a variety of different sectors in this century, which has been distinguished by technical developments on a scale never before seen [1]. The field of mobile wallet solutions is one area in which this synergy has a significant amount of untapped potential. This means that digital financial platforms have completely changed the manner in which people, organizations, and even governments handle their own financial situations [2]. However, payment fraud still poses a significant challenge to financial institutions, merchants, and consumers worldwide, resulting in substantial financial losses and reputational damage [3].

Traditional rule-based fraud detection systems are no longer able to accurately identify and stop fraudulent transactions due to the growing sophistication and complexity of fraudulent operations. Machine learning (ML) techniques have surfaced as viable solutions to these problems, offering increased precision and efficacy in the identification of payment fraud [4]. Recent advancements in ML techniques have enabled the development of more sophisticated fraud detection models capable of detecting intricate patterns and anomalies indicative of fraudulent behaviour.

One such method proposed by the author [5] utilizes deep-learning algorithms, specifically CNNs, to extract features from transaction data and detect falsified activities with high accuracy and precision. By leveraging the inherent capabilities of CNNs in capturing spatial and temporal dependencies within sequential data, the proposed model demonstrates superior performance in detecting previously unseen fraud patterns [6].

Moreover, the incorporation of ensemble learning techniques, proposed by the author [7], has further enhanced the robustness and generalization capabilities of fraud detection models. By combining multiple base learners, such as RF, GBMs, and SVMs, into a unified ensemble model, the author [8] achieved significant improvements in fraud detection accuracy and reduced the risk of false positives.

Additionally, the integration of Explainable AI (XAI) techniques into fraud detection models has gained traction in recent research efforts. XAI methods, such as LIME and SHAP, enable the interpretation and explanation of model predictions, thereby enhancing transparency and accountability in fraud detection systems [9]. By providing insights into the features driving the model's decisions, XAI facilitates better understanding and trust in the model's outputs, fostering collaboration between human analysts and automated fraud detection systems.

Meanwhile, the implementation of mobile wallets is of special relevance when seen within the framework of Somalia. Since a long time ago, the nation's financial landscape has struggled to overcome difficulties that are caused by political unpredictability and restricted access to official banking channels.

Mobile wallets are a ray of sunshine since they democratize access to financial services and help the economy to become more resilient. To recognise the full potential of big data and AI to revolutionize financial inclusion in Somalia, it is important to have a concrete understanding of the intricacies that are unique to this particular setting.

In light of these recent advancements, this paper explores MLA methods to address the issue of fraud in Somali wallet payments. We propose to develop ML models specifically tailored to detect fraudulent activities occurring within Somali wallet payment systems. Additionally, we aim to leverage these models to design and implement a wallet application that effectively mitigates fraud risks for users.

2. Related Work

Big Data and Artificial Intelligence (AI) have become a powerful force reshaping industries globally in the era of digital transformation. The synergy between different technologies has been especially successful in the development of mobile wallets, which are digital financial platforms that have transformed the way we handle, conduct transactions, and engage with money [10].

Historically, financial activities were limited to physical locations such as bank branches and cash transactions. Mobile wallets signify a significant advancement towards a future where transactions occur instantly through a screen, beyond geographical limits and time restrictions. Digital archives of financial information are now essential in modern life, providing a more efficient option compared to traditional payment methods [11].

Meanwhile, the use of MLA for spotting fraudulent activities in online financial dealings has become crucial, particularly with the rise in e-commerce and digital money transfers [12]. Advanced algorithms have been applied to analyze large volumes of transactional data to identify fraud. Notably, collective methods like random forests have shown higher effectiveness by delivering more accurate results. Further advancements in this field have been driven by deep learning, which delves into the transaction data to unravel complex patterns not immediately evident. This approach has proved to be exceptionally effective, surpassing traditional techniques and showcasing the significant promise of deep learning in bolstering the security of digital financial services [13].

Furthermore, the author [14] focused on the application of anomaly detection methods, specifically Isolation Forest and Local Outlier Factors, for detecting fraudulent activities in mobile payment transactions. The author conducted experiments on real-world datasets and demonstrated the effectiveness of anomaly detection techniques in identifying unusual patterns indicative of fraudulent behaviour.

In addition to algorithmic approaches, efforts have been made to enhance the transparency of fraud detection models through explainable AI techniques. Meanwhile, the author [15] conducted a comparative study of LIME and SHAP, two popular methods for generating interpretable explanations of machine learning models. Their research highlights the importance of explainability in gaining insights into model predictions and fostering trust in fraud detection systems.

On the other hand, Natural Language Processing (NLP) capabilities equip mobile wallets with the ability to interact with users in a human-like manner. This opens up avenues for seamless customer support interactions, transcending linguistic barriers and ensuring accessibility for diverse user demographics. AI-powered chatbots effectively turn mobile wallets into personalized financial concierges [16].

While the convergence of Big Data and AI in mobile wallets undoubtedly ushers in a new era of convenience, its true power lies in its potential for social transformation. In the context of Somalia, a nation with a complex socio-political landscape, mobile wallets offer a lifeline to economic resilience.

