IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 September 2023, accepted 26 September 2023, date of publication 4 October 2023, date of current version 29 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3321666

RESEARCH ARTICLE

Wallet-Based Transaction Fraud Prevention Through LightGBM With the Focus on Minimizing False Alarms

CAN ISCAN[1], OSMAN KUMAS[1], (Member, IEEE), FATMA PATLAR AKBULUT[1,2], (Member, IEEE), AND AKHAN AKBULUT[3], (Member, IEEE)

[1]Research and Development Center, FormicaAI, 41056 Istanbul, Turkey
[2]Department of Software Engineering, Istanbul Kültür University, 34158 Istanbul, Turkey
[3]Department of Computer Engineering, Istanbul Kültür University, 34158 Istanbul, Turkey

Corresponding author: Akhan Akbulut (a.akbulut@iku.edu.tr)

ABSTRACT E-wallets' rising popularity can be attributed to the fact that they facilitate a wide variety of financial activities such as payments, transfers, investments, etc., and eliminate the need for actual cash or cards. The confidentiality, availability, and integrity of a user's financial information stored in an electronic wallet can be compromised by threats such as phishing, malware, and social engineering; therefore, fintech platforms employ intelligent fraud detection mechanisms to mitigate the problem. The purpose of this study is to detect fraudulent activity using cutting-edge machine learning techniques on data obtained from the leading e-wallet platform in Turkey. After a comprehensive analysis of the dataset's features via feature engineering procedures, we found that the LightGBM approach had the highest detection accuracy of fraudulent activity with 97% in the experiments conducted. An additional key objective of reducing false alerts was accomplished, as the number of false alarms went from 13,024 to 6,249. This approach resulted in the establishment of a machine-learning model suitable for use by relatively small fraud detection teams.

INDEX TERMS E-wallet, fintech, fraud detection, LightGBM.

I. INTRODUCTION

Financial transactions have been revolutionized by the rise of fintech (financial technology) as a result of technological improvements, increased internet access, and consumer preference for easy and individualized financial services [1]. A total of $161 billion was invested worldwide in fintech in 2022, up from $60 billion in 2017 [2]. The global fintech business is expected to be worth $324 billion by 2026 [3]. Traditional ways of preventing fraud in financial transactions have been rendered ineffective by the expansion of fintech. The use of machine learning techniques has shown promise as a means of addressing this issue. These methods can be used to teach models to look for red flags in transaction data, such as unusual patterns or outliers. Overall, the expansion of fintech has opened doors to innovation and growth, but it has also brought forth new issues that necessitate the creation of more efficient fraud prevention solutions through the application of machine learning methods.

One form of increasingly popular fintech solution is the electronic wallet, sometimes known as a digital wallet. E-wallets provide a safe and simple way to perform financial transactions by allowing users to keep digital versions of their payment cards, loyalty cards, and other payment methods in one location. The proliferation of smartphones and other mobile devices, the increasing legitimacy of digital payments, and the demand for safer and more convenient methods of making transactions all contribute to the e-wallet's meteoric rise in popularity. Juniper Research predicts 4.4 billion e-wallet users by 2025, up from 2.6 billion in 2020 [4]. E-commerce, contactless payments, and mobile banking are driving this expansion. E-wallets are faster, cheaper, and

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

safer than traditional payment methods. E-wallets promote financial inclusion, especially in underdeveloped nations [5]. E-wallets and other forms of digital financial services have the potential to alleviate poverty and promote financial stability [6]. E-wallets allow non-banked people to make payments, save money, and perform financial activities.

The widespread adoption and sustained success of e-wallets depends on overcoming a number of challenges and potential issues, despite the technology's rising popularity. E-wallets pose a security risk due to their susceptibility to hacking, identity theft, and phishing assaults, among other forms of online fraud. The security-centered discussion mostly revolves around the issues associated with fraud detection within e-wallet systems. It is crucial to acknowledge that the domain of fraud prevention is witnessing a growing prominence of machine learning approaches. A comprehensive understanding of the landscape requires consideration of traditional approaches and state-of-the-art works that do not rely on machine learning. For instance, well-established methods like rule-based systems, anomaly detection, and expert systems have played pivotal roles in fraud detection [7]. Furthermore, recent advancements in fraud prevention, such as graph-based modeling [8] and behavior analysis [9], have demonstrated their effectiveness. Providers of electronic wallets should employ stringent safety measures including two-factor authentication, encryption, and fraud detection systems to protect their customers from these dangers [10]. Interoperability is another issue, as different e-wallet providers employ different standards and technology, making it hard to move funds between them. Open standards and protocols can improve interoperability between e-wallet systems [11]. To promote uptake, e-wallets must be easy to use. E-wallet adoption was strongly influenced by usability variables such as simplicity of use, utility, and enjoyment [12]. Finally, e-wallets must comply with anti-money laundering (AML) and know-your-customer (KYC) laws and regulations. E-wallet providers, financial institutions, and regulatory agencies must work together to comply with cross-border transactions. E-wallets have many benefits, but they also confront several problems that must be solved to assure their growth and success. These include security, interoperability, usability, and regulatory compliance.

The threefold contribution of our research is a solution to the problem of fraud detection, one of the most significant challenges in e-wallet systems.

- A fraud detection model utilizing the LightGBM technique has been successfully created, exhibiting a notable accuracy rate of 97% on a prominent e-wallet platform in Turkey.
- The objective of our technique is to effectively decrease the quantity of transactions identified as alerts, hence improving the operational effectiveness of enterprises who have limited resources for fraud detection. In the conducted studies, a significant reduction in the volume of alerts was seen, specifically from 13,024 to 6,249. This reduction resulted in a notable optimization of worker utilization, amounting to a 52% improvement.
- A decision support system has been developed specifically for high-traffic shopping days, such as Black Friday and Cyber Monday, when the extensive influx of client transactions can potentially overwhelm fraud detection teams. The utilization of this method offers significant support during periods of increased traffic, hence enhancing the efficacy of fraud monitoring.

The remaining sections are organized as follows. In Section II, studies on wallet-based fraud detection are reviewed. In Section III, the proposed model and the dataset used were introduced. In Section IV, the results and their effects are described in detail. In Section V, we interpret the results, and in Section VI, we conclude the paper.

