Journal of Artificial Intelligence and Data Mining (JAIDM), Vol. 10, No. 1, 2022, 87-101.

Shahrood University of Technology

Journal of Artificial Intelligence and Data Mining (JAIDM)
Journal homepage: http://jad.shahroodut.ac.ir

Research paper

Customer Behavior Analysis to Improve Detection of Fraudulent Transactions using Deep Learning

Fereshteh Baratzadeh and Seyed Mohammad Hossein Hasheminejad*

Department of Computer Engineering, Alzahra University, Tehran, Iran.

Article Info

Article History:
Received 10 October 2020
Revised 17 July 2021
Accepted 06 January 2022

DOI:10.22044/JADM.2022.10124.2151

Keywords:
Fraud Detection, Deep learning, Machine Learning, Generative Adversarial Network, Short Term Memory Network, Data Mining

**Corresponding author: f.baratzadeh@student.alzahra.ac.ir (F. Baratzadeh).*

Abstract

With the advancement of technology, the daily use of bank credit cards has been increasing exponentially. Therefore, the fraudulent use of credit cards by the others as one of the new crimes is also growing fast. For this reason, detecting and preventing these attacks has become an active area of study. In this work, we discuss the challenges of detecting fraudulent banking transactions, and present solutions based on deep learning. The transactions are examined and compared with the other traditional models in fraud detection. According to the results obtained, the optimal performance is related to the combined model of deep convolutional networks and short-term memory, which is trained using the aggregated data received from the generative adversarial network. This paper intends to produce sensible data in order to address the unequal class distribution problem, which is far more effective than the traditional methods. Also, it uses the strengths of the two approaches by combining the deep convolutional network and the long short-term memory network in order to improve the performance. Due to the inefficiency of the evaluation criteria such as accuracy in this application, the measure of distance score and the equal error rate are used to evaluate the models more transparent and more precise. The traditional methods are compared with the proposed approach in order to evaluate the efficiency of the experiment.

1. Introduction

With the astonishing growth of e-commerce over the past decade, the credit cards are now the most common solution for online payment and open the door to different kinds of fraud. Consequently, one of the most critical subjects for all credit card issuers and online transaction management agencies is effective fraud detection solutions to reduce losses and increase customer confidence. The advanced fraud detection systems use sophisticated analytics and data mining techniques in order to identify suspicious transaction logging patterns, where illegal transactions tangle with the legal ones. It requires the viewer to understand extensive datasets and perform binary classifications to detect fraudulent or abnormal transactions from legitimate cases. Machine learning is very effective in addressing this challenge, particularly the peer-to-peer learning techniques. The pre-classified datasets include tagged transactions for class instruction that enable a recognition model to detect unusual transactions among the everyday transactions. On the other hand, the static machine learning approaches will not work if they cannot adapt to the new fraud patterns [1]. According to the Nilsson's report, losses to fraud in 2018 increased by 19.7% from 2017 [2].

The fraudulent approach to anonymity is constantly changing so standard tools to detect fraud such as using rules set by knowledgeable people are not sufficient. They behave somehow that their actions appear natural, making it difficult to detect fraud [3].

There is also the need for an expert to oversee and analyze the transactions classified as fraudulent for a final judgment, and also a control process defining the actions required in contrast to the fraudulent transaction. In this article, the transactions in the database are examined offline. If it is necessary to check the transactions online, the foundation of this matter should be performed according to the volume of data at the time of the transaction with a suitable execution time. These issues can be explored in a future work. Also since it is a matter of recognizing the customer behavior pattern if a transaction is fairly similar to the customer patterns, the system does not recognize it as fraud. In that case, transaction prevention should be done by the usual authentication and authorization system applied by the banks. The following are some of the challenges of credit card fraud detection that this article tried to resolve.

• Lack of access to actual datasets [4], [5].
• Unbalanced dataset [6], [8], [56], [34], [11].
• Bank transaction database problem analysis [9], [11], [34], [56].
•Determination of appropriate evaluation parameters [10], [14].
• Dynamic behavior of fraudsters [11].

In this paper, [12], [13] are used to solve the dataset imbalance problem.

We found that a reasonable data balancing could improve the result of the application. Therefore, we employed the generative adversarial network to fix the problem and generate the data from the original dataset. For processing the raw dataset, we used the feature engineering methods. We knew that the influential features were more effective in achieving the results. Thus we extracted appropriate dependencies from the raw data as new features. Then we used them as the input of our networks. We used C-LSTM to get the best possible result. We also found that the traditional evaluation criteria such as accuracy in this application were insufficient. Therefore, we employed the distance score criterion and equal error rate to evaluate the models accurately and comprehensively. Afterward, we performed experiments for assessing the performance of the proposed methods in comparison to the traditional methods.

The remainder of the paper is organized as what follows. The second section provides a literature review of the credit card fraud and deep learning. The third section presents the proposed methods of this paper to tackle the problems and challenges. In the fourth section, the results of the empirical analysis are reported based on the real-life datasets. Finally, the conclusions and future works are summarized.

2. Literature Review

2.1. Related Works

In the last few years, there have been a variety of uses of machine learning techniques in fraud detection, as in [19]. There are also various obstacles to fraud detection modeling associated with the disparity of data available. The factors like feature selection, real-time response problems, and discovery of the most appropriate approach should be considered [20], [21], [22]. The influential features are effective in achieving the results [6]. In order to obtain an advanced model and features in the transaction data such as time, amount, location, and customer account balances, we require their behavioral attributes to spend [23]. An article with the standard modeling approach to customer behavior is described in [24], which defines a transactional aggregation method for modeling the customer behavior.

To be accurate in the operations, to speed up the detection of fraudulent behavior, and to cover different aspects of customer behavior, we need more parameters, which are derived from the current raw variables. As a result, the current raw variables over the period and feature extraction are done based on the account, transaction type, terminal type, transaction location, etc., and such as the account balance, total amount spent, and number of transactions. The following papers have used this subject: [20], [25], [6], [26], and [27].

In addition to the variables of each transaction, the aggregate variables analyzed for the customer behavior over some set times are extracted. Therefore, a combination of the new variables will exist. The value of each variable is calculated from the historical variable by modeling the behavior of these variables and using a method to detect the anomalies with the transaction occurring and comparing with the previous cases and expressed in the numerical form between zero and one. That indicates the risk of differentiation from the former customer behavior.

The proposal of Syeda *et al*. [19] is to apply parallel neural networks. The purpose of this procedure is to advance the data mining and knowledge learning process. Maes *et al*. [28] have explained that the Bayesian belief networks provide better results in detecting fraudulent transactions. Also the actual detection process with artificial neural networks is much quicker. The neural network-based approaches are

generally compact but not accurate enough, and the retraining neural networks is challenging.

Chen *et al*. [29] have used an online questionnaire to collect the user transaction response data from the users. Also it uses a support vector machine trained with this data, and the response-transaction models are used to predict new transactions. Chen *et al*. [30] have lately proposed a personalized approach by applying the support vector machines and artificial neural networks. It is an attempt to prevent fraud for the users even without any transaction information. However, these systems are not fully automated, and depend on the level of the user knowledge.

Chan *et al*. [31] have classified a comprehensive collection of transactions in small subsets, and later used the distributed data mining to build models of the user behavior. It then applies models, and is made to create a hybrid classification to improve the detection accuracy.

Brause *et al*. [32] have studied the probability of the merging high-level data mining techniques and neural networks to detect fraud in banking transactions. Chiu and Tsai [33] have improved the application of data mining concerning web services to exchange information among banks. Fraud pattern mining is an algorithm extracted from the association rule mining communication that provides information about the features of fraudulent transactions. The banks are using new fraud models to block attacks by developing their original fraud detection systems.