The author [17] underscores the potential of digital financial services in fostering economic stability, particularly in regions facing adversity. Yet, this convergence is not without its challenges. As the volume of data exchanged through mobile wallets escalates, concerns about data privacy and security come to the forefront. Striking the delicate balance between leveraging data for insights and safeguarding user privacy requires vigilant regulation and ethical guidelines [18].

Furthermore, advancements in biometric authentication have redefined the security landscape of mobile wallets. Fingerprint recognition, facial recognition, and even iris scanning have become standard features, replacing traditional

PINs and passwords [19]. This not only enhances security but also streamlines the user experience, making the process of accessing and using a mobile wallet more intuitive and convenient. Beyond security, technological innovations have also been instrumental in enhancing the personalization of mobile wallet services [20].

In addition to these advancements, the proliferation of Near Field Communication (NFC) technology has been instrumental in simplifying the process of making payments. NFC allows contactless transactions, permitting users to make payments. This not only accelerates the speed of transactions but also minimizes the need for physical interaction with payment terminals, a particularly pertinent feature in times of heightened hygiene concerns [21].

Furthermore, AML and KYC regulations are paramount in the mobile wallet landscape. Ensuring that users are properly identified and verified is crucial in preventing illicit activities [22].

Mobile wallet providers must implement robust AML and KYC processes, collaborating closely with regulatory bodies to uphold the integrity of the financial system. Consumer protection is another regulatory consideration. Ensuring transparency in fees, providing recourse for unauthorized transactions, and setting limits on liability in cases of fraud are key areas of focus.

Regulators are keen on creating an environment where users can have confidence in the safety and reliability of mobile wallet services. Additionally, as the technology evolves, regulators are grappling with issues related to cross-border transactions and international regulatory harmonization. The global nature of digital financial services demands cooperation among regulatory bodies to establish a framework that allows for seamless, secure, and compliant cross-border transactions [23].

In the Somali context, the adoption and implementation of mobile wallets take on a distinctive significance. This dynamic East African nation has a history marked by political complexity and economic challenges. Against this backdrop, mobile wallets emerge as a beacon of hope, offering a lifeline to financial stability and economic resilience [24].

One of the defining characteristics of Somalia is its limited access to formal banking channels. Years of political instability and conflict have disrupted the traditional banking infrastructure. In this context, mobile wallets step in to bridge the gap, providing a digital alternative to the conventional banking system. With a mobile phone and an internet connection, individuals in even the most remote regions of Somalia can now engage in financial transactions, expanding economic opportunities for a previously underserved population [25].

Furthermore, the Somali diaspora plays a crucial role in the nation's economic landscape. Remittances from Somalis living abroad constitute a substantial portion of the country's GDP. Mobile wallets offer a streamlined and secure avenue for these remittances to reach their intended recipients. By digitizing these transactions, mobile wallets reduce the reliance on informal and potentially risky channels, ensuring that remittances have a direct and positive impact on the Somali economy.

The resilience and adaptability of the Somali people are further exemplified by the widespread adoption of mobile technology. Despite challenges in infrastructure and connectivity, mobile phone penetration is remarkably high. This tech-savvy population is quick to embrace innovations that offer solutions to their unique circumstances. Mobile wallets, with their potential to empower individuals economically, have found fertile ground in Somalia [26].

However, it's important to note that the unique landscape of Somalia also presents its own set of challenges. Regulatory frameworks for digital financial services are still evolving, and issues related to security and trust remain paramount. Ensuring the security of transactions and protecting user data are critical concerns that mobile wallet providers and regulatory bodies must address collaboratively.

Moreover, education and awareness about the benefits and proper use of mobile wallets are essential. In a landscape where formal financial education may be limited, providing accessible and user-friendly resources is crucial in ensuring that individuals can make the most of this transformative technology.

For that reason, it is important that trust forms the bedrock upon which mobile wallet adoption is built. Users must have confidence that their financial information is secure and that transactions will be conducted reliably. Research by the author [27] underscores the pivotal role of trust in influencing consumer attitudes towards mobile wallet adoption.

Trust manifests on multiple levels - trust in the platform itself, trust in the technology underpinning it, and trust in the broader financial ecosystem. Given the sensitive nature of financial transactions, security concerns loom large in the minds of potential users. Mobile wallet providers must invest significantly in robust security measures to assuage these concerns.

The integration of AI in mobile wallets plays a critical role in fortifying security. Machine learning algorithms continuously analyse transactional data, identifying and flagging suspicious activities in real time. This not only protects users from potential fraud but also bolsters trust in the platform.

3. Methodology

This research methodology comprises several key steps aimed at developing and evaluating ML models for fraud detection in Somali wallet payments. Firstly, we will acquire and pre-process a comprehensive dataset containing transactional data. Next, we will explore and implement various ML algorithms of LR, DT, RF, and NN to train and validate fraud detection models on the prepared dataset. Additionally, we will use techniques such as cross-validation and hyperparameter tuning to optimize model performance and generalization capabilities. Furthermore, we will incorporate explainable AI methods to enhance the transparency and interpretability of the developed models, enabling stakeholders to understand and trust the model predictions.

3.1. Proposed Methodology

To facilitate the experimental process and enable the training of classifiers adept at predicting fraudulent transactions, a series of fundamental steps were carried out. These steps encompassed various essential procedures, starting with the collection of pertinent data sets. This initial phase involved gathering sufficient data that encompassed both fraudulent and legitimate transactions, ensuring a comprehensive representation for subsequent analysis.