II. RELATED WORK

Because of the explosive expansion of e-wallets, companies that provide financial services are becoming increasingly concerned about their ability to detect fraudulent activity involving wallets. Credit card fraud is a significant problem that already results in annual losses of billions of dollars. However, this has resulted in an increase in the number of cashless transactions as well as the likelihood of fraud due to the proliferation of mobile payment systems. Real-time alerts and transaction monitoring are necessities if one wishes to discover fraudulent activity in financial dealings as effectively as possible. Because of this, more advanced methods of detection are required. Real-time alert and transaction monitoring have been used for fraud detection increasingly in recent years, with traditional and machine learning-based approaches being used. Traditional techniques for detecting fraud include rule-based systems, statistical models, and expert systems, all of which use already-established rules and heuristics. However, these approaches may lack the flexibility necessary to detect and prevent new types of fraud as they emerge. As a result of its ability to automatically learn and adapt to changing patterns of fraudulent conduct, solutions based on machine learning show potential as a real-time alert and transaction monitoring for fraud detection in wallet-based transactions.

Rule-based systems [13] are frequently included in traditional approaches to fraud detection. These types of systems are dependent on a set of established rules and criteria in order to recognize fraudulent behavior [14]. These algorithms are constructed according to a specified set of rules, and their primary purpose is to recognize particular patterns or behaviors that are characteristic of fraudulent financial operations. These rules are designed to emphasize transactions that fulfill specific criteria. These rules can be based on a range of parameters, such as the amount of a transaction, how frequently it occurs, or where it takes place. Rule-based systems are helpful for detecting typical fraud schemes, but they have a blind spot when it comes to detecting innovative or evolving fraud schemes [15]. Rule-based systems are not good for detecting common fraud schemes. In addition,

because of the high rate of false positives produced by these systems, a sizeable percentage of legitimate transactions may be flagged for further investigation. This can lead to an increase in operational expenses as well as a loss in customer satisfaction. On the other hand, statistical models [7] make use of statistical methods like clustering and regression in order to locate aberrant patterns in the transaction data. For the purpose of detecting and preventing fraudulent behavior, expert systems [16] rely on information and expertise that are specific to their respective domains. When it comes to detecting and preventing fraud in real time, the financial industry has always relied heavily on the aforementioned traditional approaches. However, they have limits when it comes to detecting increasingly complicated and sophisticated fraud patterns. Traditional systems, despite the fact that they have a number of drawbacks, are nonetheless extensively used in conjunction with other, more cutting-edge methods such as machine learning and deep learning to provide a more comprehensive approach to the identification of fraudulent activity.

In contrast to more traditional approaches [13], machine learning-based solutions [17] have gained traction in recent years due to their capacity to automatically learn from data and adjust to shifting patterns of fraudulent conduct. This ability has contributed to the rise in popularity of these methods. Methods that are based on machine learning include both supervised and unsupervised learning algorithms. Examples of supervised and unsupervised learning techniques that are employed in machine learning-based approaches include artificial neural networks (ANNs) [18], decision trees [19], random forests [20], logistic regression [21], support vector machines [22], and k-nearest neighbors [23]. There has also been the successful use of deep learning algorithms [24], which is a type of machine learning, to the detection of fraudulent activity. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are two types of deep learning techniques that have recently shown promise for detecting fraudulent behavior in financial transactions. This is in addition to their applicability in image-based and sequential data recognition tasks. Real-time alerts and transaction monitoring in conjunction with algorithms that are based on machine learning are crucial components for achieving the most accurate identification of fraudulent behavior. On the other hand, in order to adequately train the models, these methods require a substantial amount of data, which may be difficult to get in the context of fraud detection. There must be a delicate equilibrium between the quantity of data collected and the precision of the resulting models.

It has been demonstrated that using techniques based on ML can improve the detection accuracy of fraudulent activity while simultaneously reducing the number of false positives and false alerts. A variety of machine learning-based methodologies have been investigated in the endeavor to achieve precise fraud detection. In the research carried out by Dheepa and Dhanapal [25], the classification of credit card fraud was handled by using a support vector machine (SVM) model. It was demonstrated that the SVM model significantly increased the system's ability to detect fraudulent activity while at the same time reducing the number of false positives. In a study on the detection of credit card fraud using a logistic regression model, Bayes, and kNN, Fayaz and Singh [21] found that the ML model was superior to traditional statistical methods due to its higher detection rates and lower false positive rates. This was due to the fact that the ML model had a lower rate of false positives. Rajora et al. [26] conducted a detailed comparative analysis of multiple machine learning algorithms, such as Random Forest, Support Vector Machines, and Neural Networks, in the context of credit card fraud detection. In a similar vein, Ge et al. [27] proposed a novel model that combines the advantageous features of XGBoost and LightGBM algorithms in order to improve the efficacy of fraud detection systems. Furthermore, there has been increasing adoption of sophisticated neural network topologies in order to enhance the capacities of fraud detection. In their study, Karthikeyan et al. [28] introduced a framework that employs a deep learning approach combined with a swarm optimization-based deep neural network. The objective of this framework is to accurately identify fraudulent patterns within transactional data. These findings provide evidence that machine learning models can be effective in reducing the number of false positives and increasing the accuracy of fraud detection.

In spite of the fact that the traditional approach to detecting fraudulent activities has, to some extent, been successful, research has shown that methods based on machine learning are far more effective in this regard. Machine learning models can detect trends and abnormalities in real time by making use of vast datasets and intricate algorithms [29]. This helps to reduce the number of false alerts [30] that occur while simultaneously boosting the accuracy of fraud detection. This is of utmost significance for financial institutions, since lowering the number of false alarms at these establishments can help save time and money, in addition to easing the frustration of their customers. In addition, technologies that are based on machine learning have the potential to produce more detailed statistical findings, which can assist financial institutions in gaining a deeper comprehension of the nature and features of fraudulent operations. Therefore, the development of detection approaches that are more accurate and efficient, such as those given by models that are based on machine learning, can play a key role in reducing the number of false alerts and enhancing the overall effectiveness of fraud detection systems.

III. METHOD

This study's methodology outlines how machine learning techniques can be used to identify fraudulent behaviors in e-wallet transactions. Here, we describe in depth the dataset used in the research, the machine learning algorithms utilized, and the data pretreatment strategies put into play before the dataset was analyzed. Furthermore, we detail how the

machine learning models are trained and the evaluation measures employed to rank their efficacy. This section's goal is to provide a high-level summary of the approach taken in this research to identify fraudulent activity related to e-wallet transactions.