Eshghi *et al*. [11], using a multi-criteria decision-making approach, intuitive fuzzy set, and reasonableness verification, have introduced a new method for fraud detection, showing several behavioral pieces of evidence of a transaction affecting uncertainty.

Zhang *et al*. [34] have studied the offline training model. The training dataset was sampled from the past transactions over given times (different periods) in the data storehouse. They used feature engineering based on a framework described as HOBA[1] in order to receive attribute variables for the statistical model. Then a deep learning model was extended to detect credit card fraud. After the training, the model was employed in the online fraud detection system to measure the suspected credit card transactions in real-time. An attribute can be a category based on a particular feature or it can be a category based on the human laws. For example, if the input state is a POS transaction, that was inserted through a magnetic stripe. Therefore, it has a magnetic input state characteristic. The behavior of the transaction with the magnetic input state characteristic separately analyzes its value. Heryadi *et al*. [15] have examined a model to study the short-term and long-term patterns from an Indonesian transactional dataset.

This paper aimed to analyze the customer behavior and the impacts of return activities after online shopping. The dataset was a questionnaire obtained from two cities. In order to solve this issue, they developed a framework to consider the possibility of return after shopping. Structural equation modelling[2] was employed to describe the relationships between the potential and observed variables based on interpreting certain variables [52]. Kim *et al*. [36] have presented a rule-based expert system to detect the fraud telecommunications network of an organization. They produced rules with the help of expert knowledge and applying data mining methods. Kanavos *et al*. [37] have used the data mining methods on a predictive model based on each customer's behavior. The purpose is to classify the customers in addition to products. Subsequently, the intent was to recommend new products to the customers based on their consuming behavior. The rules were applied to the dataset to obtain information about the customers' behavior. They applied the vector space model for the expression of text documents as vectors. Also, they used apache spark for programming. Furthermore, the selected evaluations were the TP rete, FP rate, precision, recall, and F-measure metrics.

The time response is critical to obtain an efficient IoT. This article aimed to reduce the response time of systems and the cost of energy-consuming when heavy network traffic. The study examined the problems such as minimizing the network traffic by searching for the shortest path to the destination. They studied the Ant Colony (ACO) algorithms compared to the K-means clustering algorithms to find the shortest path. The results obtained represented that in this area, ACO was more efficient [7]. Nematzadeh *et al*. [53] have studied noise detection and classification. They compared the selection of classifiers for detecting the noisy instances. Then the noise classes were produced as Strong Noise (SN) and Weak Noise (WN). Next, the calculating distance by the Euclidean distance formula was conducted.

[1] Homogeneity-Oriented Behavior Analysis

2 SEM

Finally, the 10-nearest neighbor was applied to each class of noise-free sets for classification.
The purpose is to help the vendors to be informed about the customer behavior. They presented a method to estimate the customer internet usage for online shopping activities and the amount customers spend online. Then for analyzing the customer behavior, the regression method was applied [54].
Pejhan *et al*. [60] studied improving automatic text recognition from the picture using the GAN network.

2.2. Feature Engineering

As mentioned earlier, feature engineering has a significant impact on the fraud detection performance. The former research works have essentially focused on the transaction aggregation approaches in feature engineering. Each time a transaction occurs, the attribute variables are calculated based on the past transactions during the set period. Two strategies, aggregation of transactions and rule-based expert system, were used that realized the homogeneous orientation behavior analysis and extracted the attribute variables in the historical transaction data [34]. Also, in [23], [34], and [11], the feature engineering methods have been used.
Mohamad *et al*. [56] have studied attribute selection in big datasets. They presented a parameterization method to generate the optimal attribute set when there is no suitable model to use as a guideline. In conclusion, they used the Best First Search (BFS) algorithms and correlation-based feature selection (CFS) to obtain the most optimized attribute. Then the highest attribute was identified and added to the attribute set.
Razooqi *et al*. [51] have modeled the history of customer transactions. Next, the data was categorized into attributes. The difference between the neural network and fuzzy logic algorithms were examined. The output was organized into legal, suspicious, and fraud transaction.

2.3. Concept Drift

The concept drift occurs due to the changes in behavior, the characteristics of legitimate users or the creative actions of a fraudster. Anomaly detection is very suitable for a network security domain, especially network intrusion detection [35]. It is related to preventing telecommunications fraud or detecting an attacker's impersonation in the mobile system. The data mining techniques are applied to observe the movements of financial transactions such as credit cards and internet banking to inform the potential frauds [38], [39], [40]. Therefore, the training models must have a mechanism for a continuous performance recognition and adapt to data changes over time. In data mining, machine learning and predictive analysis of unexpected improvements in data distribution across time are called concept drift [41], [42], [43], [44].
In pattern recognition, this phenomenon is known as a correlation shift or shift [42]. In signal processing, this phenomenon is dynamic [45]. The changes in primary data might be due to the changes in personal interests, population changes, enemy activities or related to the complex nature of the environment. Priya *et al*. [55] have studied the factors affecting the handling of concept drift approaches on imbalanced datasets.
Analysis of multiple imbalanced datasets with concept drift has been examined. The main challenge of this project was online learning. The results obtained showed that the ensemble-based methods presented a more reliable accuracy.
Integration of the concept drift detection methods concerning the nature of data was more efficient [57]. Incremental learning can be more effective in the fraud detection environments [58].

3. Current Challenges and Research Gaps

The purpose of this article is to present an optimal method for financial fraud detection. As mentioned earlier, some challenges are required to be discussed.

3.1. Imbalanced Data Problem

One strategy to solve the problem of an imbalanced dataset is to reduce the discrepancy between the classes. It is implemented by sampling the majority class in a training set [46] and accidentally delete some of the majority class cases, assuming that redundancy in the data causes such elimination not to interfere with the classification objectives.
Dal Pozzolo *et al*. [49] have examined the tendency created by under-sampling. In [10], the minority class over-sampling by replacing the minority samples has been performed in the dataset. The disadvantage of such a strategy is that it does not add informative content, thus limiting the ability of the classifier to improve for generalization. In order to overcome this difficulty, the minority class uses more artificial sampling techniques to produce the synthetic samples along the line between the minority

samples and their nearest neighbors. The weakness of SMOTE[3] is that there are too few samples of the minority class for a model to effectively learn the decision boundary. Therefore, it increases the likelihood of creating new examples incorrectly around the majority class. This problem is manageable by the safe-level SMOTE method. It will develop the clusters around every minority observation. The main idea of safe-level SMOTE is to produce synthetic samples at a safe level in a secure area [50]. SMOTE has created several different types including Border-SMOTE, which analyzes the synthetic samples along the boundary among classes. The safe-level-SMOTE algorithm also runs across a dataset, and places the synthetic samples in the overlap area near the safe zone. Accordingly, these examples scatter in a region. In [12], they have pursued the same goal, specifically rebalancing a training set by injecting valid samples for the minority class. Thus there is no simple sampling of the minority class. Instead, the task of generalization of the minority class samples is delegated to a productive hostile network, which has shown a positive performance in producing valid samples. Besides, no data will be deleted from the training set.

3.2. Inequality Problem

As mentioned earlier, the data attributed to the fraudulent transactions is insignificant so it is difficult to establish a structure for detecting fraudulent transactions from the genuine ones. Therefore, many methods have been used to solve this problem in a related work, which generally fall into three general categories.