Once the data had been thoroughly explored, the next phase involved preparation and pre-processing, where the data underwent cleaning, transformation, and normalization procedures to render it suitable for analysis and model training. This stage is vital as it ensures the data is in a standardized format and free from inconsistencies or biases that could affect the performance of the classifiers. Subsequently, outlier detection techniques were applied to identify anomalous data points that could potentially skew the results or adversely affect model performance. After addressing outliers, the data was then used for model training, where various machine learning algorithms were used to develop classifiers capable of accurately discerning fraudulent transactions. Finally, model evaluation was conducted to assess the performance and efficacy of the trained classifiers in accurately predicting fraudulent activities, thereby completing the experimental process outlined in Figure 1.

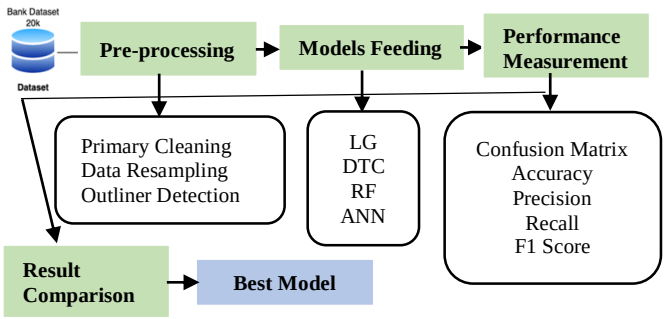

Fig. 1 Proposed methodology

3.2. Data Collection

As we know data collection is the initial phase in any data analysis or machine learning model and involves gathering relevant data from various sources. In the context of fraud detection using the "Fraud detection bank dataset 20K records binary" from Kaggle, data collection used as our dataset comes from the Kaggle platform.

This dataset is specifically designed for fraud detection purposes, containing 20,000 records with binary labels indicating whether each transaction is fraudulent or not. This dataset includes various features or attributes associated with each transaction, such as transaction amount, timestamp, and merchant information. The upcoming Figure 2 shows the dataset.

	0	1	2	3	4	5	6	7	8	9
Unnamed: 0	0.0	1.0	2.0	3.0	4.0	5.0	6.0	7.0	8.0	9.0
col_0	9.0	0.0	0.0	17.0	1.0	0.0	12.0	10.0	0.0	0.0
col_1	1354.0	239.0	260.0	682.0	540.0	11.0	2584.0	6036.0	1233.0	182.0
col_2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
col_3	18.0	1.0	4.0	1.0	2.0	0.0	6.0	3.0	8.0	1.0
...	...	...	...	...	...	...	...	...	...	...
col_108	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
col_109	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	1.0	0.0
col_110	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0
col_111	49.0	55.0	56.0	65.0	175.0	95.0	78.0	103.0	191.0	392.0
targets	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

114 rows × 20468 columns

Fig. 2 Dataset

3.3. Data Pre-Processing

In the data pre-processing phase, various techniques are used to prepare the collected data for further analysis and model development. One common pre-processing task is handling missing values, which involves identifying and addressing any instances where data points are absent or incomplete. In our dataset, there were no missing values of the transaction records as the upcoming figure shows it.

	Unnamed: 0	col_0	col_1	col_2	col_3
count	20468.000000	20468.000000	20468.000000	20468.000000	20468.000000
mean	10233.500000	3.226256	294.793043	0.420021	2.329343
std	5908.746991	20.564308	717.541984	7.367275	10.068512
min	0.000000	0.000000	0.000000	0.000000	0.000000
25%	5116.750000	0.000000	38.000000	0.000000	0.000000
50%	10233.500000	0.000000	97.000000	0.000000	1.000000
75%	15350.250000	2.000000	283.000000	0.000000	2.000000
max	20467.000000	2301.000000	37808.000000	904.000000	772.000000

8 rows × 114 columns

Fig. 3 No missing data

3.4. Data Resampling

To address class imbalance, data resampling is the act of changing the distribution of classes within the dataset. When one class fraudulent transactions in this case is substantially underrepresented in comparison to another class non-fraudulent transactions class imbalance arises. This can skew model performance and affect the dataset. We used to oversample the minority class to address this imbalance in order to address it.

In order to equal the number of examples in the majority class (non-fraudulent transactions), oversampling entails increasing the number of instances in the minority class (fraudulent transactions). Usually, to accomplish this, one can either create synthetic instances by utilizing methods like the SMOTE found in the Scikit-learn (sklearn) module or duplicate examples that already exist in the minority class.

By oversampling the minority class, the dataset becomes more balanced, allowing machine learning algorithms to learn from both classes more effectively and reducing the likelihood of biased predictions towards the majority class. Implementing oversampling techniques using the sklearn library provides a convenient and standardized way to perform data resampling, ensuring reproducibility and ease of integration into the fraud detection pipeline.

3.5. Model Training and Evaluation

Moving forward with the development of predictive models for fraud detection, we'll be employing a variety of MLAs. These will include KNN, RF, LR, SVM, and ANN. These models will be meticulously trained and assessed to accurately identify fraudulent transactions by analyzing the characteristic patterns within the dataset.

