Credit Card Fraud Detection and Classification Using Deep Learning with Support Vector Machine Techniques

First Author[1*], Second Author[1], Third Author[2], and Fourth Author[2]

[1]Affiliation, Town/City, Country
firstname.secondname@springernature.com

Abstract. Detecting credit card fraud is a critical problem online vendor's face in the finance marketplace. Many sectors of the financial sector suffer from fraud and heavy financial losses due to the rapid and fast growing of modern technologies. The support vector machine (SVM) and multi-layer perceptron Learning (MLP) techniques are used to quantify the uncertainty of credit card fraud detection and classification. Through experimental analysis, the accuracy of the SVM and MLP techniques is 94.59% and 91.21%, respectively. Experimental results show that SVM and MLP techniques are classified credit fraud transactions with more than 90% accuracy.

Keywords: Classification, Machine Learning, Deep Learning, Data Analytics.

1 Introduction

A growing threat to the finance industry, corporations, and governments is financial fraud. A criminal act of deception to gain financial gain can be defined as fraud. The increased use of credit cards can be attributed to the high reliance on Internet technology. Credit card fraud rates have also risen as credit card transactions have become more prevalent for online and offline transactions. There are two types of credit card fraud: internal and external.

Financial institutions have been severely affected by fraudulent credit card transactions. According to a recent report, credit card fraud accounted for 27.85 billion dollars in losses in 2018. It was a 16.2% increase over 23.97 billion dollars in losses in 2017; estimates predict 35 billion dollars to be lost by 2023 (Tingfei et al., 2020) [1]. Fraud monitoring and prevention can reduce these losses. Fraud monitoring and prevention can reduce these losses. Nonetheless, class imbalances in the datasets make it challenging to detect credit card fraud from a learning perspective (Dal Pozzolo et al., 2017) [2]. Many problems hinder credit card fraud detection, but class imbalance is the most important (Makki et al., 2019) [3]. Real-world ML applications suffer from class imbalance problems where datasets have an uneven distribution of classes (Rani, Singh, et al., 2022 [4]; Rani, Verma, et al., 2022 [5]).

Similar tasks can be accomplished by numerous machine learning algorithms (Bhattacharyya et al., 2011 [6]; Seeja & Zareapoor, 2014 [7]). Each transaction is classified as legitimate or fraudulent by the algorithm in such a task. Supervised and unsupervised machine learning classifiers have been proposed to detect credit card fraud (Lucas & Jurgovsky, 2020) [8]. Supervised ML classifiers can teach the behavior of the customer(s) and fraudsters by using labelled transaction data. However, unsupervised machine learning does not rely on labelled data; it observes outliers. ML classifiers that are supervised produce fewer false alarms than those that are unsupervised. In this study, supervised ML classifiers are considered along with deep learning. In this paper, Multi-Layer Perceptron (MLP) is used to detect credit card fraudulent transactions and Support Vector Machine (SVM) is used to classify the credit card fraud transactions.

This paper makes the following significant contributions:

- Data preprocessing has been performed, so errors and malware are effectively eliminated.
- The deep learning (ML) technique is considered for detecting credit card fraud transactions.
- The SVM-supervised ML classifiers were implemented on the public data to classify credit card fraud transactions.
- The performance of the deep learning and machine learning technique are compared based on the various performance parameters.

The remainder of the paper is organized as follows: Section 2 presents the related works based on the latest techniques and presents a comparative analysis based on their proposed method and objective. Section 3 gives a brief description of the proposed methodology. The result analysis and discussion of the dataset are presented in Section 4. Finally, the conclusion is discussed in Section 5.

2 Related Works

The past decade has seen much attention paid to fraud detection. The purpose of this section is to review various techniques used in the fraud detection domain of credit cards. Increasingly, fraud detection techniques have been proposed in related work.

There are two types of credit card fraud transaction: internal and external (Chaudhary & Mallick, 2012 [9]; Shen et al., 2007 [10]), but a broader classification has been made into three groups, namely, traditional card fraud (application, theft, fake, counterfeit, and account takeover), merchant fraud, and Internet frauds (site cloning, false merchant sites, and credit card generators). A study (Evans et al., 2015) [11] shows that in 2014 banks and businesses worldwide suffered fraud losses worth more than USD 16 billion, an increase of nearly USD 2.5 billion over the previous year's recorded losses. According to the report, 5.6 cents of every USD 100 were fraudulent or 5.6 % for each USD 100.

The latest research focused on developing a hybrid model combining RF, LR, Gradient Boosting (GB), and voting classifiers to identify the fraud transaction using credit card datasets (Sivanantham et al., 2021) [12]. According to the author, there was a maximum detection rate for RF and GB. The studies mentioned above dealt with fraud detection; however, the algorithms used varied according to the datasets.

