


Research Article

Credit Fraud Recognition Based on Performance Evaluation of Deep Learning Algorithm

Rawaa Ismael Farhan¹ 

Department of Computer Science

University of Wasit, College of Education of Pure Science

Wasit, Iraq

ralrikabi@uowasit.edu.iq

ARTICLE INFO

Article History

Received: 29/12/2023

Accepted: 4/2/2024

Published: 1/6/2024

This is an open-access

article under the CC

BY 4.0 license:

<http://creativecommons.org/licenses/by/4.0/><http://creativecommons.org/licenses/by/4.0/>**ABSTRACT**

Over time, with the growth of credit cards and financial data, credit models are needed to support banks in making financial decisions. Hence, developing an efficient fraud detection system is essential to avoid fraud in Internet transactions, which increased with the growth of technology. Deep learning techniques are superior to other machine learning techniques in predicting the behavior of credit card customers based on the probability that they will miss a payment. The bidirectional long-short term memory (BiLSTM) model is proposed to train the Taiwanese non-transactional dataset for bank credit cards to decrease the losses of banks. The BiLSTM reached an accuracy of 98% in fraud credit detection compared with other machine learning techniques.

Keywords: Credit Card Fraud Detection; Deep Learning; BiLSTM, Bank Management; Customer Behavior.

1. INTRODUCTION

The basic risk for credit cards in banks is customer default, that is, the customer is unable to recover from debt in the case of an assurance or loan. Thus, the borrower either misses or stops payments. In the case of customer default, no assets are assuring the debt, but the bank still has legal back. Credit card companies generally give several months before an account becomes default [1].

Presently, Internet banking is very common. Consequently, electronic payment systems have facilitated services and product buying. Credit cards enable cashless transactions and supply insurance for things that have been lost, stolen, or damaged [2]. In addition, customers must confirm transactions when using their credit cards as a kind of security [3]. However, the theft problem of credit cards still exists and costs customers and financial companies further losses. Fraudsters improve methods frequently to exploit Internet transactions, and thus identifying and stopping fraud is difficult for banks [4].

Card payments are influenced by fraudulent abuse, and the increasing use of mobile devices for payment initiation leads to losses owing to fraudulent transactions [5]. Over the years, banks had a large database of customers, allowing them to analyze their performance and make financial decisions [6]. Banks must know whether a customer is a good or bad payer. Therefore, they should use credit and behavioral scoring to examine the behavior of current customers based on their different behaviors and then estimate their behavior of payment and credit status, helping to make decisions at the customer level [7].

In this study, a deep learning algorithm was implemented to detect fraud in credit cards using a real-world dataset. A bidirectional long-short term memory (BiLSTM) algorithm is used for the estimation of the customer behavior score. The main contributions of this study are as follows:

1. A framework has been proposed to help banks register credit card customers.
2. A deep learning model is proposed using the BiLSTM algorithm to determine customer behavior.

3. The proposed BiLSTM model outperforms other classifiers by comparing their performance.

This study is directed to the importance of automatically scoring customer behavior during reimbursement when making risk decisions. Then, banks use such scores to classify customers according to risk, which could limit losses by detecting potential bankruptcy and timely blocking the card of customers. Thus, the bank management estimates the likelihood that a customer will miss payments.

2. METHODOLOGIES

Fig. 1 shows the major framework of the implemented fraud detection model in this study.