The KNN algorithm is a simple yet effective method used for classification tasks. It works by assigning a class to a new instance based on the most common class among its 'k' closest neighbors in the feature space. The choice of 'k' is crucial for the algorithm's success and is typically determined through cross-validation to ensure optimal performance.

On the other hand, RF is an ensemble-learning technique that constructs multiple decision trees during training. It then aggregates their outcomes by averaging predictions for regression tasks or by determining the most frequent prediction (the mode) for classification tasks. This method helps reduce overfitting and enhances the robustness of the model.

LR, although linear and seemingly simplistic, is a robust classification technique used for binary classification problems. It predicts the probability of an instance belonging to a particular class using a logistic function. Its efficacy is particularly pronounced when the predictors are linearly related to the log odds of the outcome.

Support Vector Machines (SVM) represent a powerful supervised learning approach, well-suited for both regression and classification challenges. They excel by identifying an optimal separating hyperplane in the feature space that maximizes the margin between different class instances, demonstrating high effectiveness, particularly in spaces with many dimensions.

In parallel, Artificial Neural Networks (ANN) draw inspiration from the human brain's neural network architecture. They consist of layers of interconnected nodes: input, multiple hidden layers, and an output layer. ANNs are capable of recognizing complex patterns through a learning process involving both forward propagation of inputs and backpropagation of errors. This structure makes them highly adaptable to tasks with intricate, non-linear relationships in the data.

4. Results and Discussion

In the following section, we will discuss the outcomes of the ML models that were implemented, along with the results of those models.

4.1. Results

The first algorithm was the K-Nearest Neighbors (KNN) model, and it exhibited a commendable performance in detecting fraudulent transactions, achieving an accuracy of 87%. With a precision of 76%, the model demonstrated its ability to accurately identify untrue transactions among all transactions labelled as fraudulent, as can be seen from Figures 4 and 5.

Additionally, the recall score of 69% highlights the model's effectiveness in capturing actual fraudulent transactions among all instances of fraudulent activity. Interpretation of precision and recall indicates that while the model minimizes false positives, there is a proportion of actual fraudulent transactions that remain undetected.

Classification Report for K-Nearest Neigbours:

	Precision	Recall	F1-Score	Support
0	0.90	0.93	0.91	3810
1	0.76	0.69	0.72	1307
Accuracy			0.87	5117
Macro Avg	0.83	0.81	0.82	5117
Weighted Avg	0.86	0.87	0.86	5117

Confusion Matrix of K-Nearest Neigbours:

[[3526 284]

[403 904]]

Fig. 4 KNN classification report

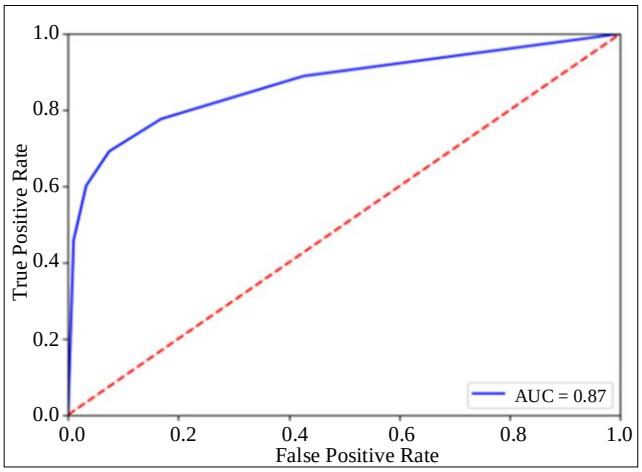

Fig. 5 KNN ROC report

The confusion matrix further clarifies the model's performance, with 904 out of 1307 actual fraudulent transactions correctly classified as fraudulent, while 403 instances were misclassified as non-fraudulent. While the KNN model showcases promising accuracy, precision, and recall in fraud detection, there is a need for further refinement to reduce misclassifications and enhance the model's ability.

Meanwhile, RF demonstrated strong performance in detecting falsified transactions, gaining an accuracy of 90%. With a precision of 77%, the model displayed its ability to accurately identify fraudulent transactions among all transactions labelled as fraudulent, indicating a relatively low rate of false positives, as can be seen from Figures 6 and 7.

Moreover, the recall score of 87% signifies the model's effectiveness in capturing actual fraudulent transactions among all instances of fraudulent activity, indicating a lower rate of false negatives compared to KNN. The confusion matrix provides additional insights into the model's performance, with 1138 out of 1307 actual fraudulent transactions correctly classified as fraudulent, while only 169 instances were misclassified as non-fraudulent. In general, the Random Forest Classifier exhibits robust accuracy, precision, and recall in fraud detection, suggesting its suitability for identifying fraudulent transactions.

On the other hand, the Logistic Regression model demonstrated moderate performance in detecting fraudulent transactions, getting correctness of 77%. With a precision of 54%, the model showed its ability to accurately identify fraudulent transactions among all transactions labelled as fraudulent, albeit with a higher rate of false positives compared to the Random Forest Classifier, as can be seen from Figures 8 and 9.

