Fraud Detection in Credit Card Transaction Using ANN and SVM

Anchana Shaji(✉), Sumitra Binu, Akhil M. Nair, and Jossy George

Department of Computer Science, CHRIST (Deemed to be University), Bengaluru, India
anchana.shaji@science.christuniversity.in

Abstract. Digital Payment fraudulent cases have increased with the rapid growth of e-commerce. Masses use credit card payments for both online and day-to-day purchasing. Hence, payment fraud utilizes a billion-dollar business, and it is growing fast. The frauds use different patterns to make the transactions from the cardholder's account, making it difficult for the organization or the users to detect fraudulent transactions. The study's principal purpose is to develop an efficient supervised learning technique to detect credit card fraudulent transactions to minimize the customer's and organization's losses. The respective classification accuracy compares supervised learning techniques such as deep learning-based ANN and machine learning-based SVM models. This study's significant outcome is to find an efficient supervised learning technique with minimum computational time and maximum accuracy to identify the fraudulent act in credit card transactions to minimize the losses incurred by the consumers and banks.

Keywords: SMOTE · Artificial neural network · Support vector machine · Credit card fraud detection

1 Introduction

In the financial sector, frauds are becoming a significant issue harming the organization and individual user's socioeconomic status. The fraudsters exploit payment mode through cards and online transactions to steal cardholder's money using various techniques. The fraudsters can retrieve data from different websites about the details of cardholders. Due to this criminal activity, the detection of fraud is an essential need in society. Fraudsters find different techniques to achieve their goals. Various types of frauds such as CNP (Card Not Present), Skimming, Phishing, making duplicate cards, attacks by using the magnetic strips behind the card are the major fraud attacks in the network [1]. Attackers fetch the details of cardholders from different websites to steal the amount from cardholder's account. The available prevention techniques [2] for fraudulent transactions in credit cards were Manual Review, Negative and Positive lists, Card Verification Methods (CVM), and Payer Authentication. Due to changes in fraudster's techniques, the detection of fraudulent transactions is difficult in credit card transactions.

N. Kumar et al. (Eds.): UBICNET 2021, LNICST 383, pp. 187–197, 2021.
https://doi.org/10.1007/978-3-030-79276-3_14

There is an exponential increase in online fraudulent transactions in the recent past, utilizing various e-mail spoofing, phishing, cloning a card, etc. These fraudulent transactions are contributing to revenue loss for both the financial institutions and customers. Although researchers have proposed many techniques to spot fraudulent activities with various models, there are still many limitations in the existing models that need to be addressed. Hence, this issue must be addressed, and the losses are reduced by an efficient online credit card detection mechanism. The study aims to develop an efficient fraud detection model by comparing supervised learning techniques such as deep learning-based, Artificial Neural Network, and machine learning-based, Support Vector Machine. By calculating and comparing each model's computation time and classification accuracy, this study focuses on developing a model capable of detecting fraudulent transactions in various credit cards.

The study is organized as follows: Recent and Related works are observed in Sect. 2 that compares different classification models to detect fraudulent transactions. Section 3 introduces the proposed framework along with its validation. The evaluation of the proposed approach is demonstrated throughout Sect. 4. Section 5, focuses on the results of the study. Further Section, concludes the work and discusses future work.

2 Related Work

As credit card becomes the most popular payment mode both in online and offline shopping, fraud cases are also rising. Recent studies have focused on detecting these fraudulent transactions by various techniques. Thulasyammal Ramiah Pillai et al. [3] have implemented a Multi-layer perceptron deep learning model to detect fraud by various parameters. Among the parameters, the activation functions such as logistic function and hyperbolic tangent function provide high performance, and the proposed model attains about 82% sensitivity. Further research can be conducted by improving the model accuracy by new activation functions in balanced data with more advanced deep learning models. The optimum results could be observed while adding hidden layers and nodes to the network.