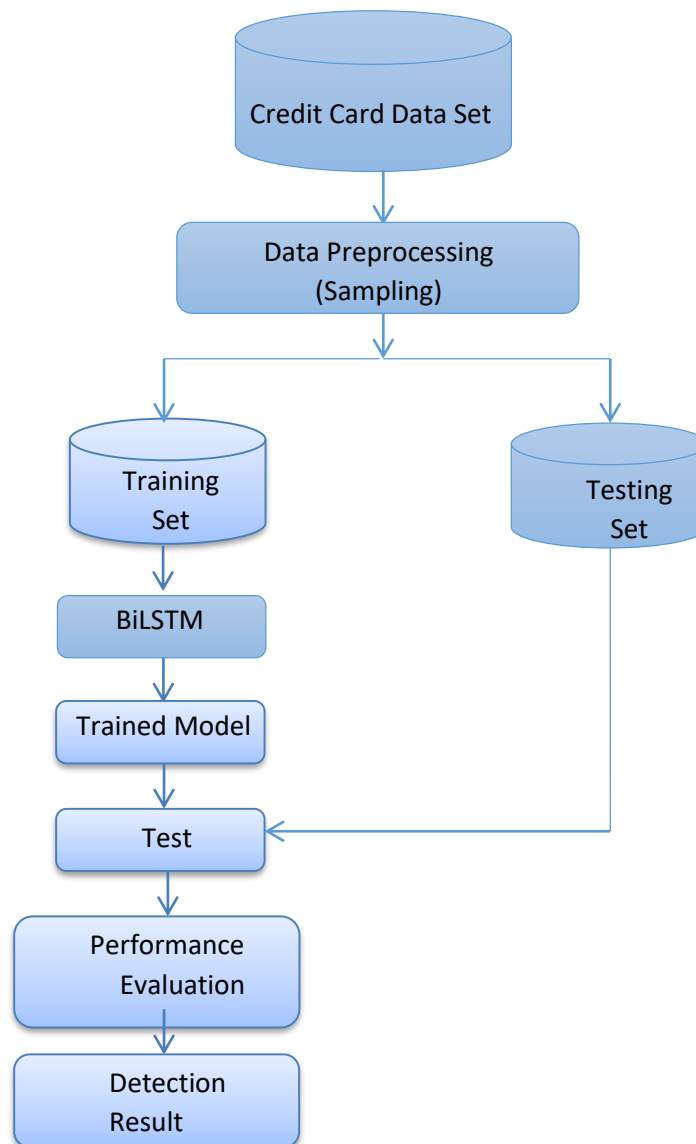


Fig. 1. Major framework

Table I shows the hyper parameters for the proposed model where grid search is used for the automatic selection of the number of layers and number of neurons in each layer.

TABLE I. HYPERPARAMETERS DESCRIPTION

Hyper parameter	Description
Number of features	23
Number of BiLSTM layer	2
Attention layer	1
Activation Function	Sigmoid

2.1 Fraud Detection

Fraud detection is the process of recognizing fraudulent behavior [8]. The credit card industry encourages the deployment of fraud detection mechanisms; thus, fraud detection may become a preventive approach in the future [9].

Fast detection of fraud allows the card issuer to limit losses. Presently, considerable money can be stolen in a very short period without leaving any trace of the fraudster. Hence, legal card owners may not realize that they have been exploited until weeks after the actual fraud incident, making credit cards an easy and preferred target for fraud [10]. Financial institutions try to detect credit fraud quickly after it occurs, rather than in real time because detecting fraud can slow down the license application to the point that it expires. Banks flag the transaction as a potential fraud and then contact the cardholder to determine if the transaction is legitimate. Finally, the card can be blocked as necessary [11].

Publicly publishing the exact information of the techniques used in fraud detection enables fraudsters to develop ways to circumvent systems, which will hinder the process of developing fraud detection systems and the possibility of sharing information about their development. Card issuers are also typically very reluctant to make an annual report about fraud figures because of the stigma associated with potential financial loss, which gives issuers another reason to keep the results of internal fraud detection out of the public domain [12].

One challenge is the unacceptable false alarm rates, which make it much more likely to inconvenience legitimate customers than to detect fraud. This study proposed techniques based on BiLSTM that can relatively classify fraud rapidly. This technique is dynamic because it tries to learn the existing time series depicted as a series of the same transactions of the cardholder [13].

2.2 BiLSTM Algorithm

BiLSTM refers to a sequence model that implements two LSTM layers for bidirectional processing: the forward direction for input processing and the backward direction processing. The concept of this approach is to improve the understanding of the sequences and the relationship between them by processing data in both directions.