Additionally, the recall score of 57% indicates the model's effectiveness in capturing actual fraudulent transactions among all instances of fraudulent activity, albeit with a lower rate compared to both KNN and Random Forest. The confusion matrix illustrates the model's performance, with 746 out of 1307 actual fraudulent transactions correctly classified as fraudulent, while 561 instances were misclassified as non-fraudulent.

Classification Report for Random Forest Classifier:

	Precision	Recall	F1-Score	Support
0	0.95	0.91	0.93	3810
1	0.77	0.87	0.82	1307
Accuracy			0.90	5117
Macro Avg	0.86	0.89	0.88	5117
Weighted Avg	0.91	0.90	0.90	5117

Confusion Matrix of Random Forest Classifier:

[[3475 335]

[169 1138]]

Fig. 6 Random Forest classification report

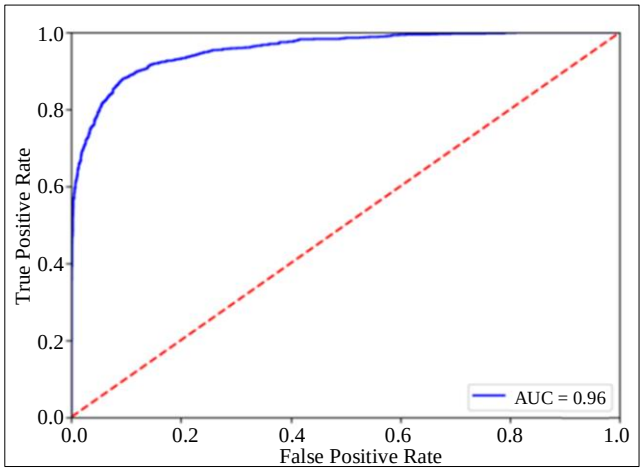

Fig. 7 Random Forest ROC report

Classification Report for Logistics Regression:

	Precision	Recall	F1-Score	Support
0	0.85	0.83	0.84	3810
1	0.54	0.57	0.56	1307
Accuracy			0.77	5117
Macro Avg	0.70	0.70	0.70	5117
Weighted Avg	0.77	0.77	0.77	5117

Confusion Matrix of Logistics Regression:

[[3176 634]

[561 746]]

Fig. 8 Logistic Regression classification report

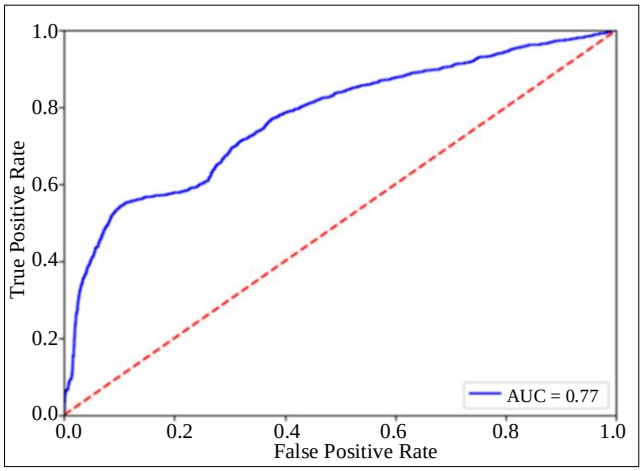

Fig. 9 Logistic Regression ROC report

Classification Report for Support Vector Machine (SVM):

	Precision	Recall	F1-Score	Support
0	0.74	1.00	0.85	3810
1	0.00	0.00	0.00	1307
Accuracy			0.74	5117
Macro Avg	0.37	0.50	0.43	5117
Weighted Avg	0.55	0.74	0.64	5117

Confusion Matrix of Support Vector Machine (SVM):

[[3810 0]

[1307 0]]

Fig. 10 Support Vector Machine classification report

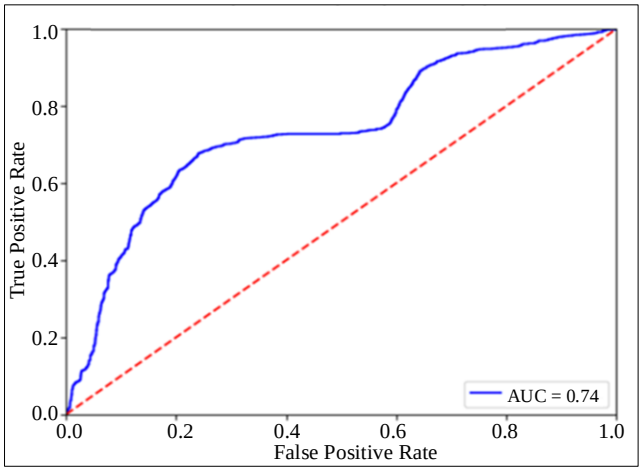

Fig. 11 Support Vector Machine ROC report

While the Logistic Regression model demonstrates reasonable accuracy and precision, there is still a need for improvement in reducing misclassifications and enhancing the model's efficacy in accurately identifying fraudulent transactions.

Meanwhile, the SVM model exhibited suboptimal performance in detecting fraudulent transactions, achieving an accuracy of 74%. With a precision of 55% and recall of 43% for detecting fraudulent transactions, the model demonstrated significant limitations in accurately identifying instances of fraud.