Debachudamani Prusti et al. [4] have compared the accuracy of different classification algorithms such as KNN, Extreme Learning Machine, Random Forest, Multilayer Perceptron, and Bagging Classifier. Moreover, the rate at which the models can identify the non-ethical transactions in credit cards was much faster enough. These individual classification models are hybridized in which the ensemble machine learning algorithms improve the model's performance in detecting fraud and non-fraud. Further studies can be done by implementing the model by utilizing real-time data, which leads to more efficient outputs. Chunzhi Wang et al. [5] proposed a Back Propagation (BP) neural network which detects frauds in networks. The authors propose a fraud detection algorithm using the Whale Optimization Algorithm to optimize the Neural Network algorithm with Back Propagation. This algorithm leads to improved accuracy, which contributes to the efficiency of the detection system. Saurabh C. Dubey et al. [6] have considered the real-time dataset for detecting fraud in credit card transactions. ANN with the Backpropagation technique is proposed with 99.96% of accuracy. The research can be extended further by integrating the proposed model with cloud services, which detects fraud faster using automated techniques.

Rimpal R. Popat et al. [7] have reviewed the credit card fraud detection by different methods such as Logistic Regression, deep learning, SVM, Naive Bayesian, Artificial Immune System, KNN, Decision Tree, and Genetic Algorithm. The work also discusses various types of fraud such as skimming, phishing, Card NOT Present (CNP), and Stolen Card. The patterns of fraud keep on changing, and hence it is not easy to detect them. Pradheepan Raghavan et al. [8] deal in evaluating Machine Learning techniques such as SVM, RF, KNN, and Deep Learning techniques such as Convolutional Neural Network, Deep Belief Networks (DBN), and Restricted Boltzmann Machine (RBM). The work has utilized German, Australian, and European datasets to evaluate each dataset type's suitable method. For large datasets, integrating SVM with CNN is the best method, and for small datasets, an ensemble model consisting of SVM, Random Forest, and KNN produces better results.

S. S. Harshini Padmanabhuni et al. [9] have implemented machine learning techniques such as SVM, KNN, Linear Regression, Adaboost, Decision Tree, Random Forest, classification with Neural Network, and PNN (Probabilistic Neural Network) were implemented. These techniques are compared with the generated hybridized models which include of SVM, KNN, Logistic Regression, Neural Network, and Decision Tree. Among these techniques, the hybridized model ensures accuracy of around 82.47%. Mrs.Vimala Devi. J et al. [10] have generated models like Random Forest, Decision Tree as well as SVM. They have compared an imbalanced dataset in detecting the fraudulent transactions of the credit card. Among these models, the Decision Tree has better accuracy. Further studies can be done after balancing the datasets by oversampling the dataset. Jasmine A Hudali et al. [11] have identified various types of credit card fraud and have reviewed different algorithms such as deep learning-based ANN and machine learning-based Decision Tree. While detecting such fraudulent transactions in credit cards, the card owner has the right to block the card, which will protect the corresponding user's privacy.Y. Sahin [12] has analyzed classification techniques such as SVM and Decision tree with real-time data. SVM technique with different kernel functions such as RBF, Polynomial, Sigmoid, and linear gives 99% accuracy in detecting the credit card fraud transactions that lead banks to reduce their risk.

Nana Kwame Gyamfi et al. [13] have analyzed several forms of fraud and the Support Vector Machine with Spark (SVM-S) technique has been implemented for the classification of customer's normal and fraudulent behaviour. This classification focuses more on the validity of new incoming transactions. Comparison of this technique with the Back-Propagation Network shows that the performance of SVM-S is more efficient than the Back-Propagation Network. Aihua Shen et al. [14] analyze and compares different classification problems such as Decision Tree, Logistic Regression, and Neural Network to provide an efficient model to detect fraudulent transactions. Evaluating the model ANN and Logistic Regression performance were the best models to spot fraudulent transactions to minimize the bank's risk.