BiLSTM architecture is composed of two LSTMs, forward and backward, to process the sequence, as shown in Fig. 2. Thus, an LSTM network takes the tokens sequence as its inputs, and the other LSTM network gets in the reverse order. Therefore, LSTM networks give the output as a vector of probability, which contains the combination of both probabilities [14]:

$$pt = pt^f + pt^{2b} \quad (1)$$

where pt refers to the final vector of probability, pt^f refers to the forward probability vector, and pt^{2b} refers to the backward probability vector.

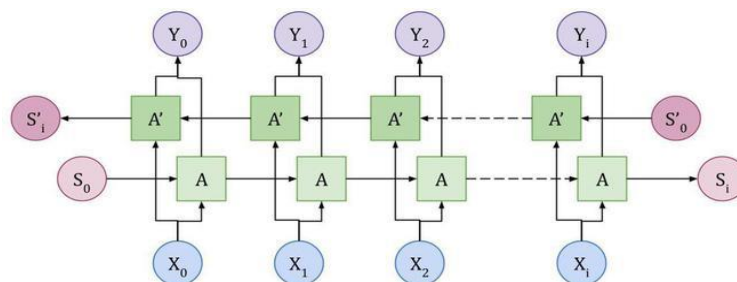


Fig. 2. Architecture of the BiLSTM

2.3 Credit Card Dataset

This study used the Taiwanese dataset, which is “a public non-transactional credit card dataset” containing default payments of customers. This dataset has been exploited in evaluating customers’ behavior and models to determine their credit scores and is also widely used in deep learning models [15]. For security, banks do not expose the raw form of their transactional databases, so many of the datasets are in processed form and not in open access. Here, we used a public dataset available that can convert customer payments into a temporal format monthly instead of grouped values. The size of dataset records is 30,000, where the default payment number is 6636, and the remaining 23,364.23 are non-default. A total of 23 features were divided into numerical and categorical as follows

- V1: amount of the given cards
- V2: male or female gender
- V3: level of education
- V4: personal status married or single
- V5: customer age
- V6–V11: past payment history
- V12–V17: amount of bill statement
- V13–V23: amount of previous payment

2.4 Performance Metrics

The following performance measures are implemented to validate the proposed model and evaluate the proposed method’s predictive accuracy: accuracy, area under the curve (AUC), and confusion matrix, where TP represents the number of true positives, FN is false negatives, FP is false positives, and TN is true negatives. These criteria are used in the confusion matrix for the accuracy of the proposed model. The accuracy represents the percentage of true classified inputs as follows:

$$TP + TN / TP + TN + FP + FN \quad (2)$$

AUC is an area under the ROC curve to evaluate the measured classifier. AUC is useful in analyzing binary classification to identify which one of the models predicts the best classes.

3. RESULTS AND DISCUSSION

In this section, all the experiments were implemented using Python. The proposed BiLSTM model results are depicted, including comparisons to the other machine learning models. The model on the defined dataset is evaluated using different measurements of performance.

The BiLSTM model based on the last 6 months provides the probability that each customer will miss a payment in the next month. Thus, future data are not used. To clarify the power of identification in the BiLSTM algorithm, performance measurements were applied not only for active customers but also for the following [13]:

- Customers who have missed one payment in the last 2 months are classified as a low risk of default.
- Customers were recognized as bad or good payers based on whether they had missed a payment.
- Customers with two sequential missed payments mean that they have financial problems.
- Customers with three consecutive missed payments are expected to be near default. Thus, BiLSTM predicts a default in the fourth missed payment.