Using machine learning methods, credit card fraud has been detected (Fanai & Abbasimehr, 2023 [13]; Ni et al., 2023 [14]). A supervised learning algorithm, which uses labelled datasets containing previous transactions to build ML techniques that can identify the fraudulent transactions, is highly effective in detecting credit card fraud. There are supervised learning techniques which contain logistic regression (Singadkar et al., 2021) [15], support vector machines (SVM) (Hussain et al., 2021) [16], decision trees (Mienye et al., 2019) [17], adaptive boosting (AdaBoost) (Randhawa et al., 2018) [18], random forest (Lin & Jiang, 2021) [19], and artificial neural networks (ANN)(Akande et al., 2021 [20]; Asha & KR, 2021 [21]; Dubey et al., 2020 [22]). Another study (Ileberi et al., 2022) [23] applied a genetic algorithm (GA) to feature selection to detect credit card fraud. After selecting features, ML models were trained using naive Bayes (NB), logistic regression (LR), decision trees (DT), ANNs, and random forests (RF). Various machine learning algorithms can detect fraud on credit cards using various algorithms, but random forest achieves the highest accuracy. A neural nestwork model based on artificial intelligence and machine learning (Ansari et al., 2023) [24], a distributed data mining system (Phua et al., 2010) [25], a sequence alignment algorithm based on a cardholder's spending profile, and an intelligent decision-making engine that uses meta-learning agents and fuzzy systems of artificial intelligence (Rani et al., 2021) [26].

Table 1: Research literature summary

Authors & Year	Proposed Method	Problem Statement	Objective

(Xuan et al., 2018) [27]	Random Forest	A weak classifier is used, and the data is not normalized	The standard/fraud behaviour features are trained using two different types of random forests to deal with fraud detection
(Randhawa et al., 2018) [18]	AdaBoost	Classification is computationally complex, and features are not selected properly.	An evaluation of various ML models for fraud detection using real-world credit card data.
(Dubey et al., 2020) [22]	Backpropagation Neural Network	In education, classical algorithms are used	The model is created using Artificial Neural Networks (ANN) technique with Backpropagation.
(Taha & Malebary, 2020) [28]	Gradient Boosting	The input space has no feature selection, resulting in a complex input space.	Combining bio-inspired optimization techniques with ML models may enhance the performance of the ML.
(Shukur & Kurnaz, 2019) [29]	Artificial Neural Network	Trial and error is the best way to choose activation functions	Proposed the combination of the ML and ANN technique
(Yee et al., 2018) [30]	Bayesian, Logistics and J48	Teaching different models is computationally complex	The Bayesian Logistic and J48 ML technique is used for fraud prediction.
(Save et al., 2017) [31]	Decision Tree	Transfer of data between directories is not possible	Design a novel technique for fraud detection using a tree-based ML technique.

3. Methodology

Large datasets can be used for decision-making and evaluating the probability of future events using machine learning methods. Fraud detection, marketing, and scientific discovery use machine learning insights (Alkhalili et al., 2021 [32]; Özdemir et al., 2019 [33]). In this paper, Multi-Layer Perceptron (MLP) is utilized to detect credit card fraudulent transactions and SVM is used to classify the credit card fraud transactions. The layout of the proposed methodology is presented in Figure 1.

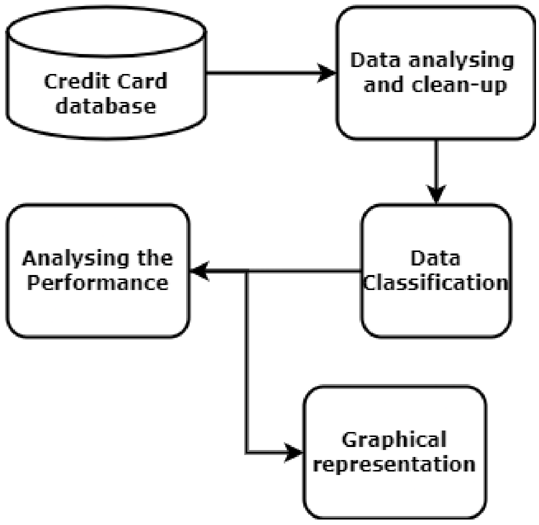

Figure 1: The layout of the proposed methodology.

3.1 MLP

In ANNs, the biological neural system is modelled mathematically. Multiplication, addition, and activation are the three main stages of this technique. An artificial neural network's value is multiplied by each weight. A full function, which includes all the inputs' weights, is on the middle side of the ANN. A weighted and activated input that is used activation phase, also known as the transfer function, is found at the end of the ANN. In MLP, each neuron is linked by its weights to form a feed-forward ANN. An MLP generates the desired outputs based on a set of inputs. The 28 input layer, 12 hidden layer, and 1 output layer make up the MLP, as shown in Figure 1. A hidden layer receives the input data from the input layers and forwards it to the output layer via the input layer (Krenker, n.d.; Ramchoun et al., 2016) [34].