3 Methodology

Supervised techniques learn the previous behaviour from the data and can detect real-time credit card frauds. A binary classification model which determines the fraudulent

and non-fraudulent transactions in credit card has been chosen and considered. The labelled data, which includes fraudulent or non-fraudulent transactions, is passed into the model. The model is then trained with input-output pairs, including various independent variables and the corresponding target(output) variable. During the testing phase, the model predicts the label of the unseen test data. Hence, supervised learning techniques such as deep learning-based ANN and machine learning-based SVM are analyzed and compared.

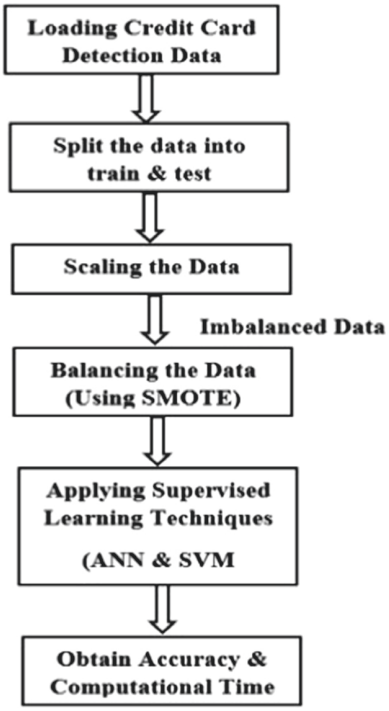

Fig. 1. Model framework using supervised learning techniques

Figure 1 shows the workflow of the proposed model. The imbalanced data is split into 70% for training and 30% for testing the data randomly. Hence, the data is scaled in the range of 0 and 1. Since the data is imbalanced, Synthetic Minority Oversampling Technique (SMOTE), an oversampling technique, is applied to balance the data. The SMOTE algorithm generates an arbitrary number of synthetic minority examples to balance the classifier's learning bias toward the minority class (i.e., fraudulent transactions) [15]. The resultant data is used to build supervised learning techniques such as deep learning-based Artificial Neural Network (ANN) and machine learning-based Support Vector Machine (SVM) models. Finally, these generated models would be evaluated by the classification's performance matrix, such as accuracy, precision, Recall, confusion matrix, F1-score, ROC-Curve, AUC-Curve, and computational time.

Overview of Artificial Neural Network (ANN)
Neural Network, as a classification technique, the training of the model is influenced by the initial parameter setting, bias, weight, and learning rate of the algorithm. This network's learning starts with some initial value, and the weights get renewed on each iteration. ANN works similar to the human brain. Propagated forward signals from the input layer to the hidden layer and then to the output layer would be implemented. The output layer's Job compares the output given by the hidden layer and the targeted output. If they are the same, that output will be updated. If an error is found, that will backpropagate the output, and then the weights get updated until the loss function is minimized [16].

This study' ANN framework consists of an input layer, four hidden layers, and an output layer. Two activation functions are compared with the corresponding accuracy of the model. In the first phase of the model training, ReLU (Rectified Linear Unit) Function will function as an activation function for the hidden layers. It acts like a linear activation function, which is easier to optimize [17]. The sigmoid function will be used as an activation function in the output layer for a binary classification problem to get the probability of the transaction in credit card is fraudulent or not. The second phase of the model training uses tanh (Hyperbolic Tangent) Function as an activation function for the hidden layers, and the sigmoid function will be used as an activation function in the output layer for a binary classification problem to get the probability of the credit card transaction is fraudulent or not. This model's significant parameters consist of the count of neurons in the input layer, hidden layer and output layer, activation function, batch size, learning rate, no. of epochs, dropout, and loss function as binary cross-entropy.

Overview of Support Vector Machine (SVM)
SVM considers all the input data and provides the output as a decision boundary as a Hyperplane that classifies both the fraudulent and non-fraudulent transactions. SVM learns a separating hyperplane, which maximizes the margin and produces good generalization ability. The distance between either nearest point is known as the margin. It finds a hyperplane that separates two classes (fraud or non-fraud) and has a high generalization capability that handles high-dimensional data. SVM transforms the attributes into high dimensional feature space and finds the optimal decision boundary that maximizes the classes' margin. A kernel function is used to remodel the dataset. This study uses a linear function that consists of only one hyperplane to classify the transactions into fraudulent or non-fraudulent.