3.2.1. Under-sampling of Majority Class Data

Since the imbalanced datasets lead to one model of instruction, deleting part of the majority class data may aid the learning process and prevent the majority of data from being oriented to one class. Although this method dramatically reduces data inequality due to the removal of part of the available data, the performance of the trained model is less than ideal, although it may slightly increase the accuracy of the minority detection, and significantly reduce the accuracy of the majority class detection. On the other hand, not all the modeling approaches necessarily address the problem of one-way training [49].

[3] Synthetic Minority Over-sampling Technique

3.2.2. Valuation of Minority Class

The inaccurate categorization of the minority class (fraudulent transaction) can cost more than the majority class (normal transaction). Different valuations of the minority class in the practical training of this data can increase, and the accuracy of the minority data recognition can improve [10].

3.2.3. Increase Minority Class Data through Generative Adversarial Networks

Another approach to counteract the imbalanced data is to use the generative methods to produce the minority data. Due to the weakness of the previous approaches, this method can generate new artificial data. Among the traditional and modern methods for generating similar data, the generative adversarial networks have attracted a great deal of attention in the recent years, especially in the image and video processing. Also the data produced by these models are hardly recognizable as the synthetic data. Hence, in our approach, in order to solve the problem of imbalance between the classes, generative adversarial networks (GANs) have been used to generate the minority class data. GANs are composed of two models; a generative one and a discriminative one with different architectures are used and trained. In each training iteration, a certain number of synthetic artificial transaction data is generated by a random input noise generated by the generative network, and the goal of the adversarial discriminator network is to distinguish these synthetic candidates from the real data; then the generator produces better and more realistic as possible to increase the error rate of its adversary, where both competitors improve their ability until a balance is reached, where the generated examples are indistinguishable from the real ones.

In order to solve the problem of imbalanced data, generative adversarial networks (GANs) were applied in our approach. GANs are composed of two models, a generative and a discriminative unit with different architectures. In each training iteration, the generative network generates a certain number of synthetic transactions by random input noise. The goal of the adversarial discriminator network is to distinguish these synthetic candidates from the real data. Then the generator produces better and more realistic as possible to increase the error rate of its adversary, where both competitors improve their ability until they reach a balance until the generated examples are indistinguishable from the real ones.

Therefore, in such an inferential situation, the generator network generates more genuine

examples over time. On the other hand, the discriminator distinguishes real instances from the synthesized ones and continuously improves its skill. The training continues until the discriminator is deceived. Then it is no longer capable of detecting synthetic data from the real ones. Finally, the output network is used to generate the pseudo-real synthetic data. The structure of the generating network used in this work consists of 4 hidden layers with 64, 128, 256, and 512 units and 32 input noise dimensions. The discriminator network structure used also comprises 4 layers of 256, 128, 64, and 32 units. The ADAM algorithm and the training rate of 0.0002 are also used to train the desired GAN model [12] and [13].

3.2.4. Fix a Time Dependency Difficulty for Bank Transaction Data

Given that the customer and fraudulent behavior is revealed over time and one transaction does not provide specific information about the customer and fraudulent behavior individually, this paper presents two different approaches to account for the time dependencies and increase accuracy. Modeling is used, which will be discussed below.

3.3. Proposed Model's Architecture

This figure is representative of our three different methods. We created this in regards to examine the results of each one and choose which one works better. Also due to the common objects, we draw them as one figure, but each block has its result. The architecture of the proposed methods is represented in Figure 1.

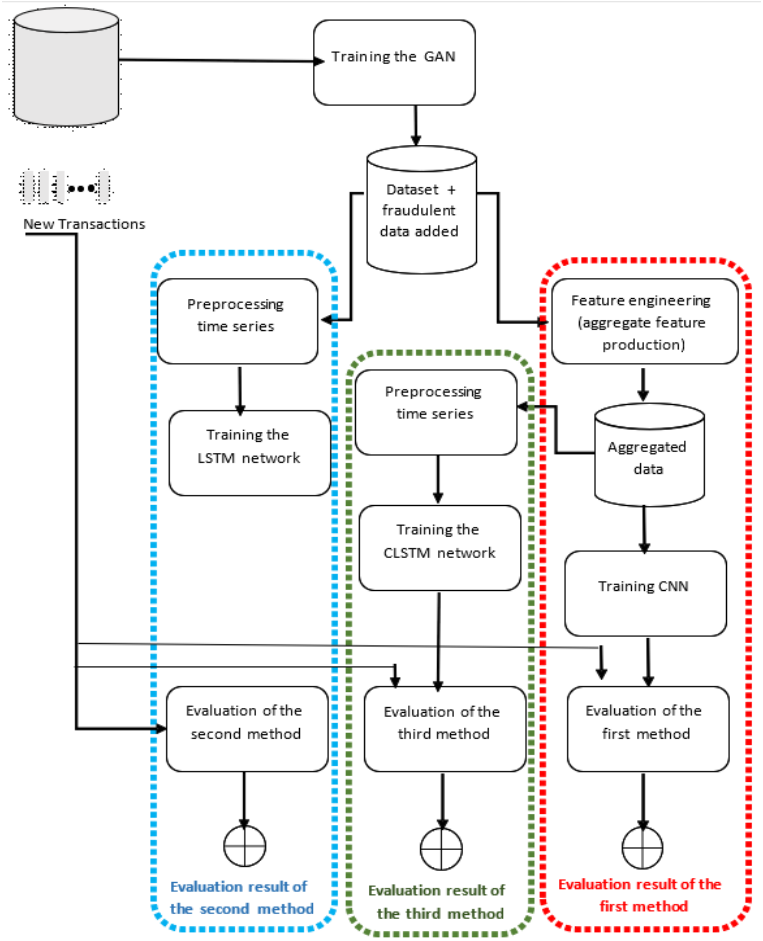

Figure 1. The proposed model's architecture (a) Output of the first method using the feature engineering and deep convolutional neural network. (b) Output of the second method using the long short-term memory network. (c) Output of the third method using the deep convolutional long short-term memory network.

3.3.1. First Method: Feature Engineering and Deep Convolutional Neural Network

In this method, appropriate time dependencies as new features are extracted from the raw data, and then consider the power of deep convolutional networks in different data classification applications, especially image processing and signal processing. The deep convolutional neural

network is used to train the normal transactions to detect fraudulent transactions, as in [39]. The extracted features are matrixed (2D array) to the deep convolutional network input. These features have been extracted in different periods including one-day, two-day, one-week, two-week, and one-month.

3.3.2. Second Method: Long Short-term Memory Network

Theoretically, due to the memory contained in the cells of the recursive networks, these networks can understand the temporal dependencies. Also due to the specific architecture of the short-term durable memory cells of this network, they can understand the short and long-term dependencies of time series data. Therefore, in this approach, raw data is provided to the long short-term memory network by simple preprocessing, and converted to constant-length time series. The training process is performed on these features. Figure 2 presents a cell of LSTM.

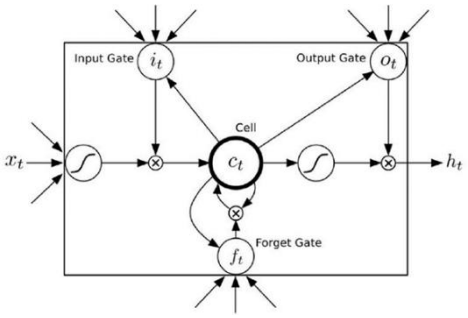

Figure 2. A cell of LSTM.

3.3.3. Third Method: Deep Convolutional Long Short-term Memory[4] Network

CLSTM has been recently used in the video processing applications and with acceptable results [16]. The model understands 2D patterns with their temporal dependencies, and has the strengths of both the convolutional and long short-term memory networks. They have sustainable benefits to one another [17] and [18]. In this paper, the data extracted from feature engineering is divided into fixed-length time series and is provided to the network for training. Figure 3 presents a simple C-LSTM network.