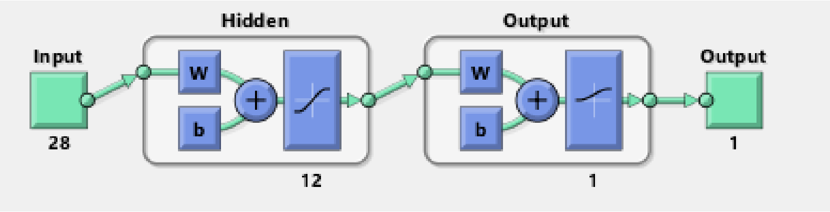

Figure 2: MLP network with 28 inputs, 12 hidden layers and 1 output.

Perceptrons with multiple input, input, and output layers are called multi-layer perceptions. Each node uses encoders. When the weighted sum of the inputs is computed, the activated function adds bias. Research can be done by removing and ignoring individual transistors during external network construction (Asha & KR, 2021) [21].

$$X_F^2 = \frac{12N}{K(K+1)}\left[\sum_j R_J^2 - \frac{K(K+1)^2}{4}\right] \qquad (1)$$

R_j represents the algorithm j's average ranking out of the total set of algorithms K, N, and K

3.2 Support Vector Machine (SVM)

The SVM can classify, predict, recognize patterns, and detect outliers (Pouyan et al., 2014) [35]. On the credit card dataset, SVMs are used for prediction and classification. Credit card transactions are classified into two categories using the SVM algorithm: fraud and genuine. The hyperplane acts as the decision-maker in the SVM. Kernel representation and margin optimization are the two important characteristics of SVM technique strength.
The optimal hyperplane has the following characteristics:

$$Y_i\left[\left(V^T x_i\right) + b\right] \geq \geq 1,\ i = 1, 2, 3, ..., n, \qquad (2)$$

An objective function can be seen in equation (2):

$$\varphi(vv) = \|(vv)\| \qquad (3)$$

A kernel function is defined in the following way: x_i is the average vector to the hyper-plane, x_i is the credit card fraud transaction to classify, and y_i is the type of credit card transaction that point fits to.

$$k\left(x_1, x_2\right) = (\emptyset\left(x_1\right), \emptyset\left(x_2\right) \qquad (4)$$

Where $\emptyset$: $X \longrightarrow D$ maps transactions used as the input space X to higher dimensional space D. The credit card fraud dataset is processed using KF as distinct transactions; resultant is mentioned in the following:

$$\{v, x\} + b = 0 \qquad (5)$$

Here is how an SVM is classified:

$$\sum_i^n \left(\alpha_i, y_i, k\left(x_i, x\right) + b\right) = 0 \qquad (6)$$

The kernel function (KF) inclination is determined based on the various dataset with classification requirements. In cryptography, there are 6 easily recognizable kernel functions available such as Gaussian matrix kernel (matrix kernel), polynomial function, normalized polynomial function, precompiling kernel, and string kernel. For classification tasks, $(k(x, y) \leq x, y\ *\ \wedge D * \wedge \mathrm{D})$ is used as the polynomial kernel function. The best-selected features are applied to the SVM algorithm to build a classification model. In addition to being famous for the solution to classification problems, the SVM is also accomplished of dealing with high dimensions dataset.

4. Result Analysis and Discussion

We have considered deep learning and machine learning technique for detecting and classifying credit card fraud transactions. The performance of both models is observed based on accuracy, recall, precision and specificity parameters. The result analysis and discussion of the proposed model is designed based on the mentioned Figure 3.

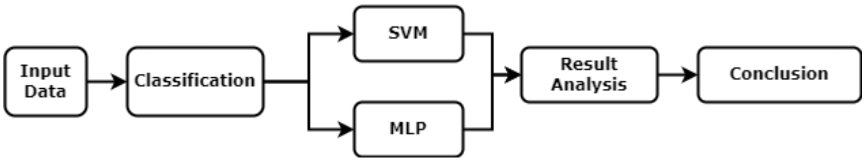

Figure 3: The analysis of the proposed model.

4.1 Performance Matrices

A binary classification task based on ML and DL is presented in this paper. The primary performance metric is the accuracy (AC) of the training and test data. The recall (RC), the precision (PR), and the specificity (SC) of each model are additionally computed (Kasongo & Sun, 2020) [36]. AUC can also assess the quality of a model's classification. The confusion metric measures the effectiveness of a classifier for a specific classification task.