A. DATASET

Within the dataset provided, there exists a collection of six notable companies that make use of the e-wallet service. In addition to Turkey, financial transactions to these wallets are also initiated from nations including Azerbaijan, Kyrgyzstan, and Turkmenistan. There are a total of 471,787 digital wallet transactions in the dataset gathered from United Payment during a period of four months. The majority of the 54 columns in the dataset are either not useful for the ML model or are used as identifiers. Each transaction in the dataset is assigned a status of "Not-Alarm,", "Alarm," "Risky," or "Fraud" depending on the criteria and analysis performed by the fraud detection team. The *Not-Alarm* transactions are those in which no suspicious behavior was uncovered by the rules, while the *Alarm* ones are the ones in which the rules uncovered suspicious behavior but the human review did not uncover any signs of fraud. The *Risky* label indicates that the fraud team deemed the alert to be legitimate and marked the transaction for future monitoring, while the *Fraud* label indicates that the fraud team confirmed fraudulent conduct. Figure 1 shows the breakdown of deals based on their intended total.

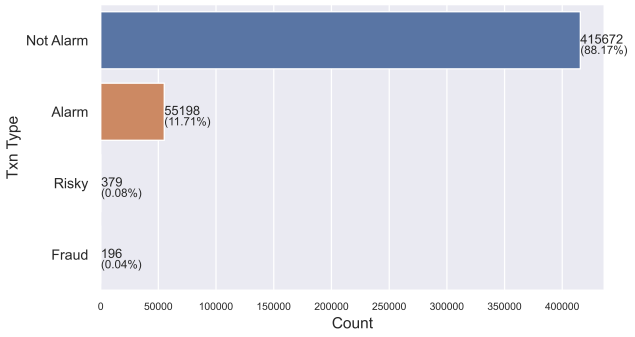


FIGURE 1. Distribution of classes in the dataset: Proportion of fraudulent and non-fraudulent instances.

B. PREPROCESSING

In order to make the most of the machine learning techniques, we preprocessed the original dataset, which we will refer to as $\mathcal{D}$. The matrix of n samples and p characteristics from the dataset can be represented as $\mathbf{X} \in \mathbb{R}^{n\times p}$. We used feature engineering methods to improve the features' prediction ability and record the wallet owner's activity over time. The following is an entire overview of our feature engineering methodology

Variable Selection: During the initial phase, the dataset is subjected to a process where nonusable columns are eliminated, resulting in a selection of 11 relevant columns from the original set of 54 columns. We eliminated features that were deemed non-usable, such as ID fields or those without importance for machine learning, in order to narrow our emphasis to a subset of pertinent columns.

Aggregation: In order to enhance the historical context of machine learning models, we conducted aggregation on the 11 selected features. The process of aggregation entails the condensation of historical transactions associated with a certain walletId, occurring within designated time intervals. The number of transactions in the last 24 hours, the number of unique walletId's that money was transferred to, sum of the transactions in specific transaction types in the last 3 days are some examples of the aggregations that are applied to create new features. The objective of this step was to identify and analyze patterns and trends within the data in order to facilitate the detection of fraudulent activities.

Feature Creation: The creation of characteristics was influenced by established rules and aggregations employed in fraud detection systems. Nevertheless, we took measures to include those features that were correlated with each other in the dataset, hence improving the predictive capability of the model.

To be more precise, we computed a number of statistical measures across specified time intervals and aggregated the corresponding columns. Let's call the aggregated feature matrix $\mathbf{X}' \in \mathbb{R}^{n\times q}$, where q is the new number of features. One definition of the aggregation function $g(\cdot)$ is as follows:

$$\mathbf{X}'_{ij} = g(\mathbf{X}_{ij_1}, \mathbf{X}_{ij_2}, \ldots, \mathbf{X}_{ij_k}) \tag{1}$$

The column indices utilized in the aggregate are $j_1, j_2, \ldots, j_k$, and $\mathbf{X}_{ij}$ represents the value of feature j for sample i. Depending on the type of feature and the information being sought, the function $g(\cdot)$ can take on a number of different shapes, including summing, averaging, and counting.

The dataset's missing values and outliers were fixed after feature engineering was completed. Depending on the severity of the missing values and their effect on the dataset as a whole, either imputation or deletion was performed. Extreme values that deviated greatly from the mean were identified as outliers such as transactions, and appropriate methods, were applied to remove them. We also used preprocessing methods to normalize the numerical features, making them scale correctly and work with machine learning techniques. So, the normalized feature matrix can be represented as $\mathbf{X}'' \in \mathbb{R}^{n\times q}$. Each feature was scaled using the function $f(\cdot)$.

$$\mathbf{X}''_{ij} = f(\mathbf{X}'_{ij}) \tag{2}$$

Standardization methods like min-max scaling and z-score normalization are examples of functions $f(\cdot)$ that can be used to map the values of each feature to a common range or distribution. We encoded categorical features like 'processStatus' and 'channelId' with suitable methods like one-hot encoding or label encoding, yielding a modified feature matrix $\mathbf{X}''' \in \mathbb{R}^{n\times r}$. The input for subsequent machine

learning algorithms is a refined and standardized feature matrix $\mathbf{X}'''$ that we obtained through these preprocessing stages.

C. SAMPLING

Imbalanced data is a common problem in fraud detection, where the number of samples in one class (such as fraud) is much smaller than the number of samples in the other class (such as non-fraud). There is a serious issue of class imbalance because the minority class (fraud cases) only accounts for 0.05% of the data in this set.