[4] C-LSTM

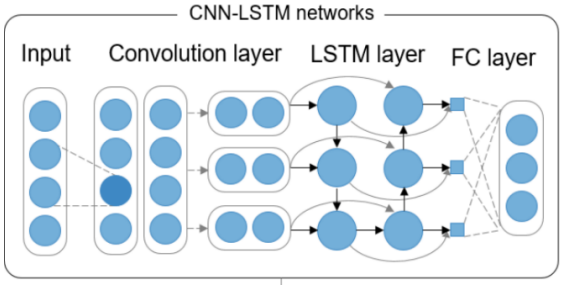

Figure 3. A C-LSTM network architecture [48].

4. Empirical Analysis

4.1. Data Description

The dataset used in this work is a real-life dataset from one of the largest commercial banks in Iran. The fraudulent transactions were labeled according to the records from the fraud investigation department. The dataset contains 268465 transaction records, and is highly imbalanced (only 617 (0.23%) fraudulent transactions).

The pre-process of factors in the dataset consist of outliers, duplicates that need to rule out, and some transactions that were not launched by the customers, for instance, reversal transactions.

Finally, the number of data generated by the GAN network to improve the detection efficiency of the introduced models is 30100.

The main variables included the transaction amount, transaction date, transaction time, deposit number, branch code, previous balance, current balance, transaction type, and terminal number. However, the main variables do not explain the cardholder behavior. The aggregate variables are added to the main variables to represent the user behavior.

We obtained 298565 transactions for the experiment. The dataset was split into a training dataset and a test dataset. The training dataset contains 200,000 randomly separated transactions, and the test dataset includes the rest of the transactions.

4.2. Experimental Setup

The main intention of this paper is to achieve an optimal method for fraud detection. We compare three popular deep learning models including LSTM, CNN, and C-LSTM with the three most widely used data mining techniques in fraud detection, i.e. the random forest (RF) and support vector machine (SVM), together with a traditional shallow structured artificial neural network. We fundamentally experiment with the efficiency of a deep learning-based method. Also we made a balanced dataset for more accuracy, which uses

the feature variables produced by a feature engineering analysis as the model input.

Under the feature engineering framework, we used the transaction aggregation and rule-based strategy to produce 30100 more transactions. For utilizing the transaction aggregation strategy, we picked a subset of all potential combinations of 12 aggregation characteristics, four aggregation periods, three transaction behavior measures (transaction amount, geographical distance period between two transactions, the period gap between two transactions), and four aggregation statistics (average, standard deviation, max, and count). The five aggregation periods we choose including the past one day, the past two days, the past week, the current transaction, the past two weeks, and the past month can be categorized into short, medium, and long periods to provide a summary of the behavior information from short term to long term. We choose some aggregation features like abnormal time, purchase, geographical distance of each transaction, cash withdrawal, online transaction, high-risk MCC, and some other characteristics related to distinguishing fraudulent acts. For comparison, the traditional machine learning methods use the variables under the RFM framework as suggested in the literature [47]. We similarly calculated our features under five levels of aggregation to construct 100 variables.

We randomly used 80% of the dataset for model training and the remaining was used for system evaluation. Also we used the GAN method to generate some fraudulent synthetic data to eliminate the unbalancing problem.

4.3. Evaluation Criteria

Several commonly used classification performance measures based on the confusion matrix were employed in this work to evaluate the fraud detection performance.

Table 2. Definition of confusion matrix.

		Predicted class	
		Positive	**Negative**
Actual class	Positive	TP	FN
	Negative	FP	TN

4.3.1. Accuracy

The most common evaluation criterion in various classification applications is calculated from the ratio of correct diagnosis data to the total number of data, as in Formula 1.

$$Accuracy = (TP + TN) / (TP + FP + TN + FN) \quad (1)$$

4.3.2. Precision (Positive Class True Detection Rate)

This criterion is calculated from the ratio of the number of positive class correct diagnoses to the total number of data detected as the positive class.

$$Precision = TP / (TP + FP) \quad (2)$$

4.3.3. Recall

This criterion can be calculated from the ratio of the number of positive class correct positives to the total number of positive class data.

$$Recall = TP / (TP + FN) \quad (3)$$

4.3.4. F1 Score

The F1 score is obtained by combining the two precision and recall criteria, and can be calculated from the four relationships below.

$$F1\,score = 2 \times (pre \times rec) / (pre + rec) \quad (4)$$

4.3.5. Rate of false-positive class

This criterion is the proportion of negative cases incorrectly identified as positive cases in the data. It is defined in Equation 5 as the total number of negative cases incorrectly identified as the positive cases divided by the total number of negative cases.

$$FPR = FP / (FP + TN) \quad (5)$$

4.3.6. Equal Error Rate and Receiver Operating Characteristic Curve

The equal error rate is a criterion used for determining the threshold limit for the false-positive and false-negative classes. When the two rates are similar, their equality is considered as the error rate. Therefore, the imbalance of the two-class data and the model imbalance in the data detection will not affect the performance of this model. Equal error rates are also detectable on the system performance characteristic diagram, in which the axes are the threshold of positive class error rate and negative class error rate.

A receiver operating characteristic curve (ROC) is created by plotting the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings. TPR defines how many correct positive results occur among all the positive samples available during the test. FPR, on the other hand, defines how many incorrect positive results occur among all the negative samples available during the test.

4.3.7. Distance Score

D score is a novel fit function that performs well in unbalanced datasets. The subject eliminates the bias for precision by simultaneously learning the minority and majority classes of equal importance. If the output is greater than the threshold value (zero), this sample belongs to the

minority class; otherwise, it belongs to the majority class. The output distance is calculated from the threshold value. Therefore, the bigger the distance, the higher the weight, and the better the prediction. We followed this step of multiplying the distance for both classes and calculate the class scores. This score is denoted as C1 for the majority class and C2 for the minority class. C1 and C2 range from 0 to 1, with the worst score being zero and the best score being one. Finally, to calculate D, the harmonic averages C1 and C2 are taken into account. The reason for choosing the harmonic mean is that even if one of the values between C1 and C2 is zero, the D score will be zero. It ensures that for a high D score, both C1 and C2 must increase [14].

D Score is calculated as follows:

$$Dsc = (2 \times C1 \times C2) / (C1 + C2) \quad (6)$$

C1 is calculated as follows:

$$C1 = \frac{\sum_{i=0}^{N_{maj}} sig(P_{Maj_i}) \times |T - sig(P_{Maj_i})|}{N_{maj}} \times func(1, P_{Maj_i}) \quad (7)$$

C2 is calculated as follows:

$$C2 = \frac{\sum_{i=0}^{N_{min}} sig(P_{Min_i}) \times |T - sig(P_{Min_i})|}{N_{min}} \times func(1, P_{Min_i}) \quad (8)$$

$$func(1, k) = \begin{cases} 1, if\ k \leq 0\ majority\ class\ instance \\ 1, if\ k > 0\ minority\ class\ instance \\ 0, otherwise \end{cases} \quad (9)$$

4.3.8. Proposed Matrix Extracted from Feature Engineering Operation

In this method, appropriate time dependencies are extracted from raw data as the new features. Then due to the power of the convolutional neural network (CNN) in various applications of data classification, especially image, signal processing is used. The growing applications of these models in various other approaches are caused using CNN to train and detect the fraudulent transactions from the genuine ones, as in [34]. CNN can learn and recognize specific types of features at a spatial location at the input by the convolutional layer [59]. The extracted properties are given as matrices (2D array) to the input of CNN. These features are extracted in different periods such as one-day, two-day, one-week, two-week, and one-month periods, and for each transaction, as follows (Figure 4). This subject ranges from one to zero, and represents the possibility of being a positive class.