- **True positive (TP):** An attack/intrusion accurately recognized as an attack.
- **True Negative (TN):** It is common for traffic patterns/traces to be classified as expected when they follow a normal pattern.
- **False positive (FP):** It is incorrectly labelled intrusive when legitimate network traces exist.
- **False Negative (FN):** Incorrectly classified attacks/intrusions as non-invasive.

$$AC = \frac{TN+TP}{TP+TN+FP+FN} \quad (7)$$

$$RC = \frac{TP}{FN+TP} \quad (8)$$

$$PR = \frac{TP}{FP+TP} \quad (9)$$

$$SC = \frac{TN}{TN+FP} \quad (10)$$

4.2 Dataset

This implementation considers a dataset accessible via a public web platform called "Kaggle". A dataset is available in CSV format. In September 2013, European cardholders used their credit cards to make transactions. The input variables are all numerical and the results of a PCA transformation. The original features of the data, as well as more background information, cannot be shared due to confidentiality issues. PCA has transformed all but two features: 'Time' and 'Amount'. The remainder is the principal components derived through PCA. Each transaction in the dataset is elapsed seconds from the last transaction until the first transaction. The amount feature can be used for cost-sensitive learning based on example-dependent transaction amounts. If fraud is detected, the response variable 'Class' will take value 1; otherwise, it will take value 0.

4.3 Result Discussion

We have implemented five SVM and MLP techniques in Matlab R2020a. The system configuration is an i5-4310U CPU with a 2.60 GHz clock speed. Each system's secondary and primary memory space is 1TB and 16GB, respectively.

Figure 4 shows the SVM model's accuracy, recall, precision and specificity. The SVM technique's performance is measured based on above mentioned performance parameters, as shown in the bar plot in Figure 4. As shown in the Figure, the recall has the highest value compared to other performance parameters. The SVM technique observed the maximum valid positive rate is 96.99%, and the number of accurate predictions is 95.59 %.

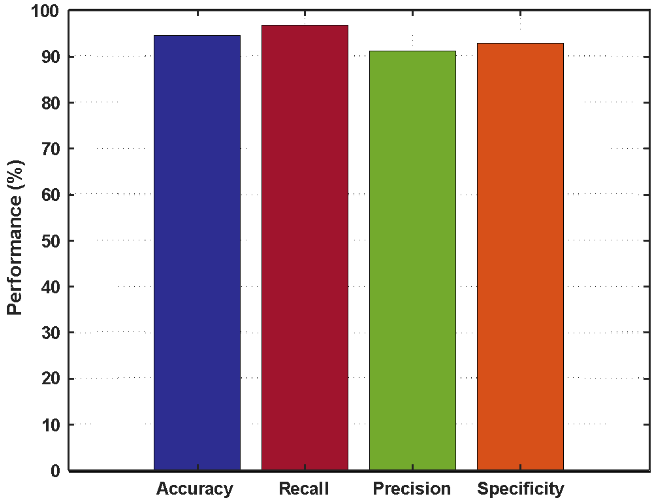

Figure 4: Performance analysis of the SVM technique based on accuracy, precision, recall, and specificity.

The SVM technique shows the percentage of correct and incorrect classification is 94.59 %, and 5.40 %, respectively, as shown in Figure 5.

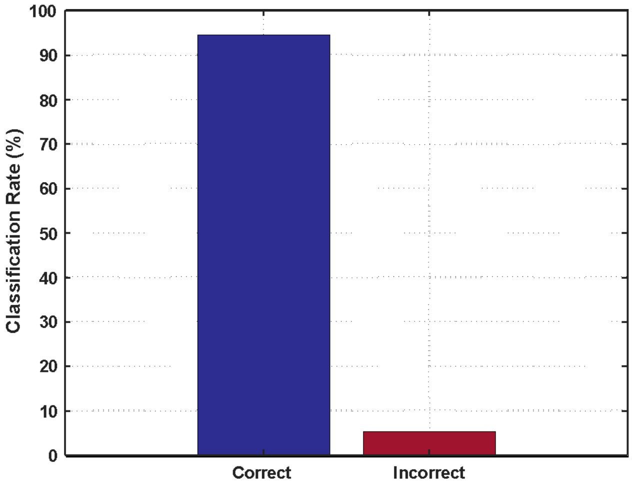

Figure 5: Classification rate of the SVM technique.

The performance analysis of the MLP technique is observed based on accuracy, recall, precision and specificity, as shown in Figure 6. The graphical representation of the MLP technique performance shows that the accuracy is 91.21 %, recall 95.08 %, precision 85.29 %, and specificity 88.51 %. Experimental results show that MLP gives the highest accuracy (91.21%) with the lowest error rate (0.003). The MLP has used 28 inputs, 12 hidden layers and 1 output. The MLP technique shows the percentage of correct and incorrect classification is 91.21% and 8 .78%, respectively, as mentioned in Figure 7.