Steps involved in developing an efficient supervised learning technique to detect credit card fraudulent transactions are as follows:

3.1 Dataset Used

The credit card data is available in the Kaggle data platform, in CSV format. It is used for research purposes that can be classified into fraudulent or non-fraudulent transactions. The dataset consists of 31 columns and 284,807 transactions of cardholders in Europe in 2013 for two days. Out of the 284,807 transactions, only 492 transactions are proportion fraudulent, making the data highly imbalanced. Two types of classes are identified in the dataset (i.e.) Fraudulent or non-fraudulent transactions.

Among the 31 features, 28 features named as V1, V2,……, V28 are the principal components derived from applying PCA, and the remaining three features, such as Time, Amount, and Class, have not been transformed by PCA. Class is a categorical variable describing whether the transaction is fraud or not. The amount is the transaction amount, and time denotes the interval elapsed between two successive transactions in the dataset. Because of the confidentiality of the data, original features are obfuscated [18]. However, we may guess that these features might be initially credit card number, type of transactions, transaction date-time, expiry date, purpose to use a credit card, CVV, credit card transaction history, transaction location, Job of the cardholders, cardholder name etc.

3.2 Data Splitting

The data is split into 70% for training and 30% for testing the new set of observations that predicts a fraudulent or non-fraudulent transaction randomly.

3.3 Data Scaling and Balancing

Except for the target variable, all other features are normalized into the range of 0 and 1 by using MinMax scaler from the sklearn library because it has only zeros and ones. The data has only 492 fraudulent transactions among 2,84,807 transactions, which shows that the data is highly imbalanced. Thus, the imbalanced data is balanced by the Synthetic Minority Oversampling Technique (SMOTE) which leads to an increase in the number of minority class observations (i.e., Fraudulent transactions) by creating synthetic observations [15]. Among the fraudulent transactions (minority class), k-Nearest Neighbors (KNNs) for each of the samples in the fraudulent transaction are identified. Then a line is drawn between the neighbors and generates random points on the line [19].

3.4 Feature Selection and Model Building

From the Oversampled data, the features are selected by feature selection methods by using mutual info classification function for the models. It is used to select the impacted features into the model, and the percentage of significant features is selected by using the select percentile function. In this study, supervised learning techniques such as deep learning-based ANN and machine learning-based SVM is implemented to identify the credit card fraudulent transactions with the training data.

3.5 Model Validation

In this study, the deep learning-based ANN model is validated through the validation_split argument in the Keras library's fit function which ranges from 0 to 1. It divides the training set accordingly by the variable' value. Hence, the first set is used for training, and the next set is used for validation after each epoch. For the machine learning-based SVM model, k-fold cross-validation is used for validating the model. It has a single parameter, k which subject to the count of different groups which splits the considered sample of data. The study considered the value of k as 10, i.e., 10-fold cross-validation which utilizes the unseen test data.

4 Evaluation Metrics

The generated algorithms can be evaluated by accuracy, Recall, precision, confusion matrix, and computational time to detect fraudulent credit card transactions.

The ANN model' first phase describes 97% of correctly predicted trained observations whether the transaction is fraud or not and 95% in testing the observations whether the transaction is fraud or not. Furthermore, the second phase of the ANN model describes 97% of correctly predicted trained observations whether the transaction is fraud or not and 98% in testing the observations on whether the transaction is a fraud or not. Also, SVM' training and testing accuracies are about 94% and 97% in predicting whether the observation is fraudulent or not.

Table 1 describes the Precision, Recall, and F1-Score of each model. Here Class 0 represents the non-fraudulent transactions, and Class 1 represents the fraudulent transactions. The first phase of the ANN model correctly predicts the fraudulent transactions with 3% and 100% for the non-fraudulent transactions. The second phase of the ANN model predicts fraudulent transactions with 8% and non-fraudulent transactions with 100% correctly. Also, the SVM model has 100% precision concerning ethical transactions and 6% for non-ethical transactions.