The BiLSTM model should be compared with different benchmark models (e.g., SVM [16], LR [18], and RF [17]) to investigate its identification power. Notably, all models use nontemporal data. Therefore, temporal data in the model should have been converted before use. Table II shows a comparison of classifiers according to the performance measures. The validation test of all the models is similar in the predictions and good enough. The closest one in performance to our BiLSTM proposed model is the RF classifier. Considering the low dimensionality of the input dataset, which is only 23 features for each customer, all classifiers’ performance is very close to one another. Therefore, fewer problems occur with simple classifiers when extracting the required feature. The optimal threshold is applied to the classifier to enhance and achieve maximum accuracy. Therefore, our BiLSTM classifier still has the highest value compared with other classifiers. We believe that the results are important because, in such a critical problem, any increase in accuracy or AUC of the classifier results in an important loss decrease for the bank, which may be caused by missed payments and bankruptcies of customers.

TABLE II. BILSTM MODEL COMPARED WITH DIFFERENT MACHINE LEARNING MODELS

Paper	Model	Accuracy
Asha RB et al. [16]	SVM	93%
Youness A. et al. [18]	LR	96%
Jonathan K.A. et al. [17]	RF	96%
proposed model	BiLSTM	98%

As shown in Figure 3 confusion matrix is a graphical tool to visualize model performance. Its idea is to understand what the model has done correctly and incorrectly. Therefore, the predicted and actual classes were arranged in columns and rows, respectively.

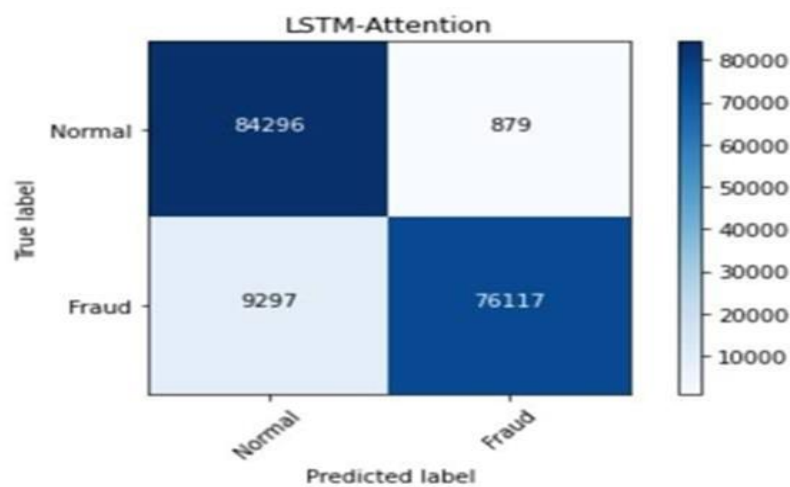


Fig. 3. Confusion matrix of BiLSTM

The ROC curve is an important tool in the case of imbalanced datasets for model evaluation of target binary classes. This curve is depicted with the X-axis representing recall and the Y-axis representing precision. In binary classification, the area under the ROC curve that represents the total test ability to detect between classes was used, where model performance records are great with high numbers, BiLSTM model performance shown in Fig 4.