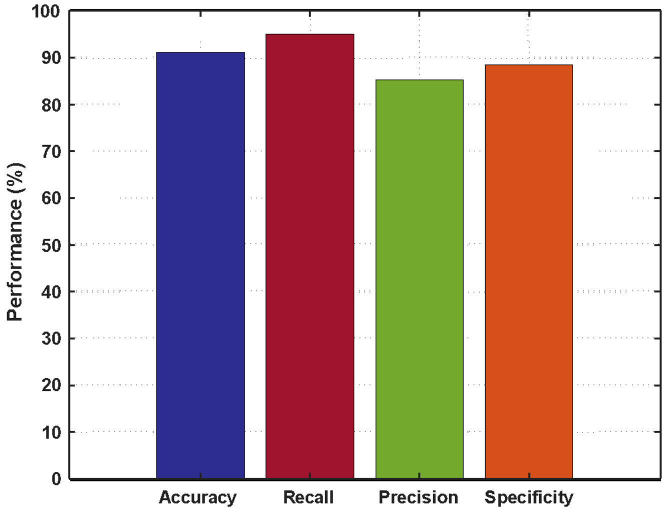

Figure 6: Performance analysis of the MLP technique based on accuracy, recall, precision and specificity.

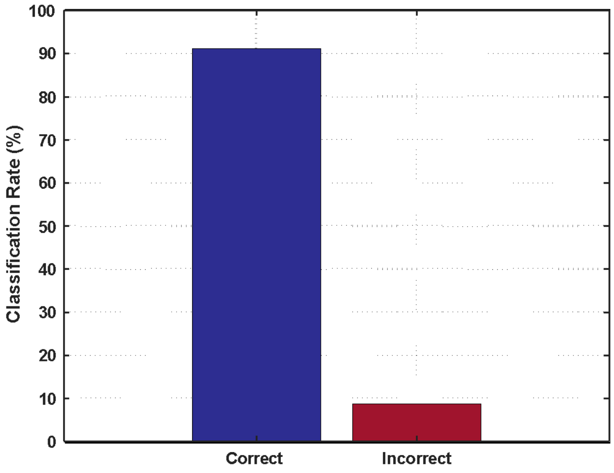

Figure 7: Classification rate of the MLP technique.

The cross-entropy represents the average square difference between outputs and input values. The lowest value of cross entropy indicates no error. Figure 8 displays that the average cross-entropy is almost 0 during the prediction of the credit card fraud transaction, which is very low. The selection of deep learning for predicting the credit card fraud transaction with train, test, and validation cross-entropy. The training cross-entropy is lower as compared to the test and validation.

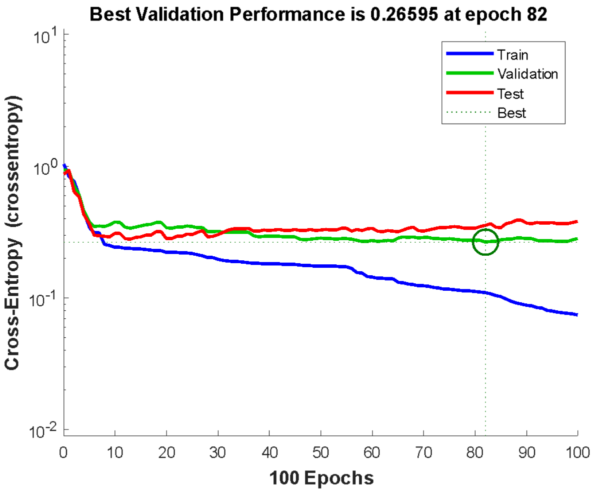

Figure 8: Cross Entropy of the MLP technique based on the train, test and validation set.

This visualization of the classification model shows the relation between input and results once the earliest results have been associated. An association table is created by transforming the anticipated results into a variable. Confusion metrics can be plotted using the association table as a heat map. While confusion metrics can be visualized using numerous built-in methods, they can also be defined and visualized according to the score to improve the correlation. The figure 9 demonstrates the confusion metrics of MLP based on the training, test, validation and complete data. The fundamental confusion metrics calculate the four main parameters: TP, FP, TN and FN. Figure 10 shows the comparative analysis of the SVM and MLP techniques based on the confusion metrics.