The precision and recall scores indicate the model's failure to correctly classify any actual fraudulent transactions, resulting in a complete inability to detect instances of fraud, as can be seen from Figures 10 and 11. The confusion matrix underscores the model's poor performance, with all transactions being classified as non-fraudulent, leading to a failure to identify any actual instances of fraud.

The SVM model shows significant deficiencies in accurately identifying fraudulent transactions, highlighting the need for alternative approaches or model refinements to improve fraud detection efficacy.

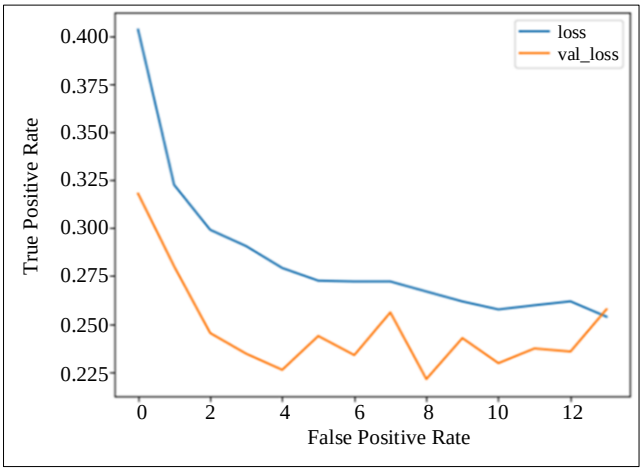

Fig. 12 ANN ROC report

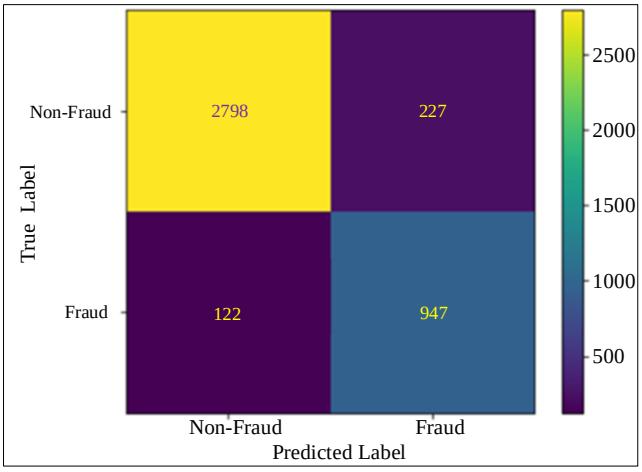

Fig. 13 Confusion matrix

On the other hand, the Artificial Neural Network (ANN) model achieved an impressive accuracy of 91.39% in

detecting fraudulent transactions. This accuracy score indicates the model's effectiveness in correctly classifying transactions overall. Additionally, the progressive improvement in recall scores observed over multiple epochs suggests that the ANN model successfully captures more instances of fraudulent transactions over time, as can be seen from Figures 12 and 13.

4.2. Discussions

There are clear differences between the models when it comes to how well they find fraudulent deals. The Random Forest Classifier stands out with an accuracy of 90%, coupled with a precision of 77% and recall of 87%. This model effectively minimizes false positives and false negatives, showcasing its robust performance in identifying fraudulent transactions. In contrast, while the K-Nearest Neighbours (KNN) model achieves a slightly lower accuracy of 87%, its precision of 76% and recall of 69% still demonstrate solid performance, there is still a need for improvement.

Logistic Regression comes up with a moderate accuracy of 77% and precision and recall scores of 54% and 57%, respectively. The Artificial Neural Network (ANN) model boasts the highest accuracy of 91.39%, indicating its potential for accurate fraud detection. Meanwhile, the SVM model lags behind, with the lowest accuracy of 74% and an inability to correctly classify any actual fraudulent transactions, as indicated by its precision and recall low scores, as can be seen in Table 1.

Overall, while some models excel in accurately identifying fraudulent transactions, others demonstrate limitations that warrant further refinement and optimization to enhance fraud detection efficacy.

5. Implementation of Mobile App

The implementation of an Artificial Neural Network (ANN)-based fraud detection model within a mobile wallet application represents a significant advancement in enhancing the security and trustworthiness of financial transactions. This innovative solution allows users of four prominent wallets – EVC Plus, Premier Wallet, Dahabshil Wallet, and IBS Wallet to benefit from realtime fraud detection capabilities, thereby safeguarding their funds and personal information.The upcoming Figure 14 shows that each user will save their number for one of the four wallets, and this will be the unique ID for key money transfers. After registration, users can transfer money between wallets while machine learning coordinates the transactions, as shown in Figure 15.