This imbalance raises critical concerns in effectively training a robust fraud detection model. To tackle this challenge, we have employed the Synthetic Minority Over-sampling Technique (SMOTE). SMOTE involves generating synthetic instances for the minority class by interpolating between existing instances, thereby augmenting its representation and mitigating the imbalance issue. This approach complements the concept of oversampling, whereas undersampling involves reducing instances of the majority class [31], [32]. SMOTE serves as a valuable strategy for addressing class imbalance within e-wallet datasets containing both fraudulent and non-fraudulent transactions. Consider a set of minority class instances $M = m_1, m_2, \ldots, m_n$, representing the fraudulent transactions. For each fraudulent transaction m_i, SMOTE identifies its k nearest neighbors, denoted as $NN(m_i) = n_1, n_2, \ldots, n_k$. To generate synthetic instances for fraud detection, SMOTE calculates the difference vectors between m_i and its neighbors:

$$\Delta m_{ij} = m_i - n_j, \quad for\ j = 1, 2, \ldots, k \tag{3}$$

The synthetic samples are subsequently generated through the process of interpolating the disparity vectors with the initial fraudulent transaction.

$$SyntheticSample_{ij} = m_i + \alpha.\Delta m_{ij}, \quad for\ j = 1, 2, \ldots, k \tag{4}$$

Within the given structure, the variable α is a stochastic quantity that assumes values between 0 and 1. This variable plays an essential role in determining the degree of interpolation between the value m_i and its neighboring values. The oversampling ratio, denoted as r, determines the quantity of synthetic samples that are produced for every fraudulent instance. The augmentation of fraudulent transaction representation in the dataset is achieved through the generation of synthetic samples. This process enhances the balance and effectiveness of the training environment for machine learning models used in e-wallet fraud detection. Subsequently, we employed the Synthetic Minority Over-sampling Technique for Nominal and Continuous (SMOTE-NC) technique, an extension of the SMOTE method, tailored for e-wallet datasets containing both categorical and continuous attributes. When dealing with categorical attributes, the SMOTE-NC algorithm replaces the continuous difference vectors, denoted as Δm_{ij}, with categorical vectors obtained from the mode of the nearest neighbors' categorical features. The implementation of this customized methodology guarantees that the fabricated instances in the e-wallet dataset preserve the distribution of both categorical and continuous characteristics.

D. PROPOSED APPROACH

The task of identifying fraudulent financial dealings can be expressed as a binary classification problem. Learning a classification function $f\theta : \mathbb{R}^d \rightarrow 0, 1$ that maps feature vectors to binary labels is the goal when given a dataset $\mathcal{D}$ of n labeled transactions, where $\mathbf{x}i$ is the feature vector for transaction i and y_i is a binary label indicating whether or not it is fraudulent. LightGBM, XGBoost, and Random Forest are three common machine-learning algorithms used for this purpose [27], [33], [34].

The LightGBM framework is a gradient-boosting method that uses decision trees. The main goal of the function utilized in binary classification is to minimize the binary cross-entropy loss. The loss function utilized in this particular situation measures the logistic loss by assessing the discrepancy between the predicted probability and the observed binary labels. The optimal parameters θ for a set of decision trees $T = T_j j = 1^J$ are learned by optimizing a differentiable loss function $L(y_i, f_\theta(\mathbf{x}i))$ with gradient descent, where J is the number of trees. To circumvent the limitations of histogram-based algorithms typically employed in other Gradient Boosting Decision Tree (GBDT) frameworks, the algorithm employs two techniques named Gradient-based One Side Sampling (GOSS) and Exclusive Feature Bundling (EFB). For each tree, GOSS employs one-sided subsampling to decrease the number of instances, whereas EFB groups together the most crucial characteristics for rapid computing.

Another gradient-boosting framework, XGBoost, combines several weak learners into one robust one. The logistic loss is utilized as an objective function for binary classification in this approach. The approach conforms to the notion of employing boosting to sequentially rectify mistakes committed by previous models. Overfitting is prevented and complex models are discouraged by optimizing a regularized objective function $Obj(\theta)$ that combines a loss function $L(y_i, f_\theta(\mathbf{x}i))$ and a regularization term $\Omega(\theta)$. The method learns several decision trees, $T = T_j j = 1^J$, from different parts of the data and then uses the average of their predictions to draw conclusions about the whole.

The Random Forest approach for machine learning creates a forest of interconnected decision trees. Each tree in the forest performs a classification, and then casts a vote for the final classification conclusion. In contrast to other approaches, this method does not employ an explicit objective function. Instead, it prioritizes the reduction of variance and the improvement of generalization by aggregating the outputs of several decision trees. In order to minimize error and avoid overfitting, the algorithm employs a bootstrap aggregating (bagging) strategy to randomly select parts of the data and features.

This research intends to train several machine learning algorithms using processed e-wallet data to reduce the frequency of false alarms while still detecting practically all fraudulent transactions that may be detected by typical rule-based systems. It is possible to find the sweet spot between recall and false positive rate by using machine learning models to evaluate the risk that a given transaction is fraudulent.

IV. RESULTS

In this section, we give the results and outcomes of the experiments that were carried out to test and assess the performance of the machine learning models. These experiments were carried out in order to test and evaluate how well the machine-learning models worked. To be more specific, the models were tested with the help of the digital wallet transactions that took place over the course of the most recent thirty days. During this evaluation, the goal was to determine whether or not the models were successful in detecting fraudulent transactions while also reducing the number of false positives. Both under sampling and over sampling techniques are utilized on the training set to find the best performant one for the data. Random under sampling obtained a better result than SMOTE method on ROC AUC, precision and recall metrics. Based on the results, only random under sampling technique is employed on the training set to reduce imbalance in the data, allowing machine-learning models to learn better, while the test set is left as is to strictly represent the production environment. The finest sampling ratio for random under sampling is determined as 1:15, which indicates that 15 legitimate transactions will be included in the set for each fraudulent transaction.