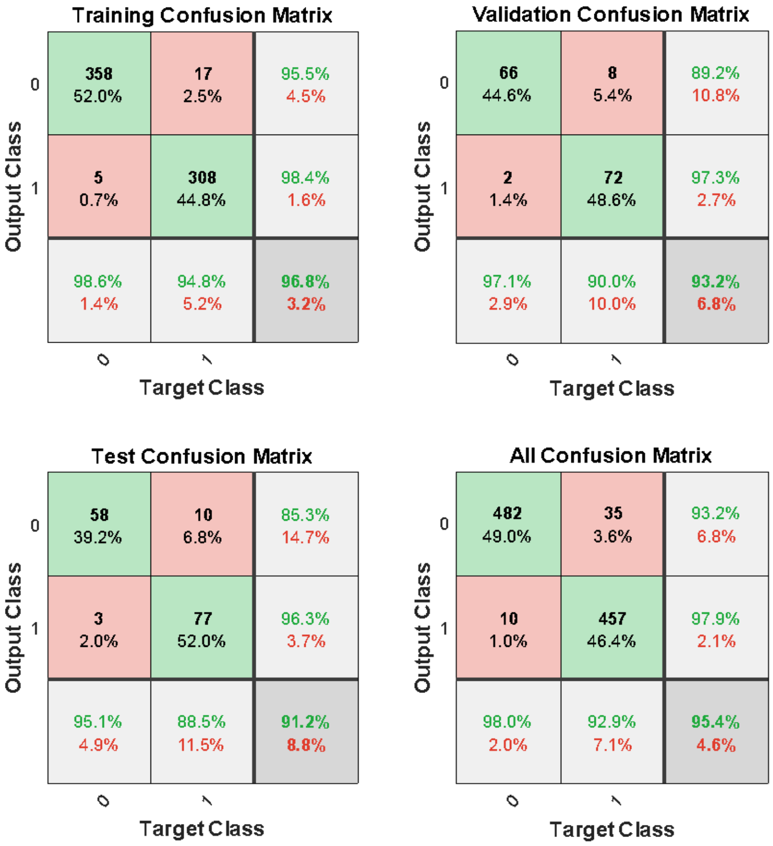

Figure 9: confusion matrix of the MLP technique for training, testing, validating and completing the dataset.

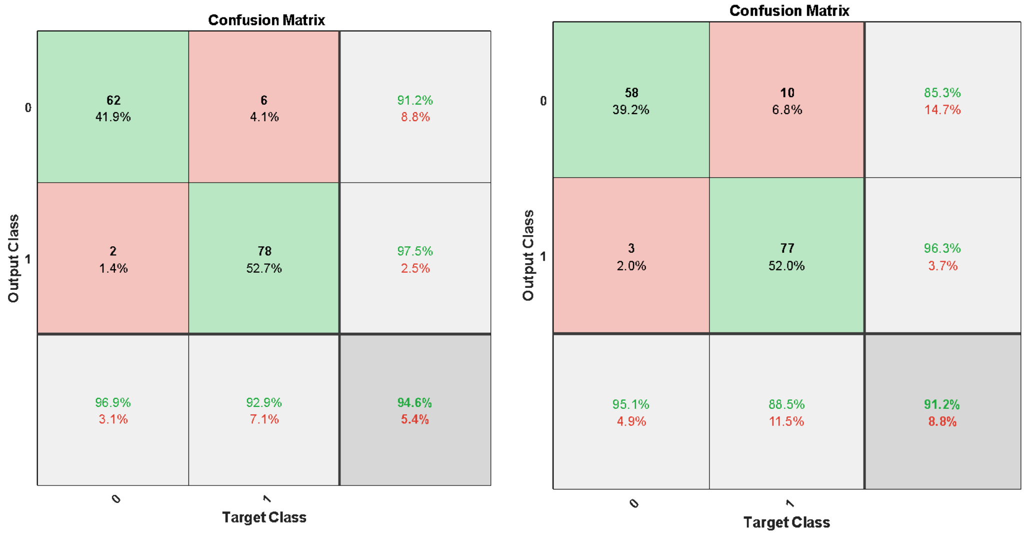

Figure 10: confusion matrix of the SVM and MLP techniques, respectively.

Figure 11 compares the various parameters like accuracy, recall, precision and specificity concerning the MLP and SVM techniques. The Figure's graphical representation shows that SVM has better performance than the MLP technique.

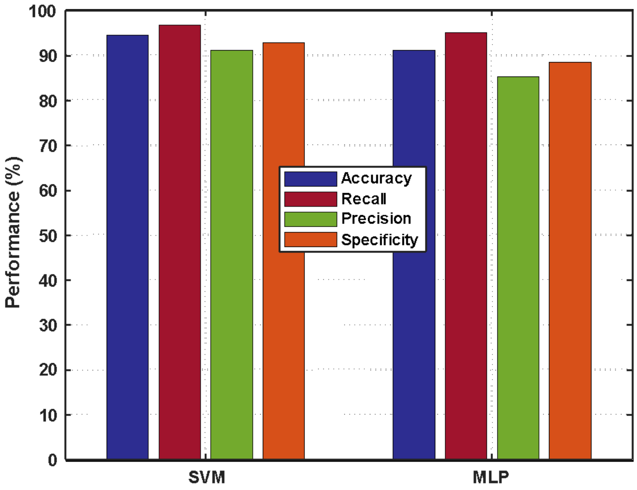

Figure 11: Comparative analysis of the SVM and MLP technique based on accuracy, recall, precision and specificity.