Figure 4. Proposed matrix extracted from feature engineering operation.

4.4. Experimental Results

Two main questions are answered through the empirical experiments. The first question is whether the deep learning techniques can provide a better fraud detection performance. The second is whether our proposed feature engineering framework can provide better variables for machine learning methods in fraud detection. Therefore, our experiment aims to investigate these two questions. We evaluated the fraud detection performance of the deep learning models and traditional machine learning methods using different feature sets. Moreover, in order to evaluate the fraud detection models from the practical viewpoint, we measured the performance of our models with the new criteria as well as the traditional approaches.

The experiments and simulations were implemented in the MATLAB programming environment and Python. The Parallel computing toolbox and deep learning library of Matlab were employed to improve the performance of deep learning models, and the Keras library was used in the Python programming language to train the generative adversarial networks. The Bosaris library was used in the MATLAB programming environment to calculate the criterion of equal error rate estimation and to draw the ROC graphs.

4.4.1. Fraud Detection Performance Results

An overview of the proposed deep model structure used in the article is shown in Figure 5. The random forest model used in this work contains 1000 decision trees. The radial basis function was chosen for the support vector machine model. The recursive network properties were adjusted to the random dropout rate of 0.3, the Adam algorithm with 30 iterations, and the initial training rate of 0.00001. Also the

convolutional neural network properties were adjusted to the initial training rate of 0.00005 and the Adam algorithm with 20 iterations.
The input data for the recursive network was divided into series containing 100 members in which all the data was sorted and belonged to one person. Also due to the ability to model long-term and short-term time dependencies, 12 main features are sufficient. The random forest input features and support vector machine include 12-dimensional main features and 100-dimensional single-vector engineering features that consist of 112-dimensional features in total. Also the input of training data obtained from feature engineering was segmented into fixed-length time series.

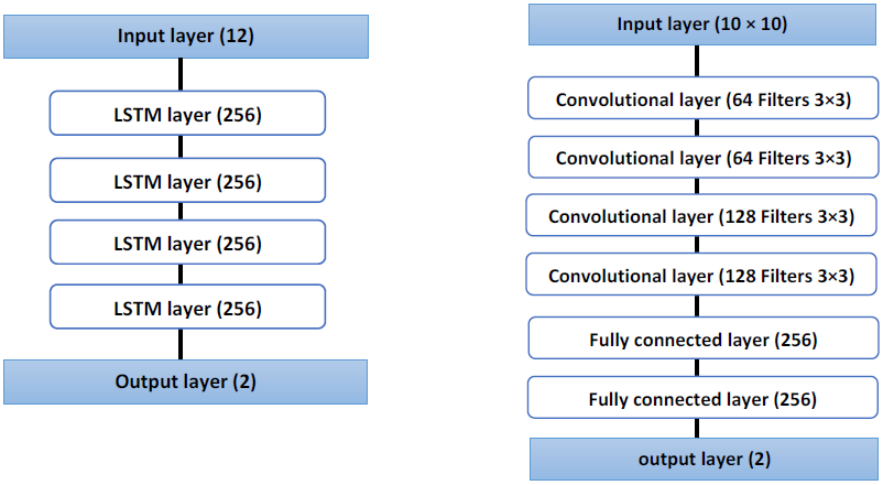

Figure 5. Structure of deep models used in this paper.

The results of different evaluation criteria included three proposed and two traditional models with all the original data used to train and evaluate the network(without GAN's data), presented in Table3.
In Table 4, the results of this experiment on the original dataset adding to the GAN's data are shown.

Table 3. Results of models without data generated by GAN.

Model	Accuracy	Precision	Recall	F1 score	FPR
C-LSTM + Feature engineering	٪99.94	٪100	٪99.94	0.9997	**٪100**
LSTM	٪99.74	٪100	٪99.74	0.9987	**٪100**
CNN+ feature engineering	٪99.73	٪99.99	٪99.74	0.9987	**٪99.64**
RF+ feature engineering	٪99.65	٪99.80	٪99.85	0.9982	**٪67.44**
SVM+ feature engineering	٪99.78	٪100	٪99.78	0.9989	**٪100**

In Table 3, despite the high errors in the classification, the accuracy, precision, recall, and F1 score are high. Also the D score and equal error rate related to Table 3 are presented in Figures 6 and 7. The reason is that the large number in positive class compared to the negative one leads to the orientation of the models towards positive class data. Therefore, by adding the data generated by GAN in Table 4, the results of negative class detection have improved but the first four criteria have remained almost constant or worse. Thus it can be concluded that these criteria are not practically suitable for this application. Also the fifth criterion will not be a good criterion due to not considering the model efficiency in positive class detection. In contrast, the equal error rate and D score criterion to considering the model performance in the classification of both positive and negative classes are presented in Figures 8 and 9.

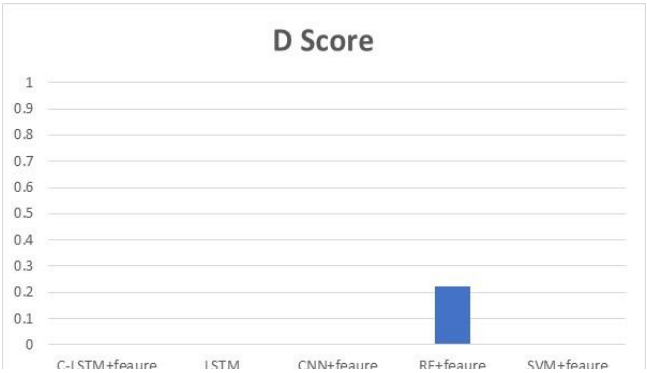

Figure 6. D score for models without data generated by GAN.

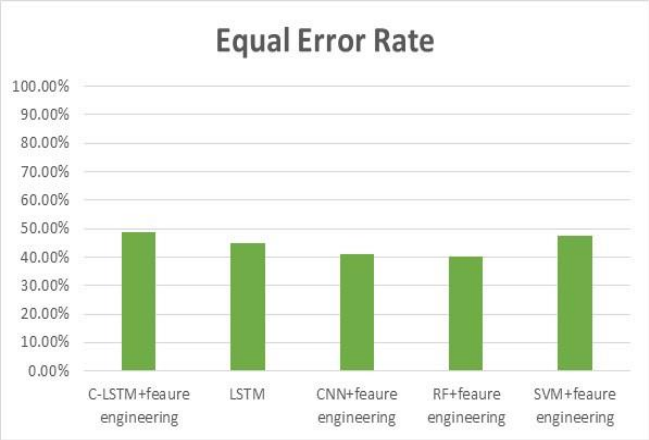

Figure 7. Equal error rate score for models without data generated by GAN.

Table 4. Results of models with data generated by GAN.