A. PERFORMANCE EVALUATION OF PROPOSED MODEL

After evaluating the machine learning algorithms, it was determined that LightGBM performed the best, with a ROC AUC score of 0.99 and the lowest number of false positives. The ROC AUC score evaluates the performance of a classifier model based on its ability to differentiate between positive and negative classes. A score of 1 represents flawless performance, whereas a score of 0.5 represents random guesswork. The ROC curve compares the true positive rate (sensitivity) to the false positive rate (1-specificity), and its area under the curve (ROC AUC) is used to summarize the model's performance. Noteworthy is the observation of a false positive score of 6218 for LightGBM. False positives are an important fraud detection metric because they represent legitimate transactions that are incorrectly flagged as fraudulent, causing consumer inconvenience and frustration. Therefore, it is essential to minimize false positives while detecting the maximum number of fraudulent transactions. The Random Forest approach demonstrates a marginally higher ROC AUC score in comparison to the Multi-layer Perceptron (MLP) model. The MLP model has higher performance compared to the RF method, as evidenced by its ability to produce 1,377 fewer false positives. The Support Vector Machine (SVM) and XGBoost algorithms exhibit a high degree of concordance in their ROC AUC scores. In contrast, the support vector machine (SVM) model has a higher level of accuracy in predicting an extra fraudulent transaction while also exhibiting a lower incidence of false positives when compared to the XGBoost model. On the other hand, the LR model has the least favorable performance when compared to the other six algorithms across all criteria. The number of false positives obtained from the LR model is notably higher than that of the rule-based method. This implies that the suitability of utilizing this model as a replacement for rule-based systems may not be suitable for this study. Table 1 provides a comprehensive comparison of the ROC AUC, TP, FP, TPR, and FPR for each of the six algorithms. The results demonstrate the efficacy of machine learning in detecting fraudulent transactions and emphasize the significance of selecting the optimal algorithm for the particular task at hand.

TABLE 1. An assessment of machine learning models for fraud detection, focusing on the evaluation metrics of ROC/AUC, TP, FP, TPR, and FPR.

Model Name	ROC/AUC	TP	FP	TPR	FPR
XGBoost	0.97660	30	9817	0.9375	0.0668
LightGBM	0.98571	31	6218	0.9687	0.0423
Random Forest	0.98087	30	9252	0.9375	0.0629
Logistic Regression	0.96597	30	13242	0.9375	0.0901
MLP	0.97935	30	7875	0.9375	0.0536
SVM	0.97726	31	9377	0.9687	0.0638

For further inspection of LightGBM's performance in fraud classification, the confusion matrix in Figure 2 provides valuable insights. Among the total of 146,894 non-fraudulent transactions, LightGBM accurately identifies 140,676 as non-fraudulent, while incorrectly classifying 6,218 transactions as fraudulent, leading to the generation of false alarms. Additionally, LightGBM correctly identifies 31 out of the 32 fraudulent transactions as fraudulent. Examining the confusion matrix, we note that the total number of alarms triggered by LightGBM for the test dataset amounts to 6,249, which is 52% lower than the 13,024 alarms produced by the rule-based system for the same transactions.

In the present study, the efficacy of machine learning models is evaluated by manually establishing a fraud threshold value. The machine learning models assign a probability between 0 and 1 to each transaction input as to whether it is fraudulent or not. If the predicted probability of fraud is less than the threshold value, the transaction is classified as fraudulent and an alert is generated. If the predicted probability of fraud is below the threshold value, the transaction is considered legitimate. By adjusting the threshold value, it is possible to obtain a balance between the true positive rate (TPR) and the false positive rate (FPR).

In this manner, we evaluated the model using a threshold value of 0.15, which was chosen to detect as many fraudulent transactions as feasible while maintaining a manageable number of false positives. A higher threshold value, such

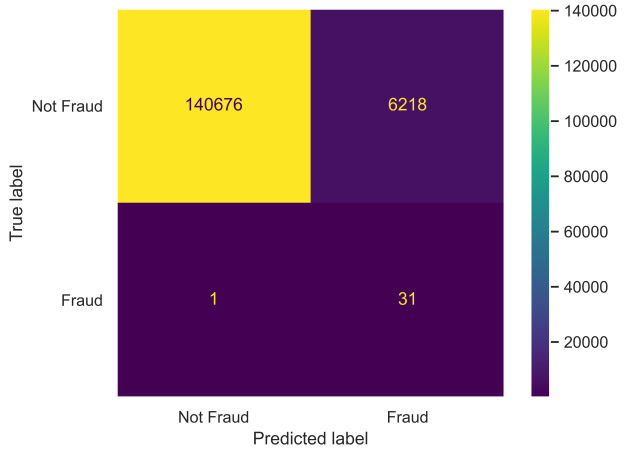


FIGURE 2. Confusion matrix of LightGBM.

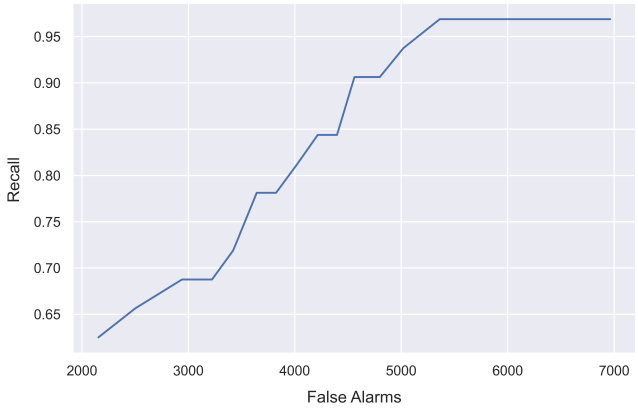


FIGURE 3. Trade-off analysis between recall and false alarms: Maximizing recall with reduced false alarms.

as 0.30, would reduce the number of false alarms, but it could also result in the misclassification of some fraudulent transactions. Thus, the choice of the threshold value is crucial for achieving a balance between the detection of fraudulent transactions and the number of false positives.

B. IMPACT OF THE PROPOSED ML-BASED APPROACH ON REDUCING FALSE ALERTS

In terms of reducing false alarms and expediting the fraud detection process, the proposed method has demonstrated remarkable efficacy. The top-performing model, LightGBM, effectively reduced the number of false alarms by 52%, from 13,024 to 6,249, while maintaining a high detection rate of 97% for rule-based system-identified fraudulent transactions. This substantial reduction in false alarms directly reduces the burden of fraud analysts, as they are no longer required to examine a large number of false alerts. The saved personnel can be reassigned to other crucial duties within the fraud analysis team, thereby enhancing the operational efficiency of the organization as a whole.

In addition, the ML-based approach allows for the dynamic adjustment of the threshold value, which is advantageous during peak purchasing periods with a high volume of transactions. By adjusting the threshold appropriately, the system can effectively manage the number of generated alarms, ensuring that all alarms can be comprehensively examined by fraud analysts. As depicted in Figure 3, this dynamic threshold adjustment establishes a balance between the precision of generated alarms and the detection of actual fraudulent transactions.