The SVM and MLP technique shows the correct and incorrect classification percentage is 94.59 %, 5.40 % and 91.21%, 8 .78%, respectively, as shown in Figure 12. The SVM techniques show a higher correct classification rate than the MLP, But MLP observed a higher incorrect classification rate. The MLP did not consider any suspicious transaction in the correctly classified transaction.

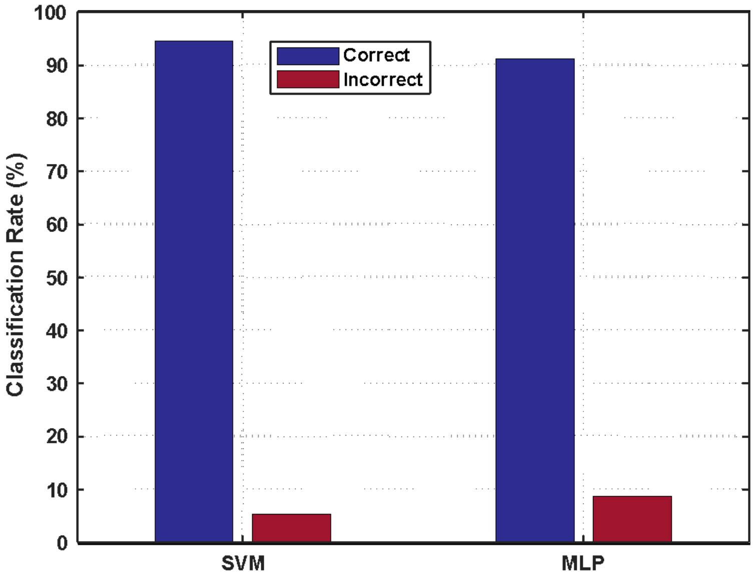

Figure 12: Comparative analysis of the classification rate of the SVM and MLP technique

5. Conclusion

Financial institutions have recently become especially concerned about credit card fraud. The need for investigating different reliable ways of detecting fraudulent credit card transactions still exists, despite the existing methods used in the past to detect fraudulent activities. The paper uses machine and deep learning techniques to detect and classify credit card fraud transactions. The accurately predictive class is high with reduced false alarms. The accuracy percentage for the SVM and MLP is 94.59% and 91.21%. Compared to the MLP technique, the accuracy of the SVM technique is observed to be the highest. The experimental result shows that SVM is considered some missed or suspicious transaction, but MLP directly rejects it and counts it as an incorrect or fraudulent transaction.

Reference

[1] Tingfei, H., Guangquan, C., & Kuihua, H. (2020). Using variational auto encoding in credit card fraud detection. *IEEE Access*, *8*, 149841–149853.

[2] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems*, *29*(8), 3784–3797.

[3] Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M.-S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. *IEEE Access*, *7*, 93010–93022.

[4] Rani, P., Singh, P. N., Verma, S., Ali, N., Shukla, P. K., & Alhassan, M. (2022). An Implementation of Modified Blowfish Technique with Honey Bee Behavior Optimization for Load Balancing in Cloud System Environment. *Wireless Communications and Mobile Computing*, *2022*, 1–14. https://doi.org/10.1155/2022/3365392

[5] Rani, P., Verma, S., Yadav, S. P., Rai, B. K., Naruka, M. S., & Kumar, D. (2022). Simulation of the Lightweight Blockchain Technique Based on Privacy and Security for Healthcare Data for the Cloud System: *International Journal of E-Health and Medical Communications*, *13*(4), 1–15. https://doi.org/10.4018/IJEHMC.309436

[6] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602–613.

[7] Seeja, K. R., & Zareapoor, M. (2014). Fraudminer: A novel credit card fraud detection model based on frequent itemset mining. *The Scientific World Journal*, *2014*.

[8] Lucas, Y., & Jurgovsky, J. (2020). Credit card fraud detection using machine learning: A survey. *ArXiv Preprint ArXiv:2010.06479*.

[9] Chaudhary, K., & Mallick, B. (2012). Credit Card Fraud: The study of its impact and detection techniques. *International Journal of Computer Science and Network (IJCSN)*, *1*(4), 31–35.

[10] Shen, A., Tong, R., & Deng, Y. (2007). Application of classification models on credit card fraud detection. *2007 International Conference on Service Systems and Service Management*, 1–4.

[11] Evans, D. S., Chang, H., & Joyce, S. (2015). The impact of the US debit-card interchange fee regulation on consumer welfare. *Journal of Competition Law and Economics*, *11*(1), 23–67.

[12] Sivanantham, S., Dhinagar, S. R., Kawin, P., & Amarnath, J. (2021). Hybrid approach using machine learning techniques in credit card fraud detection. *Advances in Smart System Technologies: Select Proceedings of ICFSST 2019*, 243–251.