Moreover, for the first phase of the deep learning-based ANN model, the Recall is 93% correctly corresponding to fraudulent transactions, and the non-fraudulent transactions are about 95%. Moreover, for the second phase of the deep learning-based ANN model, the correctly concerning the fraudulent transactions are about 98%. Along with that, the correctly concerned non-fraudulent transactions are around 90%. For machine learning-based SVM, the Recall for fraudulent transactions is 92% and for non-fraudulent transactions is 98%.

The first phase of the deep learning-based ANN model's performance concerning the fraudulent transactions is 6% and of non-fraudulent transactions is about 97%. The second phase of the deep learning-based ANN model evaluates 15% for the fraudulent transactions and 99% corresponding to the non-fraudulent transactions. For machine learning-based SVM, the performance corresponding to the fraudulent transaction is 11% and to the non-fraudulent transactions is around 99%.

Table 1. Precision, Recall, and F1-Score of each model

Models		Precision	Recall	F1-Score
ANN_Model_1	Class 0	100%	95%	97%
	Class 1	30%	93%	60%
ANN_Model_2	Class 0	100%	98%	99%
	Class 1	80%	90%	15%
SVM	Class 0	100%	98%	99%
	Class 1	60%	92%	11%

The confusion matrix evaluates the generated classification algorithms' performance on a set of test data. Table 2. shows different ratios of the confusion matrix such as True Negative (TN) as the number of predicted non-fraudulent transactions, False Negative (FN) as the number of fraudulent transactions predicted as non-fraudulent transactions, False Positive (FP) as the number of non-fraudulent transactions predicted as fraudulent transactions and True Positive (TP) as the number of predicted fraudulent transactions.

Table 2. Ratios of Confusion Matrix of each model

Ratios	ANN_Model_1	ANN_Model_2	SVM
TN	81065	83943	83212
FN	9	13	11
FP	4242	1364	2095
TP	127	123	125

ROC-Curve is a probability curve obtained by plotting the True Positives on the y-axis and False Positives on the x-axis. AUC represents the measure of separability. Both phases of the Deep Learning-based ANN model have an AUC-score of 94%, and Machine Learning-based SVM model has an AUC-score of 95%. It implies that each model has a reasonable degree of separability as plotted in Fig. 2.

5 Results and Discussions

Each of the generated supervised learning techniques, such as deep learning-based ANN and machine learning-based SVM, is compared with their accuracy and computational time under the training and testing phase of each model is illustrated in Table 3.

Comparatively, it is identified that the second phase of the ANN model has maximum training and testing accuracy with minimum computational time in the training and testing phase of the model. According to the results, the preferable supervised technique for detecting fraudulent transactions in credit cards is Artificial Neural Network (ANN) with tanh (Hyperbolic Tangent) function as an activation function in the hidden layers.