Comparing the proposed ML-based system to the traditional rule-based method, the proposed system requires less time investment. The design and development of rules for fraud detection requires considerable time and effort from the fraud teams. Using specialized fraud tools, they must analyze a large number of fraudulent transactions, identify recurring patterns, and manually construct rules and aggregates. In addition, this rule formulation process must be repeated periodically to ensure that the rules remain current and effective at detecting new fraud patterns. In contrast, the ML-based system requires minimal time investment for periodic training with new data, drastically reducing the maintenance and update efforts of rule-based systems. In comparison to traditional rule-based systems, the ML-based approach not only accomplishes a substantial reduction in false alarms, but also provides greater fraud detection flexibility, scalability, and efficiency.

C. STATISTICAL ANALYSIS OF FRAUDULENT BEHAVIOR

To acquire insight into the patterns and characteristics of fraudulent behavior, the dataset was subjected to a comprehensive statistical analysis. The analysis sought to identify significant variables and trends that differentiate fraudulent from legitimate transactions. Statistical methods were utilized to analyze the dataset and identify meaningful patterns. To comprehend the distribution and central tendency of the data, descriptive statistics, including mean, median, standard deviation, and percentiles, were computed for relevant variables. Inferential statistics were employed to investigate the relationships between various factors and fraudulent cases. The experiment disclosed a number of noteworthy findings regarding fraudulent behavior. First, it was observed that fraudulent transactions typically involve larger amounts than legitimate transactions. The mean and median transaction amounts for fraudulent transactions were substantially higher than those for legitimate transactions, indicating a possible indicator of fraud. In addition, hypothesis tests and correlation maps were utilized to explore these associations. The results of the hypothesis tests indicated that transaction amount and channel ID have a high correlation with fraudulent cases acquiring p-values from the tests $2.089e-179$ and $1.902e-05$, respectively. However, the correlation maps revealed that the independent variables demonstrated relatively weak associations with the dependent variable. To further explore the potential influence of time, additional features were created to indicate whether transactions occurred during the

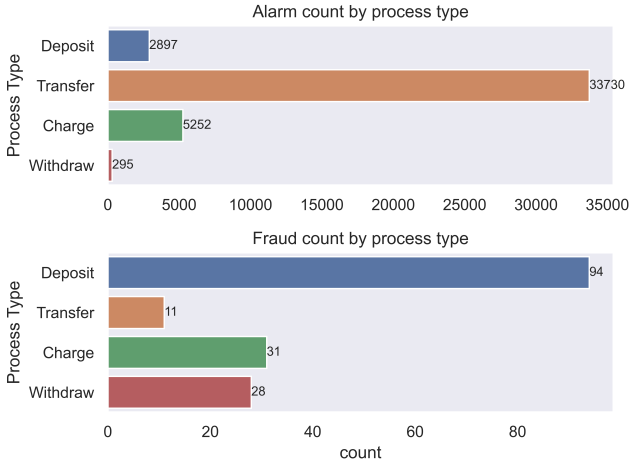


FIGURE 4. Fraud alarm distribution by process type: Analysis of deposit, transfer, charge, and withdrawal processes.

daytime or nighttime, weekdays or weekends. Nevertheless, the analysis did not uncover any significant relationship between the timing of transactions and their likelihood of being fraudulent by obtaining p-values of 0.36 and 0.60. Subsequently, the study focused on exploring the relationship between process types and fraudulent transactions. Figure 4 illustrates the distribution of process types based on the frequency of fraudulent transactions. Notably, the deposit process exhibited the highest number of fraudulent cases, despite the transfer process generating the highest number of alarms.

V. DISCUSSION

A. MAIN FINDINGS

Fraud teams are specialized departments within businesses who look for and deal with fraud in all its forms. In order to prevent monetary losses, reputational harm, and legal responsibilities, these groups use a wide variety of strategies and techniques. Several fundamental parts are usually required for their operations to succeed. To begin, they perform risk assessments to spot potential weak spots and plan for their protection. Second, they put into place cutting-edge fraud detection systems that make use of analytics, machine learning, and rule-based engines to spot anomalous behavior. Thirdly, they employ techniques like anomaly detection and behavioral analysis to keep tabs on all accounts, transactions, and user activity in real-time. As a fourth precaution, they set up solid fraud prevention policies and procedures. Finally, in cases where fraud is suspected, special teams are tasked with conducting in-depth investigations, collecting evidence, and analyzing transactional data in order to construct a solid case. Overall, fraud teams are crucial to the security of businesses, their assets, and the confidence of their stakeholders.

In order to provide context, the primary findings of the study reveal that a model developed using the LightGBM technique achieved a notable accuracy rate of 97% in the identification of fraudulent activities within the United Payment e-wallet platform, a widely recognized digital payment service in Turkey. In addition, the approach effectively reduced the number of alerted transactions, resulting in a 52% reduction in the workforce required for fraud detection. This decrease in false positives demonstrates the model's ability to distinguish between genuine and fraudulent transactions, thereby increasing the efficacy of organizations with limited fraud teams. In addition, the development of a decision support system for peak shopping days addresses the difficulties encountered by fraud teams during periods of high transaction volume, allowing for the prioritization of suspicious transactions. Overall, these results demonstrate the model's efficacy in detecting fraud, its potential for resource optimization, and its contribution to improving fraud prevention strategies for e-wallet platforms.

B. THREATS TO VALIDITY

To ensure that research findings can be relied upon and applied to real-world situations, their validity is essential. However, all studies are subject to threats to their validity, which can affect the precision, dependability, and generalizability of the results [35]. In this subsection, we discuss the internal and external validity threats that may have affected the results of our study on the wallet-based transaction fraud prevention approach. We identify and address potential limitations and confounding factors that may have affected the validity of our findings, and we propose ways to mitigate these threats in order to improve the robustness and generalizability of our findings.

1) INTERNAL VALIDITY

The model's accuracy may be biased because it was trained and tested using data related to electronic wallet transactions that isn't necessarily representative of the community at large. Electronic currency exchanges are case-specific and can't be used universally. The model could have been overfit to the training data, which would explain why it performed well on that data but poorly on novel data. We used a separate 28-day dataset for validation, distinct from the one used for training, to get eliminate such concerns. Thus, the outputs of the model may not be generalizable and the assessment dataset may be too small to provide statistical significance.