Model	Accuracy	Precision	Recall	F1 score	FPR
C-LSTM+ feature engineering	٪99.84	٪100	٪99.82	0.9991	**٪1.25**
LSTM	٪99.70	٪100	٪99.66	0.9983	**٪2.65**
CNN+ feature engineering	٪94.27	٪99.48	٪94.36	0.9685	**٪46.21**
RF+ feature engineering	٪82.81	٪87.51	٪92.68	0.9002	**٪53.63**
SVM+ feature engineering	٪90.13	٪98.96	٪90.75	0.9468	**٪79.32**

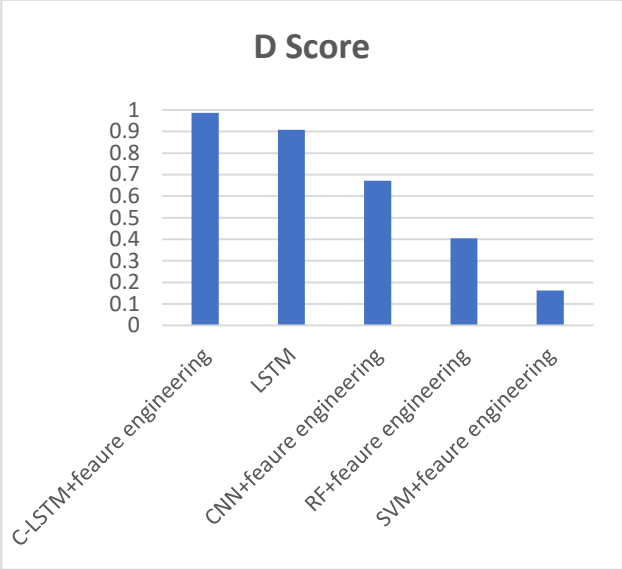

Figure 8. D score for models with data generated by GAN.

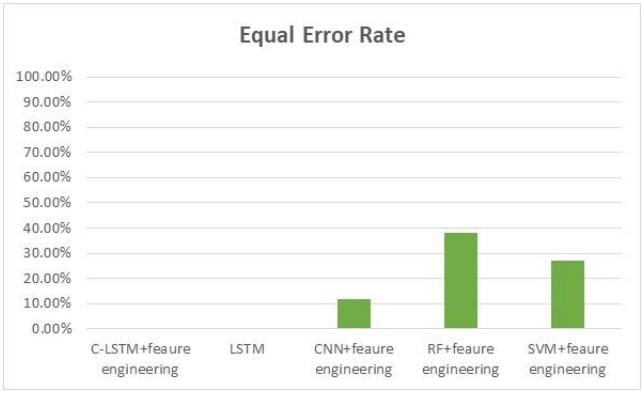

Figure 9. Equal error rate score for models with data generated by GAN.

As it can be seen, the result tables describe an understandable evaluation of the model performance. Also the results of Table 3 show that the deep learning models in the conditions of class imbalanced not only do not perform better but are also biased toward the majority class, and will not be able to identify the minority class.

The parameters selected for the two LSTM and CNN network architectures are determined according to the results shown in Table 5. This table represents the evaluation of all data with the produced data by the GAN network to train the network. Due to the limited input dimensions, no more than four layers can be selected for the CNN network. The results of the four LSTM layers are also sufficiently acceptable and appropriate so the layers have been identified.

Table 5. Results of models with different layers

Model	Layer counts	Accuracy	Precision	Recall	F1 Score	FPR	EER	D score
CNN	2	٪89.89	٪99.56	٪90.08	0.9458	٪85.17	٪38.03	0.42
CNN	3	٪96.66	٪99.64	٪90.73	0.9498	٪78.92	٪19.80	0.51
CNN	4	٪94.27	٪99.48	٪94.36	0.9685	٪46.21	٪11.59	0.6720
LSTM	2	٪90.93	٪99.97	٪90.47	0.9513	٪79.55	٪15.99	0.48
LSTM	3	٪91.98	٪97.73	٪93.42	0.9553	٪53.58	٪8.16	0.65
LSTM	4	٪99.70	٪100	٪99.66	0.9983	٪2.65	٪0.37	0.9071
LSTM	5	٪100	٪100	٪100	1	0	0	1

In this paper, one of the most important challenges, which is the inequality of class data, was tackled with the help of deep learning methods and the generation of artificial data for minority classes by GAN networks [12]. Also due to the inefficiency of the traditional evaluation criteria in this problem, the measure equal error rate and distance score [14] was used to evaluate the efficiency of the models. Finally, the performance of the proposed models is compared with two common approaches in this field (random forest and support vector machine). For a

further comparison, ROC of the used single models is depicted in Figures 10 and 11.

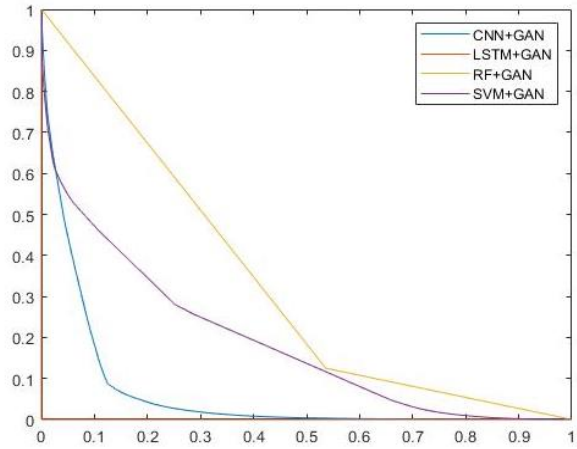

Figure 10. ROC results for models with data generated by GAN.

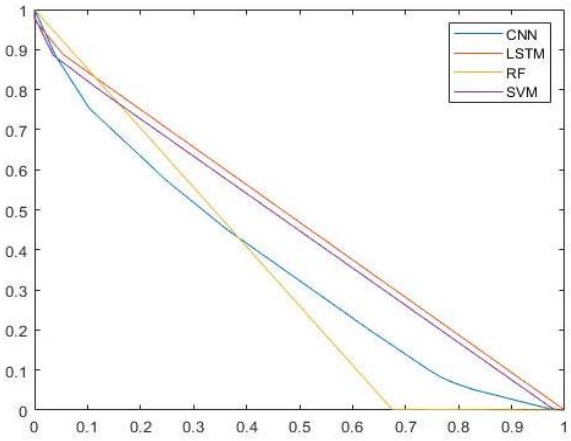

Figure 11. ROC results for models without GAN generated data.

5. Conclusions and Future Work

In this paper, we examined the problem of fraud detection in banking transactions on the data obtained from a private bank. Several recent works that address this issue and its challenges were analyzed. Various challenges in this issue including time dependencies, data imbalance problem, and selection of appropriate evaluation criteria were also explored, and solutions provided. The most important challenge, the imbalanced data, was addressed by deep learning and the generation of synthetic and semi-realistic data for the minority class. Also due to the inefficiency of the traditional evaluation criteria in this field, the measure equal error rate and distance score was used to evaluate the efficiency of the models.

Finally, the evaluation results declare that the proposed model has a high performance compared to the most usual and traditional methods in this area like random forest and support vector machine. The combinatory DNN-based classifier proposed in this work improved the results of the random forest by almost 38% for EER and 0.58 for the distance score. Using the GAN-generated data significantly improved the performance of all the models used, especially our final model, by 50%.In conclusion, the GAN-generated data improves the performance of any model by a noticeable margin, and combining it with the LSTM and CLSM classifiers shows an excellent promise.

In the future, in order to solve the concept drift problem, we will explore more efficient feature selection and other automated feature selection and extraction methods, and then improve the classification and production efficiency of the synthetic data; more sophisticated and engineered models of deep learning will be used to detect fraud in banking transactions. Finally, the investigation and examination of the more extensive dataset will be among the future work

6. References

[1] N. Carneiro, G. Figueira, and M. Costa, “A data mining-based system for credit-card fraud detection in e-tail,” Decis. Support Syst., Vol. 95, pp. 91–101, 2017.

[2] Nilson Report (2019), The Nilson Report, Issue 1164, November. Retrieved from "https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1164.pdf"

[3] T. Eliassi-Rad et al., “APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions,” Decis. Support Syst., Vol. 75, No. 2015, pp. 38–48, 2015.

[4] X. S. E.W.T. Ngai, H. Yong., Y.H. Wong, and Y. Chen, “The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature,” Decis. Support Syst., Vol. 50, pp. 559–569, 2011.

