Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822 p-ISSN: 2958-0862

Financial Fraud Identification Using Deep Learning Techniques

Fatima Adel Nama[1], Ahmed J. Obaid[1]*

[1]Faculty of Computer Science and Mathematics, University of Kufa, Iraq

*Corresponding Author: Ahmed J. Obaid

DOI: https://doi.org/10.55145/ajest.2024.03.01.012
Received October 2023; Accepted December 2023; Available online January 2024

ABSTRACT: The volume of internet transactions has rapidly increased in recent years. E-commerce and e-governance have both seen significant development in recent years. This has led to a rise in the number of persons adopting online payment options. The number of transactions that take place every day has increased exponentially as a result of this. The frequency of online scams has also increased as a result of the rise in online transactions. It is becoming more and more important to identify these fraudulent transactions as soon as possible in order to take the necessary measures and minimize any damages brought on by the fraud. In this study, ML models are proposed that might leverage previously known data and attempt to anticipate frauds using knowledge gained from the earlier data. Fraudulent actions often pose a danger to digital payment systems. Customers may avoid financial loss by having fraud transactions caught during money transfers. This article focuses on mobile-based money transfers for fraud detection. This research proposes a DL architecture for monitoring and identifying fraudulent activity. Deceptive transactions are found by implementing and using a RNN on a synthetic financial dataset produced by PaySim. The suggested technique has 99.87% accuracy, an F1-Score of 0.99for detecting illegitimate transactions.

Keywords: Machine Learning (ML),Fraud, Deep Learning (DL)

1. INTRODUCTION

Recently, there has been a sharp surge in credit card theft in online payments, forcing banks and e-commerce companies to implement automated fraud identificationmethods based on ML methods on transaction logs [1]. A supervised binary classification model that was trained on a sample dataset offers a potential way to tell illegitimate cases apart from legitimateones in order to spot illegal transactions. Highly imbalanced class data are the dataset currently available for fault detection [2]. To locate the features in a fraud detection system, either expert-driven, data-driven rules, or a mix of both kinds of rules are utilized. Fraud investigators are used in expert-driven algorithms to identify fraud discovery in certain contexts. Expert driven rules identify new incoming transactions in the data stream and identify fraudulent tendencies [3]. Decision trees, SVM, logistic regressionand ANNs were employed as ML approaches for categorization. To create a hybrid model for detection, many techniques are merged or utilized independently [4]. When compared to data samples in the majority class in the dataset, the minority class in an imbalance classification has less data instances. This issue is described as having a very unbalanced dataset and skewed data distribution. Criminal or fraudulent activity is far less prevalent than honest and legal activity [5].The number of online and cashless transactions is rising as everything moves online. The epidemic further facilitated this change. Although there are many advantages to this rise, there are also some difficulties. The prevalence of fraud in online transactions is one of the main issues. Online fraud incidents are on the rise along with the volume of online transactions. This need technologies capable of quickly identifying fraudulent transactions. This will provide the relevant authorities the opportunity to take the required steps to reduce the loss to both public and private enterprises as well as the general population.Based on prior conclusions, MLalgorithms [6] aim to forecast the result or provide us information about a data sample. The same may be used to predict if a transaction is fraudulent or not based on the data available from earlier transactions. The objective of this supervised classification work [7] is to identify and report

*Corresponding author: ahmedj.aljanaby@uokufa.edu.iq fraudulent transactions.ML approaches would be preferable to DL techniques since the system should operate in a real environment and as a result, would need quick answers. This is because the DL algorithm has a propensity to take a long time both during training and while making conclusions.

The goal of this study is to develop a highly efficient and error-free model for detecting fraudulent financial mobile money transactions. It implements this model using DLmethods. Since these methods automatically capture the hierarchical characteristics included in the financial information, they are advantageous. RNNis used in this article and adheres to DL architecture. It is suggested that a stacked RNN method be used as a recommender system for spotting fraudulent transactions. Customers will be alerted automatically when suspicious behaviors that result in unlawful efforts are detected, preventing financial loss. Quantitative, qualitative, comparative, and complexity measurements are all determined as part of the analysis of the suggested algorithms. The suggested approaches have undergone thorough dataset testing.

The article's reminder is structured as shown below. In Section 2, a brief literature review is given. The suggested strategy is presented in Section 3. Results analysis kept in Section 4. Section 5 outlines the conclusion.