2) EXTERNAL VALIDITY

It is possible that the model's performance will not migrate to other platforms due to changes in user behaviors, transaction patterns, or fraud schemes between regions and nations, despite the fact that it was built and tested on a single e-wallet platform in Turkey. From the deployment in the real-world perspective, the model's performance may vary in the real world due to unforeseen shifts in data distribution or fraud trends, or due to constraints in the system's implementation or integration with other security measures. And finally, the model's performance may change over time as fraudsters

adopt new strategies to circumvent detection or as new fraud schemes develop, necessitating periodic updates and retraining.

VI. CONCLUSION

Threats including phishing, malware, and social engineering can jeopardize the privacy, availability, and security of a user's electronic wallet and the money it contains. As a result, fintech platforms are making use of sophisticated fraud detection tools to lessen the impact of such incidents. The goal of this research is to utilize state-of-the-art machine learning algorithms to identify fraudulent behavior in data collected from the most popular e-wallet service in Turkey. LightGBm was found to be the most effective method through feature engineering and experimental analysis, with a 97% detection rate and ROC AUC score of 0.9857. The primary goal of the study was to reduce false alerts, which it did successfully, cutting the overall number of alarms from 13,024 to 6,249. These findings demonstrate the promise of machine learning-based approaches for detecting fraudulent activity in e-wallets and the ways in which they can supplement limited resources dedicated to this task. This study does have some caveats, though. Further study is required to determine the generalizability of the findings to other platforms and areas, as the dataset employed was restricted to a single e-wallet platform in Turkey. Furthermore, the study only looked at machine learning-based approaches, thus there is a need for more research into the efficacy of older methods for detecting fraud in electronic wallets. But the study's results are encouraging, and they add to the expanding body of knowledge on spotting fraud in cashless transactions. To better detect fraud in e-wallets and other cashless transactions, future research should continue to investigate the efficacy of machine learning-based technologies and classical methods.

REFERENCES

[1] E. S. Prasad, *The Future of Money: How the Digital Revolution is Transforming Currencies and Finance*. Cambridge, MA, USA: Harvard Univ. Press, 2021.

[2] Statista Report. *Total Value of Investments Into Fintech Companies Worldwide From 2010 to 2022*. Accessed: May 14, 2023. [Online]. Available: https://www.statista.com/statistics/719385/investments-into-fintech-companies-globally/

[3] *Fintech Market to Reach $324 Billion in 2026*. Accessed: May 14, 2023. [Online]. Available: https://www.globaltrademag.com/fintech-market-to-reach-324-billion-in-2026/

[4] *Digital Wallet Users to Exceed 4.4 Billion Globally by 2025*. Accessed: May 14, 2023. [Online]. Available: https://www.juniperresearch.com/press/digital-wallet-users-to-exceed-4-4-billion-by-2025/

[5] R. Rasheed, S. H. Siddiqui, I. Mahmood, and S. N. Khan, "Financial inclusion for SMEs: Role of digital micro-financial services," *Rev. Econ. Develop. Stud.*, vol. 5, no. 3, pp. 429–439, Jul. 2019.

[6] M. A. Hassan and Z. Shukur, "Review of digital wallet requirements," in *Proc. Int. Conf. Cybersecur. (ICoCSec)*, Sep. 2019, pp. 43–48.

[7] Y. Kou, C.-T. Lu, S. Sirwongwattana, and Y.-P. Huang, "Survey of fraud detection techniques," in *Proc. IEEE Int. Conf. Netw., Sens. Control*, vol. 2, Mar. 2004, pp. 749–754.

[8] E. Kurshan and H. Shen, "Graph computing for financial crime and fraud detection: Trends, challenges and outlook," *Int. J. Semantic Comput.*, vol. 14, no. 4, pp. 565–589, Dec. 2020.

[9] R. Rieke, M. Zhdanova, J. Repp, R. Giot, and C. Gaber, "Fraud detection in mobile payments utilizing process behavior analysis," in *Proc. Int. Conf. Availability, Rel. Secur.*, Sep. 2013, pp. 662–669.

[10] E. Hopalı, Ö. Vayvay, Z. T. Kalender, D. Turhan, and C. Aysuna, "How do mobile wallets improve sustainability in payment services? A comprehensive literature review," *Sustainability*, vol. 14, no. 24, p. 16541, Dec. 2022.

[11] P. G. Schierz, O. Schilke, and B. W. Wirtz, "Understanding consumer acceptance of mobile payment services: An empirical analysis," *Electron. Commerce Res. Appl.*, vol. 9, no. 3, pp. 209–216, May 2010.

[12] S. Yuan, L. Liu, B. Su, and H. Zhang, "Determining the antecedents of mobile payment loyalty: Cognitive and affective perspectives," *Electron. Commerce Res. Appl.*, vol. 41, May 2020, Art. no. 100971.

[13] J. Kumar and V. Saxena, "Rule-based credit card fraud detection using user's keystroke behavior," in *Soft Computing: Theories and Applications*. Singapore.: Springer, 2022, pp. 469–480.

[14] A. Abdelhalim and I. Traore, "Identity application fraud detection using web mining and rule-based decision tree," *Int. J. Netw. Comput. Secur.*, vol. 1, no. 1, pp. 31–44, 2009.

[15] M. E. Edge and P. R. F. Sampaio, "The design of FFML: A rule-based policy modelling language for proactive fraud management in financial data streams," *Expert Syst. Appl.*, vol. 39, no. 11, pp. 9966–9985, Sep. 2012.

[16] L. Šubelj, Š. Furlan, and M. Bajec, "An expert system for detecting automobile insurance fraud using social network analysis," *Expert Syst. Appl.*, vol. 38, no. 1, pp. 1039–1052, Jan. 2011.

[17] H. Najadat, O. Altiti, A. A. Aqouleh, and M. Younes, "Credit card fraud detection based on machine and deep learning," in *Proc. 11th Int. Conf. Inf. Commun. Syst. (ICICS)*, Apr. 2020, pp. 204–208.

[18] R. B. Asha and K. R. S. Kumar, "Credit card fraud detection using artificial neural network," *Global Transitions Proc.*, vol. 2, no. 1, pp. 35–41, Jun. 2021.

[19] Y. Sahin, S. Bulkan, and E. Duman, "A cost-sensitive decision tree approach for fraud detection," *Expert Syst. Appl.*, vol. 40, no. 15, pp. 5916–5923, Nov. 2013.