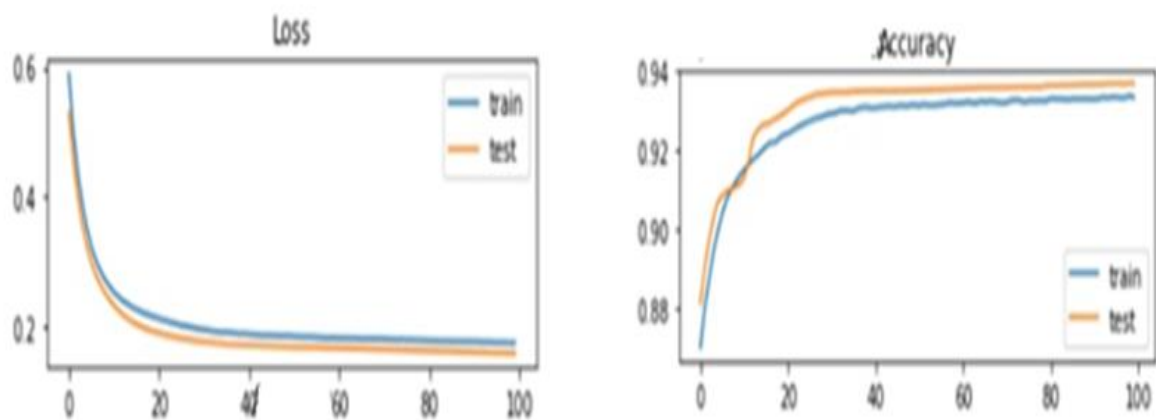


Fig. 4. BiLSTM model performance

As shown in Table III, a class label of 0 and 1 represents legal and fraudulent transactions, respectively. The time measured in seconds requires the intervals between the current and first transactions, whereas count refers to the number of transactions represented in Fig. 5 and 6.

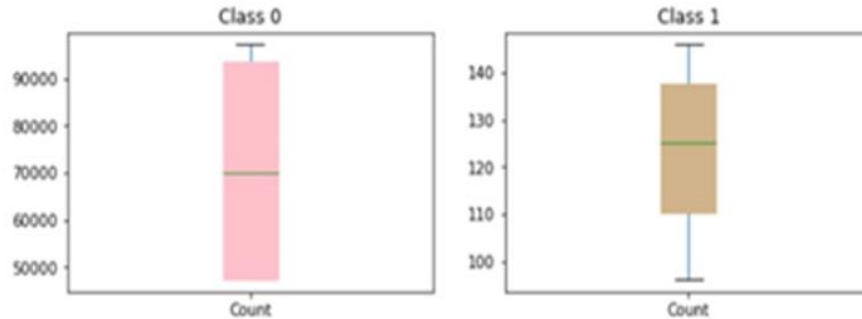


Fig. 5. Count of fraudulent and normal classes

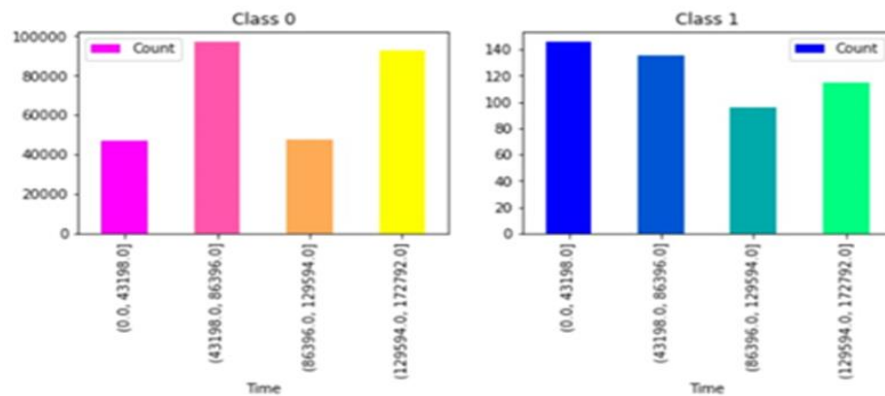


Fig. 6. Time of fraudulent and normal classes

TABLE III. TIME AND COUNT OF CLASSES

No.	Class	Time	Count
0	0	[0.0,43198.0]	47249
1	0	[43198.0,86396.0]	97252
2	0	[86396.0,129594.0]	47342
3	0	[129594.0,172792.0]	92470
4	1	[0.0,43198.0]	146
5	1	[43198.0,86396.0]	135
6	1	[86396.0,129594.0]	96
7	1	[129594.0,172792.0]	115

4. CONCLUSIONS

Fraud in credit cards arises when the card is used for unauthorized transactions or the card is stolen, or in other words, when the fraudsters use the card's information for their gain. Credit fraud is a critical problem in banks with long-term results owing to ever-changing profiles of legal and fraudulent behaviors. In addition, the data sets for fraud are quite biased. The BiLSTM model aims to automate credit card customer behavior scoring and to raise an early alarm when a credit card defaults. Then, the system analysis is accomplished by applying performance measures to customers in different groups, where the bank takes advantage of customers' bad payment history. The BiLSTM model is superior with a 98% accuracy compared with other machine learning models (i.e., SVM, LR, RF) by using different performance measures. Future studies can focus on modern and advanced deep learning models to work in real time so that credit card providers can monitor suspicious behavior and detect potential fraud.