[5] J. C. W. Jha.Sanjeev and G. Montserrat, “Employing transaction aggregation strategy to detect credit card fraud,” Expert Syst. with Appl., Vol. 39, pp. 12650–12657, 2012.

[6] J. D. J. Piotr., A.M. Niall, J.D. Hand, and C. Whitrow, “Off the peg and bespoke classifiers for fraud detection,” Comput. Stat. Data Anal., Vol. 52, pp. 4521–4532, 2008.

[7] S. Kumar, V. Kumar-Solanki, S. K. Choudhary, A. Selamat, and R. Gonzalez-Crespo, “Comparative Study on Ant Colony Optimization (ACO) and K-Means Clustering Approaches for Jobs Scheduling and Energy Optimization Model in Internet of Things (IoT),” Int. J. Interact. Multimed. Artif. Intell., Vol. 6, No. 1, p. 107, 2020.

[8] Haibo He and E. A. Garcia, "Learning from Imbalanced Data," IEEE Trans. Knowl. Data Eng., Vol. 21, No. 9, pp. 1263–1284, Sep. 2009.

[9] S. J. S. P.K. Chan, W. Fan, and A.L. Prodromidis, "Distributed data mining in credit card fraud detection," Proc. IEEE Intell. Syst., pp. 67–74, 1999.

[10] D. J. H. R.J. Bolton, "Unsupervised profiling methods for fraud detection," Conf. Credit scoring Credit Control ,Edinburgh, 2001.

[11] A. Eshghi and M. Kargari, "Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty," Expert Syst. Appl., Vol. 121, pp. 382–392, May 2019.

[12] U. Fiore, A. De Santis, F. Perla, P. Zanetti, and F. Palmieri, "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection," Inf. Sci. (NY)., Vol. 479, pp. 448–455, Apr. 2019.

[13] I. J. Goodfellow et al., "Generative adversarial nets," in Advances in Neural Information Processing Systems, 2014,Vol. 3, No. January, pp. 2672–2680.

[14] D. Devarriya, C. Gulati, V. Mansharamani, A. Sakalle, and A. Bhardwaj, "Unbalanced breast cancer data classification using novel fitness functions in genetic programming," Expert Syst. Appl., Vol. 140, Feb. 2020.

[15] Y. Heryadi and H. L. H. S. Warnars, "Learning temporal representation of transaction amount for fraudulent transaction recognition using CNN, Stacked LSTM, and CNN-LSTM," in 2017 IEEE International Conference on Cybernetics and Computational Intelligence, CyberneticsCOM 2017-Proceedings, 2018, Vol. 2017-November, pp. 84–89.

[16] A. Ullah, J. Ahmad, K. Muhammad, M. Sajjad, and S. W. Baik, "Action Recognition in Video Sequences using Deep Bi-Directional LSTM with CNN Features," IEEE Access, Vol. 6, pp. 1155–1166, Nov. 2017.

[17] S. L. Oh, E. Y. K. Ng, R. S. Tan, and U. R. Acharya, "Automated diagnosis of arrhythmia using combination of CNN and LSTM techniques with variable length heartbeats," Comput. Biol. Med., Vol. 102, pp. 278–287, Nov. 2018.

[18] R. Zhao, R. Yan, J. Wang, and K. Mao, "Learning to monitor machine health with convolutional Bi-directional LSTM networks," Sensors (Switzerland), Vol. 17, No. 2, Feb. 2017.

[19] M. Syeda, Y. Q. Zhang, and Y. Pan, "Parallel granular neural networks for fast credit card fraud detection," in IEEE International Conference on Fuzzy Systems, 2002, Vol. 1, pp. 572–577.

[20] N. Carneiro, G. Figueira, and M. Costa, "A data mining based system for credit-card fraud detection in e-tail," Decis. Support Syst., Vol. 95, pp. 91–101, Mar. 2017.

[21] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decis. Support Syst., Vol. 50, No. 3, pp. 602–613, Feb. 2011.

[22] M. Carminati, R. Caron, F. Maggi, I. Epifani, and S. Zanero, "BankSealer: A decision support system for online banking fraud analysis and investigation," Comput. Secur., vol. 53, pp. 175–186, Sep. 2015.

[23] A. Correa Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature engineering strategies for credit card fraud detection," Expert Syst. Appl., Vol. 51, pp. 134–142, Jun. 2016.

[24] M. F. A. Gadi, X. Wang, and A. P. Do Lago, "Credit card fraud detection with artificial immune system," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2008, Vol. 5132 LNCS, pp. 119–131.

[25] A. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," Expert Syst. Appl., Vol. 41, pp. 4915–4928, 2014.

[26] C. Whitrow, D. J. Hand, P. Juszczak, D. Weston, and N. M. Adams, "Transaction aggregation as a strategy for credit card fraud detection," Data Min. Knowl. Discov., Vol. 18, No. 1, pp. 30–55, Feb. 2009.

[27] 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, 2013.

[28] S. Maes, S. Maes, K. Tuyls, B. Vanschoenwinkel, and B. Manderick, "Credit Card Fraud Detection Using Bayesian and Neural Networks," MACIUNAS RJ, Ed. Interact. IMAGE-GUIDED NEUROSURGERY. Am. Assoc. Neurol. Surg., pp. 261--270, 1993.

[29] R. C. Chen, M. L. Chiu, Y. L. Huang, and L. T. Chen, "Detecting credit card fraud by using questionnaire-responded transaction model based on support vector machines," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), Vol. 3177, pp. 800–806, 2004.

[30] R. C. Chen, S. T. Luo, X. Liang, and V. C. S. Lee, "Personalized approach based on SVM and ANN for detecting credit card fraud," in Proceedings of 2005 International Conference on Neural Networks and Brain Proceedings, ICNNB'05, 2005, Vol. 2, pp. 810–815.

[31] P. K. Chan, W. Fan, A. L. Prodromidis, and S. J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," IEEE Intell. Syst. Their Appl., Vol. 14, No. 6, pp. 67–74, 1999.

[32] R. Brause, T. Langsdorf, and M. Hepp, "Neural data mining for credit card fraud detection," in Proceedings of the International Conference on Tools with Artificial Intelligence, 1999, pp. 103–106.

[33] C. C. Chiu and C. Y. Tsai, "A web services-based collaborative scheme for credit card fraud detection," in Proceedings - 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service, EEE 2004, 2004, pp. 177–181.

[34] X. Zhang, Y. Han, W. Xu, and Q. Wang, "HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture," Inf. Sci. (NY)., 2019.

[35] W. Lee, S. J. Stolfo, and K. W. Mok, "Adaptive intrusion detection: A data mining approach," Artif. Intell. Rev., Vol. 14, No. 6, pp. 533–567, Dec. 2000.

[36] C. S. Hilas, "Designing an expert system for fraud detection in private telecommunications networks," Expert Syst. Appl., Vol. 36, No. 9, pp. 11559–11569, Nov. 2009.

[37] A. Kanavos, S. A. Iakovou, S. Sioutas, and V. Tampakas, "Large scale product recommendation of supermarket ware based on customer behaviour analysis," Big Data Cogn. Comput., Vol. 2, No. 2, pp. 1–19, Jun. 2018.

[38] R. A. Becker, C. Volinsky, and A. R. Wilks, "Fraud detection in telecommunications: History and lessons learned," Technometrics, Vol. 52, No. 1, pp. 20–33, Feb. 2010.

[39] A. Sudjianto, S. Nair, M. Yuan, A. Zhang, D. Kern, and F. Cela-Díaz, "Statistical methods for fighting financial crimes," Technometrics, Vol. 52, No. 1, pp. 5–19, Feb. 2010.