2. Literature Review

The goal of fraud detection is to recognize whether a credit card transaction is legitimate or fraudulent, which is viewed as a classification problem. Credit card extortion can be identified with a good understanding of fraud detection advances. The summary of the reviewed papers is as follows. Javad Forough [8] proposed an ensemble method which utilizesRNNs as base classifier and Feed forward neural network (FFNN) is used as voting mechanism after aggregation of different RNN classifiers results. A number of GRU and LSTM networks are utilized for recurrent networks that serve as base classifiers on various dataset samples, with the results being used to train the FFNN. The ensemble technique based on GRU is more effective than the one based on LSTM in terms of both training and testing time. GRU has fewer parameters and gates than LSTM, which explains this. Homogeneity-oriented behavior analysis (HOBA) was used by Xinwei Zhang [9] as a feature engineering technique with a DL architecture as a fraud detection system. Using the transaction aggregation technique, the features are chosen based on the shared traits.Out of CNN, DBN and RNN, DBN gives better F1-Score of 0.568, Precision of 62.6%, Accuracy of 98.25% and AUC of 0.976. The findings also show that all data mining methods benefit from HOBA-based feature engineering when it comes to detecting fraudulent transactions.

Taha et al. [10] utilized an optimized lightGBM (light Gradient boosting) optimization technique. The most key features are chosen using the Information Gain approach, and the model's performance is evaluated using a 5-fold CV test. The Optimized light gradient boosting algorithm achieved the higher accuracy, AUC and F1-Score of 98%, 0.9094 and 0.5695 respectively. Even in unbalanced data sets, the P-R curve gives a complete picture of the classification's performance.Rtyali and Enneya [11] suggested a hybrid anomaly detection approach that combines supervised andunsupervised detection using the ML techniques such as to extract the better prediction features use the SVM-RFE (Recursive Feature Elimination) approach, the SMOTE technique for balancing an unbalanced dataset and the GridSearchCV approach was employed as a Hyper Parameter Optimization (HPO) by a Random Forest Classifier. The proposed model is denoted as RFC(HPO, RFE), this hybrid method outperformed other state of the art models of ML with accuracy of 99%,sensitivity of 95% and AUPR 0f 0.81.It's a reliable classifier model since it maintains a high level of accuracy regardless of data quantity.

Lucas [12] implemented automated feature engineering using a multi-perspective Hidden markov model. The model learns eight different HMMs using a combination of three binary perspectives: cardholder/ merchant, genuine/fraudulent and amount/ timing. Finally, a set of eight HMM-based features will provide data on the validity and fraudulence of both terminal and cardholder histories. Based on the chosen characteristics, a Random Forest is trained to distinguish between fraudulent and legal transactions. The precision-recall AUC of random forest classifiers continuously and considerably increases when HMM-based features are added to the current transaction aggregation technique.Yakub K. Saheed [13] used GA as a feature selection technique with Random Forest, SVM and Naive Bayes algorithms. On a German dataset RF with GA performed better with accuracy of 96.4, recall of 96.4 and precision of 96.5. Zhenchuan Li [14] employed deep neural networks with transaction aggregation strategy as feature selection technique while SMOTE is used for balancing the data collected from a financial company of China. The F1-Score of this model is 0.813, and the AUC PR is 0.825. Priyanka Kumari [15] proposed a model with classifiers as bagging, voting and CART without applying any feature selection techniques.On the German dataset, the findings show that CART provides greater accuracy, precision, and recall (0.952) than other methods.

On a dataset of European cardholders, Ugo Fiore [16] classified fraudulent and lawful transactions using generative adversarial networks without the need of a feature selection approach. This framework increased sensitivity at the cost of a little increase in false positives. Pumsirirat& Yan [17] proposed a DL-based model for the detection of fraudulent transactions. Two unsupervised learning methods of DLi.e autoencoders (AE) and restricted boltzmann machines (RBM) are employed in this model. AE used backpropagation to reconstruct the error. AE and RBM are two DL methods for detecting fraud in real time using normal transactions. The AUC score of AE is 0.9603 on a dataset of 284, 807 transactions, and the RBM-based AUC score is 0.9505.For larger datasets, it can be concluded that AE and RBM produce high AUC scores and accuracy.Randhawa [3] utilized a total of fraud detection algorithms based on ML.

The algorithmsinclude everything from basic neural networks to DL models. Additionally, the AdaBoost and majority voting approaches are used in the development of hybrid models. A 10-fold cross validation method is being utilized. SVM outperformed all twelve algorithms with the highest MCC score of 0.813. Adaboost with SVM increased the fraud detection rate from 79.8% to 82.3% while the best rate for fraud detection was achieved by NN and NB at 78.8% in majority voting.