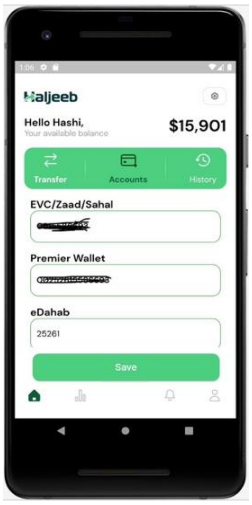

Fig. 14 Set up wallet numbers

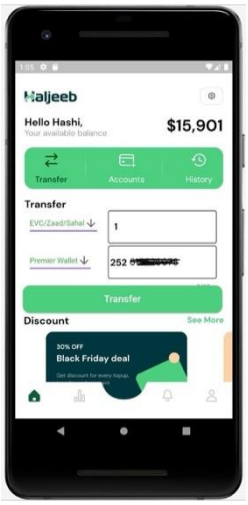

Fig. 15 Transfer screen

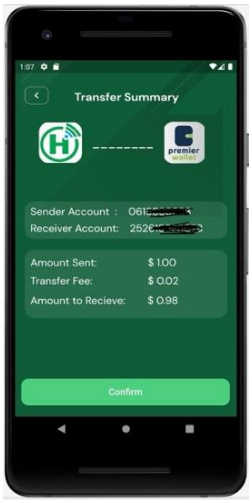

Fig. 16 Payment confirmation

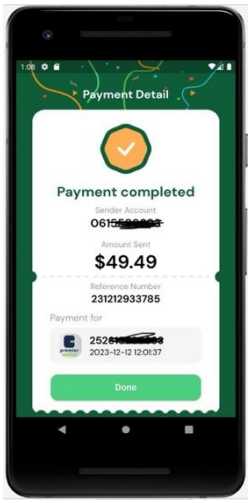

Fig. 17 Successful transaction

Table 1. Model performances

Model	Accuracy	Precision	Recall	F1 Score	Model
Random Forest Classifier	90%	77%	87%	82%	90%
K-Nearest Neighbors	87%	76%	69%	72%	87%
Logistic Regression	77%	54%	57%	56%	77%
Support Vector Machine	74%	52%	55%	43%	74%
Artificial Neural Network	91.39%	87%	90%	90%	91.39%

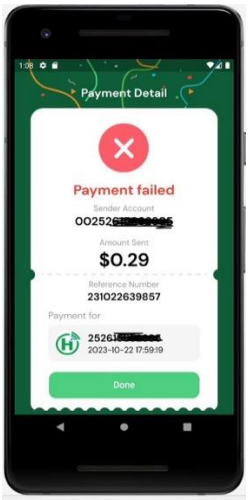

Fig. 18 Declined transaction

Before the transaction is made, there will be another screen that will confirm the transaction from the wallet. The user will have to make sure that the transaction is true, and if it is true, the ANN will initiate the transaction by contacting the wallet through an API, as can be seen in Figures 16 and 17. If the transaction is not successful, then there will be a declined screen and this screen will tell the information as well as it can be seen from Figure 18.

Therefore, by integrating the ANN model into the mobile wallet app, users gain access to a sophisticated fraud detection mechanism that analyses transactional data in-depth. As users conduct transactions, the ANN model continuously evaluates patterns and features within the data to identify any suspicious or fraudulent activities. This proactive approach enables the app to promptly alert users to potential fraud attempts, empowering them to take immediate action to mitigate risks and protect their financial assets.

Moreover, the implementation of the ANN-based fraud detection model enhances user confidence and trust in the security of the mobile wallet app. Users can conduct transactions with peace of mind, knowing that the app leverages advanced machine-learning techniques to detect and prevent falsified activities effectively. This not only enhances user experience but also fosters long-term loyalty and engagement with the app.

Furthermore, the deployment of the fraud detection model across multiple wallets – EVC Plus, Premier Wallet, Dahabshil Wallet, and IBS Wallet – underscores its versatility and scalability. Regardless of the specific wallet platform used by the user, the ANN model offers consistent and reliable fraud detection capabilities, ensuring uniform protection across different financial ecosystems.

6. Conclusion

Through this study, it was shown that machine learning-based fraud detection models can make financial activities safer in mobile wallet apps. Different models, like the RF, KNN, LR, SVM, and Artificial Neural Network, have been tested and shown to be good at finding scams. When these models are used in popular mobile wallet systems, they protect users well against fraud, which builds trust and confidence in online financial transactions.

For future work, more study needs to be done to make fraud detection models in mobile wallet apps more scalable and effective going forward. One area that could be worked on in the future is making the current machine learning methods more accurate and reducing the number of false positives and negatives. Also, looking into more advanced methods like deep learning and reinforcement learning might help us find new ways to spot changing fraud trends right away.

Adding user behavior analytics and anomaly detection algorithms could also add more layers of security and make scam detection systems better at responding to new threats. To stay ahead of fraudsters and keep digital financial activities safe and trusted, this field needs to keep coming up with new ideas and doing research.

References

[1] T. Karthikeyan, M. Govindarajan, and V. Vijayakumar, "An Effective Fraud Detection Using Competitive Swarm Optimization Based Deep Neural Network," *Measurement: Sensors*, vol. 27, pp. 1-12, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Can Iscan, and Fatma Patlar Akbulut, "Fraud Detection Using Recurrent Neural Networks for Digital Wallet Security," *2023 8th International Conference on Computer Science and Engineering (UBMK)*, Burdur, Turkiye, pp. 538-542, 2023.[CrossRef] [Google Scholar] [Publisher Link]