[40] D. J. Hand, "Fraud detection in telecommunications and banking: Discussion of Becker, Volinsky, and Wilks (2010) and Sudjianto et al. (2010)," Technometrics, Vol. 52, No. 1, pp. 34–38, Feb. 2010.

[41] G. Widmer, "Learning in the presence of concept drift and hidden contexts," Mach. Learn., Vol. 23, No. 1, pp. 69–101, 1996.

[42] J. G. Moreno-Torres, T. Raeder, R. Alaiz-Rodríguez, N. V. Chawla, and F. Herrera, "A unifying view on dataset shift in classification," Pattern Recognit., Vol. 45, No. 1, pp. 521–530, 2012.

[43] A. Tsymbal, "The problem of concept drift: definitions and related work," 2004.

[44] J. Gama, I. Zliobaite, A. Bifet, M. Pechenizkiy, and A. Bouchachia, "A survey on concept drift adaptation," ACM Computing Surveys, Vol. 46, No. 4. Association for Computing Machinery, 2014.

[45] S. Haykin and L. Li, "Nonlinear Adaptive Prediction of Nonstationary Signals," IEEE Trans. Signal Process., Vol. 43, No. 2, pp. 526–535, 1995.

[46] R. Akbani, S. Kwek, and N. Japkowicz, "Applying support vector machines to imbalanced datasets," in Lecture Notes in Artificial Intelligence (Subseries of Lecture Notes in Computer Science), 2004, Vol. 3201, pp. 39–50.

[47] E. Aleskerov, B. Freisleben, B. Rao, Cardwatch: A neural network-based database mining system for credit card fraud detection, in: Proceedings of the IEEE/IAFE Computational Intelligence for Financial Engineering (CIFEr), IEEE, 1997, pp. 220-226

[48] T. Kim and S. Cho, "Predicting residential energy consumption using CNN-LSTM neural networks", Energy, Vol. 182, pp. 72-81, 2019. Available: 10.1016/j.energy.2019.05.230

[49] A. D. Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in Proceedings-2015 IEEE Symposium Series on Computational Intelligence, SSCI 2015, 2015, pp. 159–166.

[50] C. Bunkhumpornpat, K. Sinapiromsaran, and C. Lursinsap, "Safe-level-SMOTE: Safe-level-synthetic minority over-sampling technique for handling the class imbalanced problem," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009, Vol. 5476 LNAI, pp. 475–482.

[51] T. Razooqi, K. Raahemifar, P. Khurana, and A. Abhari, "Credit Card Fraud Detection Using Fuzzy Logic and Neural Network," 2016.

[52] D. Lin, C. K. M. Lee, M. K. Siu, H. Lau, and K. L. Choy, "Analysis of customers' return behavior after online shopping in China using SEM," Ind. Manag. Data Syst., Vol. 120, No. 5, pp. 883–902, 2020.

[53] Z. Nematzadeh, R. Ibrahim, and A. Selamat, "Improving class noise detection and classification performance: A new two-filter CNDC model," Appl. Soft Comput., Vol. 94, p. 106428, Sep. 2020.

[54] D. Kalaivani and T. Arunkumar, "Multi- process prediction model for customer behaviour analysis," Int. J. Web Based Communities, Vol. 14, No. 1, pp. 54–63, 2018.

[55] S. Priya and R. A. Uthra, "Comprehensive analysis for class imbalance data with concept drift using ensemble-based classification," J. Ambient Intell. Humaniz. Comput. 2020 125, Vol. 12, No. 5, pp. 4943–4956, Apr. 2020.

[56] M. Mohamad, A. Selamat, O. Krejcar, H. Fujita, and T. Wu, "An analysis on new hybrid parameter selection model performance over big data set," Knowledge-Based Syst., Vol. 192, p. 105441, Mar. 2020.

[57] H. Mehmood, P. Kostakos, M. Cortes, T. Anagnostopoulos, S. Pirttikangas, and E. Gilman, "Concept Drift Adaptation Techniques in Distributed Environment for Real-World Data Streams," Smart Cities, Vol. 4, No. 1, pp. 349–371, Mar. 2021.

[58] B. Lebichot, G. M. Paldino, G. Bontempi, W. Siblini, L. He-Guelton, and F. Oble, "Incremental learning strategies for credit cards fraud detection: Extended abstract," Proc. - 2020 IEEE 7th Int. Conf.

Data Sci. Adv. Anal. DSAA 2020, pp. 785–786, Oct. 2020.

[59] Y. Kim, "Convolutional neural networks for sentence classification," in EMNLP 2014 - 2014 Conference on Empirical Methods in Natural Language Processing, Proceedings of the Conference, 2014, pp. 1746–1751.

[60] E. Pejhan and M. Ghasemzadeh, "Multi-Sentence Hierarchical Generative Adversarial Network GAN (MSH-GAN) for Automatic Text-to-Image Generation," *J. AI Data Min.*, vol. 9, no. 4, pp. 475–485, Nov. 2021.

تجزیه و تحلیل رفتار مشتریان برای بهبود تشخیص تراکنش های تقلبی با استفاده از یادگیری عمیق

فرشته برات زاده و سید محمد حسین هاشمی نژاد *

دانشکده مهندسی کامپیوتر، دانشگاه الزهرا ، تهران، ایران.

ارسال ۲۰۲۰/۱۰/۱۰؛ بازنگری ۲۰۲۱/۰۷/۱۷؛ پذیرش ۲۰۲۲/۰۱/۰۶

چکیده:

با پیشرفت تکنولوژی، استفاده روزانه از کارت های اعتباری بانکی به طور تصاعدی در حال افزایش است. بنابراین، استفاده متقلبانه از کارت های اعتباری توسط دیگران به عنوان یکی از جرایم جدید نیز به سرعت در حال رشد است. به همین دلیل شناسایی و پیشگیری از این حملات به یک حوزه فعال مطالعاتی تبدیل شده است. در این کار، چالش‌های کشف تقلب تراکنش‌های بانکی را مورد بحث قرار می‌دهیم و راه‌حل‌هایی مبتنی بر یادگیری عمیق ارائه می نماییم. تراکنش ها با سایر مدل های سنتی در کشف تقلب نیز مورد بررسی و مقایسه قرار می‌گیرند. با توجه به نتایج به‌دست‌آمده، عملکرد بهینه مربوط به مدل ترکیبی شبکه‌های کانولوشن عمیق و حافظه کوتاه‌مدت است که با استفاده از داده‌های جمع‌آوری‌شده از شبکه متخاصم مولد آموزش داده می‌شود. این مقاله در صدد است تا داده های معقولی را به منظور رسیدگی به مشکل توزیع نامتوازن کلاس داده تولید کند که بسیار مؤثرتر از روش های سنتی است. همچنین از نقاط قوت دو رویکرد با ترکیب شبکه کانولوشن عمیق و شبکه Long Short-Term Memory به منظور بهبود عملکرد استفاده می نماید. با توجه به ناکارآمدی معیارهای ارزیابی متداول از جمله دقت در این کاربرد، برای ارزیابی شفاف‌تر و دقیق‌تر مدل‌ها از معیار امتیاز فاصله و نرخ خطای برابر نیز استفاده گردیده است. همچنین به منظور ارزیابی کارایی، روش‌های سنتی با رویکرد پیشنهادی مقایسه می‌گردند.

کلمات کلیدی: کشف تقلب در تراکنش بانکی ، یادگیری عمیق، شبکه متخاصم مولد، شبکه حافظه کوتاه مدت، یادگیری ماشین، داده‌کاوی.