Without using any feature selection techniques, Sanaz Nami [18] created a model using dynamic random forest and KNN for the categorization of fraudulent and genuine transactions on a private bank dataset. It was shown that evaluating the resemblance of existing transactions in a cardholder's profile to test transactions could be utilized to detect payment card fraud successfully.On a very large dataset of 30,000000 instances from a Chinese e-commerce company, for classification, Xuan [19] utilized CART-based RF and random tree-based RF. With an accuracy of 96.77%, recall of 95.27%, and F-measure of 0.9601, CART (Classification and Regression trees) based RF outperformed random tree-based RF, while precision was somewhat inferior. Convolutional neural networks are used with a transaction aggregation method in a model put out by Kang Fu [20] in order to choose the predictive characteristics. Data from commercial banks that had been balanced using a cost-based sampling approach were used to run the model. When put to the test, the suggested strategy performs better than other cutting-edge approaches.

To identify credit card fraud, Carcillo [21] blended supervised and unsupervised approaches. In order to detect credit card fraud, unsupervised outlier ratings at different granularities were employed. The developed approach to remove the outliers from the dataset assessed the outlier score. In order to reduce the number of dimensions, Principal Component Analysis (PCA) was used in the feature selection process. Because independent variables are harder to comprehend in feature selection, the system is more likely to lose information as a result. To enhance the ability of focal loss and provide weight to the class that is often misunderstood, Trisanto [22] presented modified Focal loss for imbalance XGBoost. Using data on credit card fraud, the modified focal loss approach is assessed and contrasted with the standard method. In the focused loss, the imbalance parameter and tuning hyper-parameter are employed with the W-loss. Due to increased weight values on input data, the model suffers an overfitting issue. For the purpose of choosing the best features from the dataset, Trisanto [23] presented a two-stage feature reduction approach. To address the issue of imbalanced data, random undersampling and instance hardness threshold sampling were used. The ULB credit card fraud detection dataset was used to assess the two-stage feature reduction approach. The recall and MCC score are improved by the under-sampling technique. The proposed approach is limited by the classification's overfitting and outlier issues.

3. Proposed Methodology

Due to its capacity to handle sequential input and capture temporal associations, RNNs play a crucial role in the identification of financial crime. By taking into account the chronological sequence of occurrences, RNNs excel in modeling sequential data, such as transaction histories. They can record patterns, trends, and dependencies in the flow of financial transactions, allowing them to spot out-of-the-ordinary behaviors that can point to fraud. RNNs may be taught to recognize departures from known patterns and learn the typical behavior of financial transactions. RNNs may identify abnormalities in transaction amounts, frequencies, or other pertinent factors, indicating transactions that are probably fraudulent, by simulating the temporal dynamics of the data. RNNs may use contextual data from financial transactions to increase the precision of fraud detection. To determine the possibility of fraud, they may, for instance, take into account further information like client profiles, IP addresses, transaction timestamps, and historical trends. In order to detect fraudulent transactions as they take place, RNNs have the capacity to evaluate streaming data and generate predictions in real-time. This capacity is essential for detecting financial fraud since quick response and loss prevention are possible with timely discovery. RNNs are able to continually update and alter their models in response to fresh data. RNNs may learn from and integrate these modifications into their fraud detection models when criminals create new methods and fraud trends shift. This flexibility aids in preserving the system's efficiency throughout time. When it comes to financial fraud, illicit transactions are very few compared to normal ones, which leads to unbalanced datasets. Even with a small number of fraudulent transactions, RNNs can manage unbalanced data by successfully capturing the underlying patterns. RNNs are effective tools for detecting financial fraud, but it's crucial to remember that to create complete fraud detection systems, they are often combined with other methods and algorithms. These may include ensemble approaches, feature engineering, statistical models, or algorithms for anomaly detection, which may improve the fraud detection system's overall efficacy and sturdiness.

RNNs have been modified for modeling sequential data. Artificial neural networks can't scale up to model huge sequential data sets. RNNs permit the construction of linkages between neurons co-located in the same layer in addition to links across layers, which leads to the production of cycles or, in the network's design, a loop. Using cycles, the model's neurons may share weights that are determined by the interdependencies of the parameters over several iterations of an input at various time steps. This enables the often-used activation function. Relu or tanh to consider the condition of the neuron at an earlier period. As a result, the state may be utilized to carry over certain elements from earlier temporal periods into later ones. The activation function, dropout rate, and loss function are crucial variables that influence how well RNNs work.