[3] Victor Chang et al., "Digital Payment Fraud Detection Methods in Digital Ages and Industry 4.0," *Computers and Electrical Engineering*, vol. 100, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Dennis Ng et al., "Can we Classify Cashless Payment Solution Implementations at the Country Level?," *Electronic Commerce Research and Applications*, vol. 46, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Leonid Garin, and Vladimir Gisin, "Machine Learning in Classifying Bitcoin Addresses," *The Journal of Finance and Data Science*, vol. 9, pp. 1-10, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Can Iscan et al., "Wallet-Based Transaction Fraud Prevention through LightGBM with the Focus on Minimizing False Alarms," *IEEE Access*, vol. 11, pp. 131465-131474, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Imane Sadgali, Nawal Sael, and Fouzia Benabbou, "Fraud Detection in Credit Card Transactions Using Machine Learning Techniques," *2019 1st International Conference on Smart Systems and Data Science (ICSSD)*, Rabat, Morocco, pp. 1-4, 2019. [CrossRef] [Publisher Link]

[8] Vivek Ghai, and Sandeep Singh Kang, "Role of Machine Learning in Credit Card Fraud Detection," *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India, pp. 939-943, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Junhuan Zhang, Kewei Cai, and Jiaqi Wen, "A Survey of Deep Learning Applications in Cryptocurrency," *Iscience*, vol. 27, no. 1, pp. 1-40, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Bipin Bihari Jayasingh, and G. Bhagya Sri, "Online Transaction Anomaly Detection Model for Credit Card Usage Using Machine Learning Classifiers," *2023 International Conference on Emerging Smart Computing and Informatics (ESCI)*, Pune, India, pp. 1-5, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Maram A. Alamri, and Mourad A. Ykhlef, "A Machine Learning-Based Framework for Detecting Credit Card Anomalies and Fraud," *2023 27th International Conference on Information Technology (IT)*, Zabljak, Montenegro, pp. 1-7, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Manish Thakral et al., "Rigid Wrap ATM Debit Card Fraud Detection Using Multistage Detection," *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, Solan, India, pp. 774-778, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Yu-li Liu, Wenjia Yan, and Bo Hu, "Resistance to Facial Recognition Payment in China: The Influence of Privacy-Related Factors," *Telecommunications Policy*, vol. 45, no. 5, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Eray Arda Akartuna, Shane D. Johnson, and Amy Thornton, "Preventing the Money Laundering and Terrorist Financing Risks of Emerging Technologies: An International Policy Delphi Study," *Technological Forecasting and Social Change*, vol. 179, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Orăștean Ramona, "Financial Markets-Structural Changes and Recent Developments," *Reference Module in Social Sciences*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Simron Padhi, and Devi Priya Battina, "*Automating Root Cause Analysis of Anomalies in Ericsson Wallet Platform Using Machine Learning*," M.Sc. Thesis, Faculty of Computing, Blekinge Institute of Technology, Sweden, pp. 1-75, 2023. [Google Scholar] [Publisher Link]

[17] Messay Asgedom Gobena, "Money Laundering in Ethiopia: An Analysis of Typologies and Techniques," *Journal of Money Laundering Control*, vol. 26, no. 4, pp. 696-708, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Aakriti Singla, and Hitesh Jangir, "A Comparative Approach to Predictive Analytics with Machine Learning for Fraud Detection of Realtime Financial Data," *2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3)*, Lakshmangarh, India, pp. 1-4, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Khaled Gubran Al-Hashedi, and Pritheega Magalingam, "Financial Fraud Detection Applying Data Mining Techniques: A Comprehensive Review from 2009 to 2019," *Computer Science Review*, vol. 40, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Indrajani, Harjanto Prabowo, and Meyliana, "Learning Fraud Detection from Big Data in Online Banking Transactions: A Systematic Literature Review," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 8, no. 3, pp. 127-131, 2016. [Google Scholar] [Publisher Link]

[21] Jarrod West, and Maumita Bhattacharya, "Intelligent Financial Fraud Detection: A Comprehensive Review," *Computers & Security*, vol. 57, pp. 47-66, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[22] Sara Makki et al., "Fraud Analysis Approaches in the Age of Big Data-A Review of State of the Art," *2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W)*, Tucson, AZ, USA, pp. 243-250, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[23] Mario Bojilov, "*Methods for Assisting in Detection of Synthetic Identity Fraud in Credit Applications in Financial Institutions*," Thesis, Central Queensland University, 2023. [Google Scholar] [Publisher Link]

[24] Damion Gordon, *The Digital Identity Revolution: Assessing the Opportunities and Challenges for Developing Countries*, Rethinking Democracy and Governance, 1st ed., pp. 124-145, 2023. [Google Scholar] [Publisher Link]

[25] Anna Visvizi, Higinio Mora, and Erick G. Varela-Guzman, "The Case of rWallet: A Blockchain-based Tool to Navigate some Challenges Related to Irregular Migration," *Computers in Human Behavior*, vol. 139, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Chimuka Moonde, "*Secure Mobile Payment System Based on Blockchain Technology for Higher Learning Institutions*," Doctoral Dissertation, The University of Zambia, pp. 1-207, 2023. [Google Scholar] [Publisher Link]

[27] Qasim Umer et al., "Ensemble Deep Learning Based Prediction of Fraudulent Cryptocurrency Transactions," *IEEE Access*, vol. 11, pp. 95213-95224, 2023.[CrossRef] [Google Scholar] [Publisher Link]