[20] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random forest for credit card fraud detection," in *Proc. IEEE 15th Int. Conf. Netw., Sens. Control (ICNSC)*, Mar. 2018, pp. 1–6.

[21] F. Itoo and S. Singh, "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection," *Int. J. Inf. Technol.*, vol. 13, pp. 1503–1511, Aug. 2021.

[22] N. K. Gyamfi and J.-D. Abdulai, "Bank fraud detection using support vector machine," in *Proc. IEEE 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Nov. 2018, pp. 37–41.

[23] S. Nami and M. Shajari, "Cost-sensitive payment card fraud detection based on dynamic random forest and *k*-nearest neighbors," *Expert Syst. Appl.*, vol. 110, pp. 381–392, Nov. 2018.

[24] S. Sanober, I. Alam, S. Pande, F. Arslan, K. P. Rane, B. K. Singh, A. Khamparia, and M. Shabaz, "An enhanced secure deep learning algorithm for fraud detection in wireless communication," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–14, Aug. 2021.

[25] V. Dheepa and R. Dhanapal, "Behavior based credit card fraud detection using support vector machines," *ICTACT J. Soft Comput.*, vol. 2, no. 4, pp. 391–397, Jul. 2012.

[26] S. Rajora, D.-L. Li, C. Jha, N. Bharill, O. P. Patel, S. Joshi, D. Puthal, and M. Prasad, "A comparative study of machine learning techniques for credit card fraud detection based on time variance," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov. 2018, pp. 1958–1963.

[27] D. Ge, J. Gu, S. Chang, and J. Cai, "Credit card fraud detection using LightGBM model," in *Proc. Int. Conf. Internet Technol. (ECIT)*, Apr. 2020, pp. 232–236.

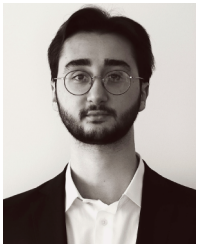
[28] T. Karthikeyan, M. Govindarajan, and V. Vijayakumar, "An effective fraud detection using competitive swarm optimization based deep neural network," *Meas., Sensors*, vol. 27, Jun. 2023, Art. no. 100793.

[29] R. A. A. Habeeb, F. Nasaruddin, A. Gani, I. A. T. Hashem, E. Ahmed, and M. Imran, "Real-time big data processing for anomaly detection: A survey," *Int. J. Inf. Manage.*, vol. 45, pp. 289–307, Apr. 2019.

[30] N. Mahmoudi and E. Duman, "Detecting credit card fraud by modified Fisher discriminant analysis," *Expert Syst. Appl.*, vol. 42, no. 5, pp. 2510–2516, Apr. 2015.

[31] G. Kovács, "An empirical comparison and evaluation of minority oversampling techniques on a large number of imbalanced datasets," *Appl. Soft Comput.*, vol. 83, Oct. 2019, Art. no. 105662.

[32] C.-F. Tsai, W.-C. Lin, Y.-H. Hu, and G.-T. Yao, "Under-sampling class imbalanced datasets by combining clustering analysis and instance selection," *Inf. Sci.*, vol. 477, pp. 47–54, Mar. 2019.
[33] E.-A. Minastireanu and G. Mesnita, "Light GBM machine learning algorithm to online click fraud detection," *J. Inform. Assur. Cybersecur*, vol. 2019, Apr. 2019, Art. no. 263928.
[34] J. T. Hancock and T. M. Khoshgoftaar, "Gradient boosted decision tree algorithms for medicare fraud detection," *Social Netw. Comput. Sci.*, vol. 2, no. 4, p. 268, Jul. 2021.
[35] A. Ampatzoglou, S. Bibi, P. Avgeriou, M. Verbeek, and A. Chatzigeorgiou, "Identifying, categorizing and mitigating threats to validity in software engineering secondary studies," *Inf. Softw. Technol.*, vol. 106, pp. 201–230, Feb. 2019.



CAN ISCAN is currently pursuing the B.S. degree in computer engineering with Istanbul Kültür University (IKU). He is a Data Scientist with FormicaAI. He is researching sensor fusion of camera and lidar data for object detection. His research interests include data science, deep learning, and computer vision.

OSMAN KUMAS (Member, IEEE) received the B.S. degree in computer engineering from Trakya University, in 2009. He is currently pursuing the master's degree in computer engineering with Bahcesehir University. He was a Computer Engineer with Nortel Netas and Turkcell. He started his managerial experience as a Software Development and Operations Manager with Netas, concluded his time there as the Director, and then a VP of Operations with Testinium. He is the Chief Operating Officer of FormicaAI. His current research interests include blockchain, machine learning, and cloud computing research.

FATMA PATLAR AKBULUT (Member, IEEE) received the B.S. and M.S. degrees in computer engineering from Istanbul Kültür University (IKU) and the Ph.D. degree in biomedical engineering from Istanbul University, in 2017. Her Ph.D. work focused on developing machine-learning-enabled wearable systems for long-term cardiovascular disease monitoring. She joined the Computer Engineering Department, IKU, in 2019, where she is currently the Department Chair of the Software Engineering Department, further contributing her expertise in the field. Before IKU, she was a Postdoctoral Researcher with the Computer Science Department and the Advanced Self-Powered Systems of Integrated Sensors and Technologies (ASSIST) Center, North Carolina State University (NCSU), from 2017 to 2019. Her research interests include biomedical signal processing, affective computing, data analytics, and wearable systems for healthcare.

AKHAN AKBULUT (Member, IEEE) received the B.S. and M.S. degrees in computer engineering from Istanbul Kültür University (IKU), Turkey, in 2001 and 2008, respectively, and the Ph.D. degree in computer engineering from Istanbul University, Turkey, in 2013. From 2004 to 2013, he was a Research Assistant with the Department of Computer Engineering, IKU, where he was an Assistant Professor, from 2013 to 2017. From 2017 to 2019, he was a Postdoctoral Researcher with the Computer Science Department, North Carolina State University, Raleigh, NC, USA. In 2019, he joined the Department of Computer Engineering, IKU, and was promoted to Associate Professor. He is currently the Chairperson of the Department of Computer Engineering, IKU. His current research interests include the design and performance optimization of software-intensive systems, machine learning applications, internet architectures, and broadening participation in cloud computing research.