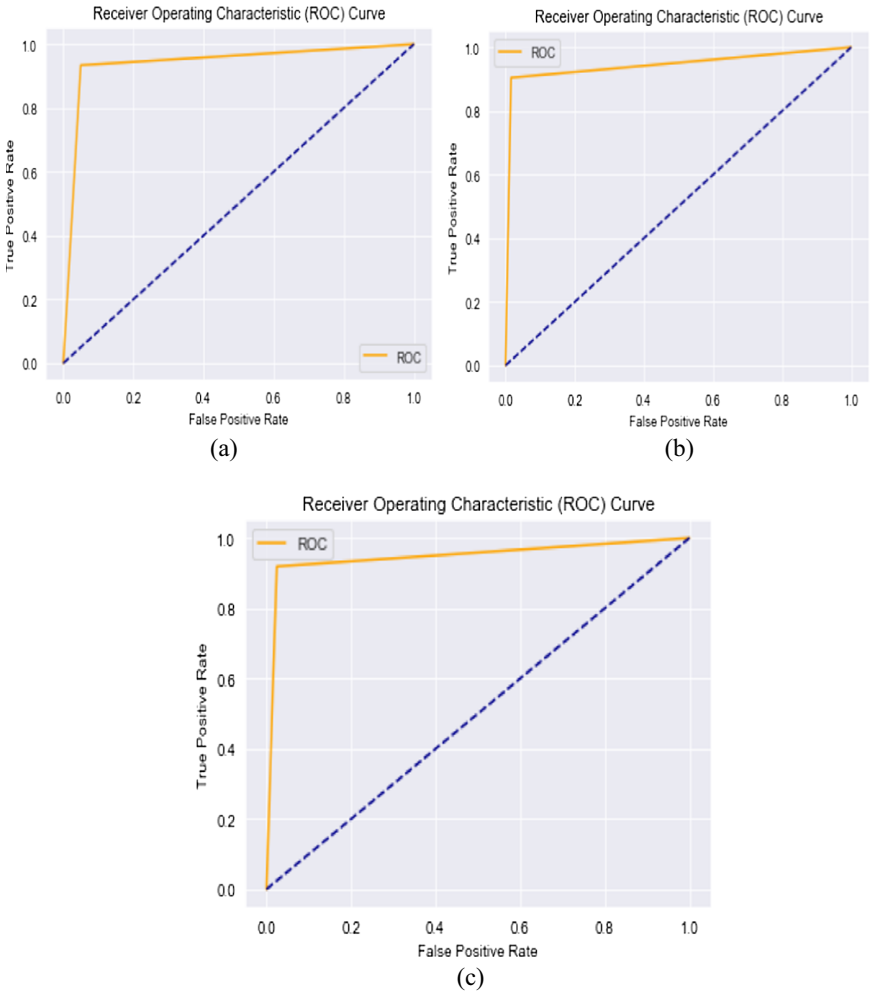

Fig. 2. (a) Roc-Auc Curve for ANN_ Model_1 (b) Roc-Auc Curve for ANN_ Model_2 (c) Roc-Auc Curve for SVM

Table 3. Comparison of each model with Accuaracy & Computational Time

Models	Accuracy		Computational time	
	Training accuracy	Testing accuracy	Training phase	Testing phase
ANN_Model_1	97%	95%	1865 s	0.10 s
ANN_Model_2	97%	98%	1816 s	0.04 s
SVM	94%	97%	2310 s	181.13 s

6 Conclusion

Credit Card fraud costs enormous losses to the customers as well as the financial companies. Fraudsters continuously find different ways of patterns and tactics to commit illegal actions. Thus, an efficient fraud detection system has become a need for users, banks, and financial institutions to reduce their losses. It has been observed that the imbalanced dataset available in the public domain gives biased results while detecting fraudulent credit card transactions. Hence, the considered credit card data is been split into 70:30 ratios.

Further, the data has been scaled by Minmax scaler and has applied the SMOTE technique to balance the data. Then, Deep Learning-based ANN and Machine Learning based SVM models are built to detect fraudulent and non-fraudulent transactions. ANN with the Backpropagation algorithm has the advantage of parallel processing capability. Also, SVM finds a hyperplane that separates two classes (fraud or non-fraud) and has a high generalization capability that handles high-dimensional data. The study shows that ANN with tanh as an activation function in hidden layers is an efficient classification to detect fraudulent transactions in credit cards.

Real-time data that describes the features for identifying the frauds in credit cards can be used for further study. Various other deep learning-based and machine learning-based techniques can be built and compared with different parameters, the activation function, loss function, and optimizer.