An ANN for the purpose of analysing sequential data, such as audio, time series, and text, is known as an RNN [24]. RNNs, as opposed to conventional feedforward neural networks, provide a feedback loop that allows information to persist and be utilized again as the network processes sequential input [24]. Given, an input sequence $(X_1 ,X_2 \ldots ,X_t)$, an RNN creates an output sequence of $(Y_1 ,Y_2 \ldots ,Y_t)$, using the formula below, and the RNN model is depicted in Fig. 1.

$$h_t = \sigma (W^{hX} X_t + W^{hh} h_{t-1}) \quad \textbf{Eq. (1)}$$

$$Y_t = W^{Yh} h_t \textbf{Eq. (2)}$$

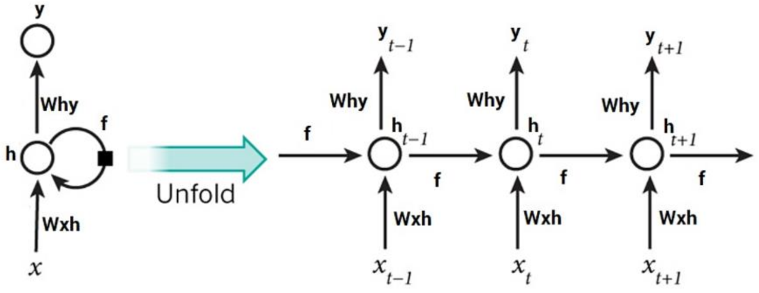

FIGURE 1. - **Architecture of RNN**

RNNs are a kind of deep models that support feedback loop design. The term "recurrent" is used because the same function is run for each data input, and the output of the current input relies on the results of the previous calculation. Because it can model sequences by taking into account interdependencies in the samples of the sequences, RNN is dominating. Designing a deep model requires taking activation function—a process that converts input signals into output signalsinto account. Popular activation functions used in this framework include sigmoid and tanh. The paper's objective is to identify any irregularities in money transactions. After learning from training data, a classifier model connects incoming data into output classes. It is suggested that a classifier model based on stacked RNNs be used to identify transactions that could have misleading problems. To create the suggested model, many RNN layers are combined onto a single platform. A sequential model is composed of four straightforward RNN layers, four dropout layers, and one additional layer. Incorporating Dropout layers lessen the issue of over-fitting by randomly deactivating a portion of the units or connections in a network after each iteration of training. Four thick layers follow the model once again. In terms of the kind of layers, number of nodes or dropout rate, form of the output generated by each layer, number of parameters received by each layer, and activation function employed, Table 1 gives a full description of the implemented model. 'Adam' optimizer and binary cross entropy loss function are used to compile these layers. Adam is a computer whiz who uses less RAM while optimizing. It is simple to develop and appropriate for stochastic objective function optimization using first-order gradients. On adaptive estimations of lower-order moments, it is predicated. Due of its application to non-stationary targets and issues with very noisy and/or sparse gradients, it is widely acknowledged.

During the process of fitting the training data into the classifier model, 64 batch sizes are employed during two epochs. A total of 33,065 trainable parameters are accepted by the model during training, and it makes use of these parameters to provide prediction results.

Table 1. - **Recommended Stacked-RNN Method**

Layers and Type	**Number of Nodes**	**Activation Function**	**Number of Parameters**
1. Simple RNN	128	Sigmoid	16640
2. Dropout	0.2	None	0
3. Simple RNN	64	Sigmoid	12352
4. Dropout	0.2	None	0
5. Simple RNN	32	Sigmoid	3104
6. Dropout	0.2	None	0
7. Simple RNN	16	Tanh	784
8. Dropout	0.2	None	0
9. Dense	8	None	136

10. Dense	4	None	36
11. Dense	2	None	10
12. Dense	1	Sigmoid	3

4. Dataset Description

This investigation makes use of a dataset of synthetically created digital transactions generated using an emulator called PaySim [25]. It mimics mobile money transactions using a sample of authentic transactions gathered from a month's worth of financial logs from an African country's mobile money service. It generates a synthetic dataset by aggregating anonymized data from the private dataset and then injecting fraudulent transactions. The dataset contains nearly 6 million transactions as well as 11 variables. There is a variable called 'isFraud' that rep-resents the transaction's real fraud status. This is the class variable for our investigation. The number 1 implies fraud, whereas the value 0 shows non-fraud.