REFERENCES

- [1] Neda Soltani Halvaiee , Mohammad Kazem Akbari, "A novel model for credit card fraud detection using Artificial Immune Systems", Applied Soft Computing, volume 24, 2014, pp. 40-49.
- [2] Alex G.C. de Sá et al., "A customized classification algorithm for credit card fraud detection", Engineering Applications of Artificial Intelligence, volume 72, 2018, pp. 21-29.
- [3] Fabrizio Carcillo et al., Gianluca Bontempi, "SCARFF: A scalable framework for streaming credit card fraud detection with spark", Information Fusion, volume 41, 2018, pp. 182-194.
- [4] Jerzy Błaszczyński et al. "Auto loan fraud detection using dominance-based rough set approach versus machine learning methods Expert Systems with Applications", volume 163, 2021, Article 113740.
- [5] Nuno Carneiro et al., "A data mining based system for credit-card fraud detection in e-tail" ,Decision Support Systems, volume 95, 2017, pp. 91-101.
- [6] Sanaz Nami, Mehdi Shajari, "Cost-sensitive payment card fraud detection based on dynamic random forest and k -nearest neighbors", Expert Systems with Applications, volume 110, 2018, pp. 381-392.
- [7] Asha RB, Suresh Kumar KR, "Credit card fraud detection using artificial neural network", Global Transitions Proceedings, volume 2, Issue 1, 2021, pp. 35-41.
- [8] Gabriele Gianini et al., "Managing a pool of rules for credit card fraud detection by a Game Theory based approach", Future Generation Computer Systems, volume 102, 2020, pp. 549-561.
- [9] panelAsha RB, Suresh Kumar KR, "Credit card fraud detection using artificial neural network", Global Transitions Proceedings , volume 2, Issue 1, June 2021, pp. 35-41.
- [10]panelGabriele Gianini a c, Leopold Ghemmogne,Fossi c e, Corrado Mio c, Olivier Caelen d, Lionel Brunie , "Managing a pool of rules for credit card fraud detection by a Game Theory based approach", Future Generation Computer Systems,volume 102, January 2020, pp. 549-561.
- [11] Yue Wu et al.,'Feature construction for fraudulent credit card cash-out detection',Decision Support Systems, volume 127, 2019, Article 113155.
- [12] Sal"vatore Carta et al., "Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model", Journal of Information Security and Applications, volume 46, 2019, pp. 13-22.
- [13] Alex G.C. de Sá L. et al.,'A customized classification algorithm for credit card fraud detection', Engineering Applications of Artificial Intelligence, volume 72, 2018, pp. 21-29.
- [14] Li Y-H, Harfiya LN, Purwandari K, Lin Y-D., "Real-Time Cuffless Continuous Blood Pressure Estimation Using Deep Learning Model", Sensor s, volume 20, No 19, 2020, Article 5606.
- [15]Yen-Wu Ti, Yu-Yen Hsin, Tian-Shyr Dai, Ming-Chuan Huang, and Liang-Chih Liu, "Feature generation and contribution comparison for electronic fraud detection", 2022 , doi: 10.1038/s41598-022-22130-2.
- [16] Asha RB, Suresh Kumar KR, " Credit card fraud detection using artificial neural network", Global Transitions Proceedings, volume 2, 2021, pp.35–41.
- [17] Jonathan Kwaku Afriyie et al., " A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions", decision analytics journal, volume 6, march 2023, Article 100163.
- [18] Youness Abakarim, Mohamed Lahby, Abdelbaki Attioui , "An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning", SITA'18: Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications, October 2018, No.30,pp.1–7, <https://doi.org/10.1145/3289402.3289530>.