References

1. Saraswathi, E., Kulkarni, P., Khalil, M.N., Chandra Nigam, S.: Credit card fraud prediction and detection using artificial neural network and self-organizing maps. In: 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, pp. 1124–1128 (2019). https://doi.org/10.1109/ICCMC.2019.8819758
2. Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., Beling, P.: Deep learning detecting fraud in credit card transactions. In: 2018 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, pp. 129–134 (2018). https://doi.org/10.1109/SIEDS.2018.8374722
3. Pillai, T.R., Hashem, I.A.T., Brohi, S.N., Kaur, S., Marjani, M.: Credit card fraud detection using deep learning technique. In: 2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA), Subang Jaya, Malaysia, pp. 1–6 (2018). https://doi.org/10.1109/ICACCAF.2018.8776797
4. Prusti, D., Rath, S.K.: Fraudulent transaction detection in credit card by applying ensemble machine learning techniques. In: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, pp. 1–6 (2019). https://doi.org/10.1109/ICCCNT45670.2019.8944867
5. Wang, C., Wang, Y., Ye, Z., Yan, L., Cai, W., Pan, S.: Credit card fraud detection based on whale algorithm optimized BP neural network. In: 2018 13th International Conference on Computer Science & Education (ICCSE), Colombo, pp. 1–4 (2018). https://doi.org/10.1109/ICCSE.2018.8468855
6. Dubey, S.C., Mundhe, K.S., Kadam, A.A.: Credit card fraud detection using artificial neural network and backpropagation. In: 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, pp. 268–273 (2020). https://doi.org/10.1109/ICICCS48265.2020.9120957

7. Khine, A., Khin, H.W.: Credit card fraud detection using online boosting with extremely fast decision tree. In: 2020 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, pp. 1–4 (2020). https://doi.org/10.1109/ICCA49400.2020.9022843
8. Raghavan, P., Gayar, N.E.: Fraud detection using machine learning and deep learning. In: 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, pp. 334–339 (2019). https://doi.org/10.1109/ICCIKE47802.2019.9004231
9. Padmanabhuni, S.S.H., Kandukuri, A.S., Prusti, D., Rath, S.K.: Detecting default payment fraud in credit cards. In: 2019 IEEE International Conference on Intelligent Systems and Green Technology (ICISGT), Visakhapatnam, India, pp. 15–153 (2019). https://doi.org/10.1109/ICISGT44072.2019.00018
10. Vimala Devi, J., Kavitha, K.S.: Fraud detection in credit card transactions by using classification algorithms. In: 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, pp. 125–131 (2017). https://doi.org/10.1109/CTCEEC.2017.8455091
11. Kazemi, Z., Zarrabi, H.: Using deep networks for fraud detection in the credit card transactions. In: 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, pp. 0630–0633 (2017). https://doi.org/10.1109/KBEI.2017.8324876
12. Popat, R.R., Chaudhary, J.: A survey on credit card fraud detection using machine learning. In: 2018 IEEE 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, pp. 1120–1125 (2018). https://doi.org/10.1109/ICOEI.2018.8553963
13. Gyamfi, N.K., Abdulai, J.: Bank fraud detection using support vector machine. In: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, pp. 37–41 (2018). https://doi.org/10.1109/IEMCON.2018.8614994
14. Shen, R.T., Deng, Y.: Application of classification models on credit card fraud detection. In: 2007 International Conference on Service Systems and Service Management, Chengdu, pp. 1–4 (2007). https://doi.org/10.1109/ICSSSM.2007.4280163
15. He, H., Bai, Y., Garcia, E.A., Li, S.: ADASYN: adaptive synthetic sampling approach for imbalanced learning. In: 2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Fraud Detection in Credit Card Transaction Using Supervised Learning Techniques 60 Department of Data Science, Christ (Deemed to be University), Pune Lavasa Campus Intelligence), Hong Kong, pp. 1322–1328 (2008). https://doi.org/10.1109/IJCNN.2008.4633969
16. Brownlee, J.: A Gentle Introduction to the Rectified Linear Unit (ReLU), Machine Learning Mastery, 9 January 2019
17. Demla, N., Aggarwal, A.: Credit card fraud detection using SVM and reduction of false alarms. Int. J. Innov. Eng. Technol. (IJIET) **7**(2), 176–182 (2016)
18. Kaggle, Credit Card Fraud Detection (2018)
19. Bhattacharyya, I.: SMOTE and ADASYN (Handling Imbalanced Data Set), Medium, 3 August 2018