5. Result Analysis

Any prediction model's performance has to be assessed, which illustrates the need of assessment metrics. The metrics used to evaluate the effectiveness of the classifier models are covered in this section. In this study, the performance evaluation indicators listed below are used to support the prediction findings.

1. Accuracy is a statistic that determines the proportion of accurate forecasts to all occurrences taken into account. Since the accuracy does not take into account incorrectly anticipated situations, it may not be a sufficient indicator for assessing the performance of the model. Therefore, it is required to compute with accuracy and recall in order to handle the difficulty mentioned above.

2. Precisionrepresents the proportion of accurate positive findings to the number of positive results that the classifier anticipated. Recall is defined as the quantity of accurate affirmative outcomes divided by the total quantity of relevant samples. The harmonic mean of accuracy and recall is used to produce the F1-Score, often known as the F-measure, a metric that is concerned with both recall and precision. One is known to be the ideal combination of F1-score, accuracy, and recall.

3. Mean Squared Erroris another grading metric that assesses the severity of discrepancies between test sample predictions and actual observations. The best non-negative floating-point value produced by MSE is one that is close to 0.0.

In further detail, the aforementioned metrics may be described as follows:

1. $$Precision = \frac{True\ Positive\ (TP)}{True\ Positive + False\ Positive\ (FP)}$$
2. $$Sensitivity\ or\ Recall = \frac{True\ Positive}{True\ Positive + False\ Negative\ (FN)}$$
3. $$F1 - Score = \frac{2\,x(Precision\ x\ Recall)}{(Precision + Recall)}$$
4. $$Specificity = \frac{True\ Negative\ (TN)}{True\ Negative + False\ Positive}$$
5. $$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

This investigation demonstrates that the suggested model greatly outperforms the industry standard for fraud transaction identification. Each epoch during the training of this model results in some loss, as seen in Fig.2. The loss decreases and eventually reaches minimal loss as the number of epochs rises. Better performing models will have a minimized loss. Our proposed stacked-RNN method got F1-Score, Accuracy and MSE as 99.87%, 0.99, and 0.01 respectively.

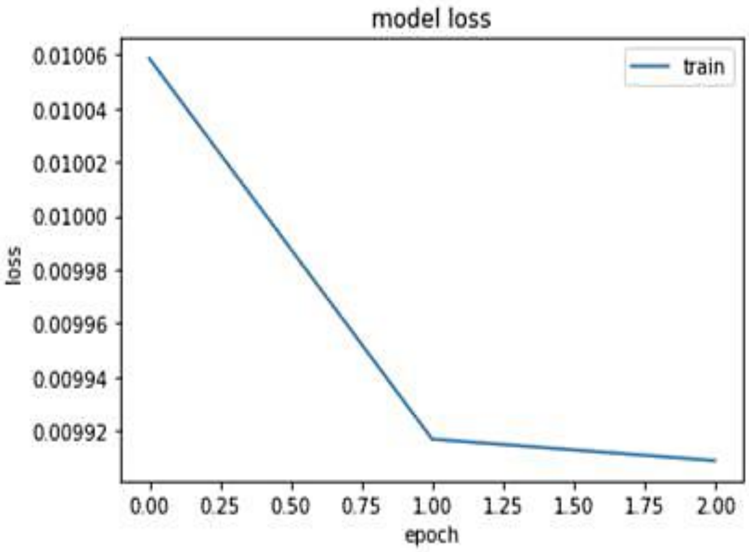

FIGURE 2. - **Loss Graph for each epoch during training phase**

6. Conclusion

In the modern financial age, finding fraud and preventing financial loss are highly hot topics. It is vital to find fraud activity during transactions due to the rising demand for mobile money transfers. A financial dispute won't annoy clients if illicit efforts are discovered. The primary goal of this research is to reduce fraud as much as feasible. The projected outcomes under the suggested model demonstrated mathematically that fraudulent transactions are outnumbered by legitimate ones. In this paper a stacked-RNN model is suggested and put into practice with the appropriate hyper-parameter fine-tuning. Hyper-parameter adjustments will help to create a model with a finer granularity and maximum performance. The suggested model is clearly capable of identifying suspicious transactions with a promising level of efficiency, according to the testing data. The fact that this suggested strategy can be used with a large financial dataset makes it advantageous. Since mobile transactions will alert consumers to fraudulent transactions, an effective and error-free mechanism is necessary. The study's findings will be helpful for businesses and organizations trying to set up or enhance their ML-based financial fraud detection systems. By using this cutting-edge technology, businesses may bolster their fraud defenses, cut down on financial losses, and protect their stakeholders from potential harm.