[13] Fanai, H., & Abbasimehr, H. (2023). A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection. *Expert Systems with Applications*, 119562.

[14] Ni, L., Li, J., Xu, H., Wang, X., & Zhang, J. (2023). Fraud Feature Boosting Mechanism and Spiral Oversampling Balancing Technique for Credit Card Fraud Detection. *IEEE Transactions on Computational Social Systems*.

[15] Singadkar, G., Mahajan, A., Thakur, M., & Talbar, S. (2021). Automatic lung segmentation for the inclusion of juxtapleural nodules and pulmonary vessels using curvature based border correction. *Journal of King Saud University-Computer and Information Sciences*, *33*(8), 975–987.

[16] Hussain, S. S., Reddy, E. S. C., Akshay, K. G., & Akanksha, T. (2021). Fraud detection in credit card transactions using SVM and random forest algorithms. *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 1013–1017.

[17] Mienye, I. D., Sun, Y., & Wang, Z. (2019). Prediction performance of improved decision tree-based algorithms: A review. *Procedia Manufacturing*, *35*, 698–703.

[18] Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit card fraud detection using AdaBoost and majority voting. *IEEE Access*, *6*, 14277–14284.

[19] Lin, T.-H., & Jiang, J.-R. (2021). Credit card fraud detection with autoencoder and probabilistic random forest. *Mathematics*, *9*(21), 2683.

[20] Akande, O. N., Misra, S., Akande, H. B., Oluranti, J., & Damasevicius, R. (2021). A Supervised Approach to Credit Card Fraud Detection Using an Artificial Neural Network. *Applied Informatics: Fourth International Conference, ICAI 2021, Buenos Aires, Argentina, October 28–30, 2021, Proceedings 4*, 13–25.

[21] Asha, R. B., & KR, S. K. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings*, *2*(1), 35–41.

[22] Dubey, S. C., Mundhe, K. S., & Kadam, A. A. (2020). Credit card fraud detection using artificial neural network and Backpropagation. *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 268–273.

[23] Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1), 1–17.

[24] Ansari, G., Rani, P., & Kumar, V. (2023). A Novel Technique of Mixed Gas Identification Based on the Group Method of Data Handling (GMDH) on Time-Dependent MOX Gas Sensor Data. In R. P. Mahapatra, S. K. Peddoju, S. Roy, & P. Parwekar (Eds.), *Proceedings of International Conference on Recent Trends in Computing* (Vol. 600, pp. 641–654). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-8825-7_55

[25] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *ArXiv Preprint ArXiv:1009.6119*.

[26] Rani, P., Hussain, N., Khan, R. A. H., Sharma, Y., & Shukla, P. K. (2021). Vehicular Intelligence System: Time-Based Vehicle Next Location Prediction in Software-Defined Internet of Vehicles (SDN-IOV) for the Smart Cities. In F. Al-Turjman, A. Nayyar, A. Devi, & P. K. Shukla (Eds.), *Intelligence of Things: AI-IoT Based Critical-Applications*

and Innovations (pp. 35–54). Springer International Publishing. https://doi.org/10.1007/978-3-030-82800-4_2

[27] Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S., & Jiang, C. (2018). Random forest for credit card fraud detection. *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, 1–6.

[28] Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE Access, 8, 25579–25587.

[29] Shukur, H. A., & Kurnaz, S. (2019). Credit card fraud detection using machine learning methodology. *International Journal of Computer Science and Mobile Computing*, *8*(3), 257–260.

[30] Yee, O. S., Sagadevan, S., & Malim, N. H. A. H. (2018). Credit card fraud detection using machine learning as data mining technique. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1–4), 23–27.

[31] Save, P., Tiwarekar, P., Jain, K. N., & Mahyavanshi, N. (2017). A novel idea for credit card fraud detection using decision tree. *International Journal of Computer Applications*, *161*(13).

[32] Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of applying machine learning for watch-list filtering in anti-money laundering. *IEEE Access*, *9*, 18481–18496.

[33] Özdemir, A., Yavuz, U., & Dael, F. A. (2019). Performance evaluation of different classification techniques using different datasets. *International Journal of Electrical & Computer Engineering (2088-8708)*, *9*(5).

[34] Krenker, A. (n.d.). Bes? Ter, J., & Kos, A.(2011). Introduction to the Artificial Neural Networks. *Artificial Neural Networks-Methodological Advances and Biomedical Applications*.

[35] Pouyan, M. B., Yousefi, R., Ostadabbas, S., & Nourani, M. (2014). A hybrid fuzzy-firefly approach for rule-based classification. *The Twenty-Seventh International Flairs Conference*.

[36] Kasongo, S. M., & Sun, Y. (2020). A deep long short-term memory based classifier for wireless intrusion detection system. *ICT Express*, *6*(2), 98–103.