FUNDING

No funding received for this work

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their efforts.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan, "Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism," IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3637-3647, 2018.

[2] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit card fraud detection using hidden Markov model," IEEE Transactions on Dependable and Secure Computing, vol. 5, no. 1, pp. 37-48, 2008.

[3] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit card fraud detection using AdaBoost and majority voting," IEEE Access, vol. 6, pp. 14277-14284, 2018.

[4] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," Journal of Big Data, vol. 9, no. 1, pp. 1-17, 2022.

[5] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," IEEE Access, vol. 10, pp. 39700-39715, 2022.

[6] G. E. Melo-Acosta, F. Duitama-Munoz, and J. D. Arias-Londoño, "Fraud detection in big data using supervised and semi-supervised learning techniques," in 2017 IEEE Colombian Conference on Communications and Computing (COLCOM), pp. 1-6, IEEE, August 2017.

[7] R. Goyal and A. K. Manjhvar, "Review on credit card fraud detection using data mining classification techniques & machine learning algorithms," IJRAR-International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269.

[8] J. Forough and S. Momtazi, "Ensemble of deep sequential models for credit card fraud detection," Applied Soft Computing, vol. 99, p. 106883, 2021.

[9] 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," Information Sciences, vol. 557, pp. 302-316, 2021.

[10] A. A. Taha and S. J. Malebary, "An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine," IEEE Access, vol. 8, pp. 25579-25587, 2020.

[11] N. Rtayli and N. Enneya, "Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization," Journal of Information Security and Applications, vol. 55, p. 102596, 2020.

[12] Y. Lucas et al., "Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs," Future Generation Computer Systems, vol. 102, pp. 393-402, 2020.

[13] Y. K. Saheed, M. A. Hambali, M. O. Arowolo, and Y. A. Olasupo, "Application of GA feature selection on Naive Bayes, random forest and SVM for credit card fraud detection," in 2020 International Conference on Decision Aid Sciences and Application (DASA), pp. 1091-1097, IEEE, November 2020.

[14] Z. Li, G. Liu, and C. Jiang, "Deep representation learning with full center loss for credit card fraud detection," IEEE Transactions on Computational Social Systems, vol. 7, no. 2, pp. 569-579, 2020.

[15] P. Kumari and S. P. Mishra, "Analysis of credit card fraud detection using fusion classifiers," in Computational Intelligence in Data Mining: Proceedings of the International Conference on CIDM 2017, pp. 111-122, Springer Singapore, 2019.

[16] U. Fiore et al., "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection," Information Sciences, vol. 479, pp. 448-455, 2019.

[17] A. Pumsirirat and Y. Liu, "Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine," International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, 2018.

[18] S. Nami and M. Shajari, "Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors," Expert Systems with Applications, vol. 110, pp. 381-392, 2018.

[19] S. Xuan et al., "Random forest for credit card fraud detection," in 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), pp. 1-6, IEEE, March 2018.

[20] K. Fu, D. Cheng, Y. Tu, and L. Zhang, "Credit card fraud detection using convolutional neural networks," in Neural Information Processing: 23rd International Conference, ICONIP 2016, Kyoto, Japan, October 16–21, 2016, Proceedings, Part III 23, pp. 483-490, Springer International Publishing, 2016.

[21] F. Carcillo, Y. A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection," Information Sciences, vol. 557, pp. 317-331, 2021.

[22] D. Trisanto, N. Rismawati, M. Muhamad Femy, and K. Felix Indra, "Modified focal loss in imbalanced XGBoost for credit card fraud detection," International Journal of Intelligent Engineering and Systems, vol. 14, no. 4, pp. 350-358, 2021.

[23] D. Trisanto, N. Rismawati, M. Muhamad Femy, and K. Felix Indra, "Effectiveness undersampling method and feature reduction in credit card fraud detection," International Journal of Intelligent Engineering and Systems, vol. 13, no. 2, pp. 173-181, 2020.

[24] W. Yin, K. Kann, M. Yu, and H. Schütze, "Comparative study of CNN and RNN for natural language processing," arXiv preprint arXiv:1702.01923, 2017.

[25] TESTIMON @ NTNU, Synthetic Financial Datasets for Fraud Detection, Kaggle, retrieved from [Online]. Available: https://www.kaggle.com/ntnu-testimon/paysim1.