International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Mitigating Credit Card Fraud Using SMOTE Sampling and Artificial Neural Networks

Vansh Sharma
Department of Computer science and engineering.

Abstract- Banking and financial institutions are increasingly encountering the challenges of credit card fraud. Statistics suggest that each year financial institutions incur losses close to billions of dollars globally due to such frauds .Hence it is evident for financial institutions to continue to invest in advanced fraud detection systems to minimize the impact of credit card fraud on their bottom line and protect their customers from financial losses.Before deep diving into the solutions which can be proposed to solve the problem of credit card fraud , it is important to know the ways in which these frauds are taking place and what loopholes are being misused to catalyze these frauds .Hence in our research paper we first look at ways in which these frauds are taking place. Moreover, one of the other challenges to proposing a solution to this problem is the presence of highly imbalanced datasets to train the model , which motivates us to apply various techniques such as Synthetic Minority Oversampling Technique (SMOTE) to make the datasets balanced which will allow us to train the model better .We implement Artificial neural network + Recurrent neural network with auto-encoder architecture to make a model for one-class classification . The model uses these relationships to make predictions about the likelihood of fraud in new transactions. ANNs can be used to process large amounts of data and are particularly effective in detecting non-linear relationships between variables.

Keywords- Credit card fraud detection, Artificial neural network (ANN), Multilayer perceptron (MLP),Random forest (RF),Logistic regression (LR),Classification, Binary Classification.

I. INTRODUCTION

Machine Learning (ML) is a subfield of artificial intelligence (AI) that allows computers to learn from previous experience (data) and to improve on their predictive abilities without explicitly being programmed to do so. [1] In this work we implement ML methods for credit card fraud detection. Credit card fraud is defined as a fraudulent transaction (payment) that is made using a credit or debit card by an unauthorized user. [2] Credit card fraud is a major concern in the modern financial world, with financial institutions and individuals losing billions of dollars each year to fraudulent activities. The rise of electronic transactions has made it easier for fraudsters to perpetrate these crimes, and traditional fraud detection methods are often insufficient to keep up with their tactics. As such, it has become imperative for financial institutions and merchants to develop and implement advanced fraud detection systems to protect themselves and their customers from the financial losses associated with credit card fraud. According to the Federal Trade Commission (FTC), there were about 1579 data breaches amounting to 179 million data points whereby credit card fraud activities were the most prevalent. According to Visa reports about European countries, about 50% of the whole credit card fraud losses in 2008 are due to online frauds. [3]It has been estimated that each year Visa Mastercard credit card issuers lose approximately $700 Million in the US due to fraudulent credit card charges. [4] World wide fraud losses are still increasing: they have risen from $800 Million in 1989 to over $10 Billion in 1996.

In this research paper, we aim to provide a comprehensive overview of the state of the art in credit card fraud detection. This includes a discussion of the various techniques used to detect fraud, such as rule-based systems, artificial neural networks, decision trees, and others. We will examine the advantages and disadvantages of each method, as well as their performance metrics, including accuracy, precision, recall, and others. Additionally, we will explore the various challenges and limitations that exist in the field of credit card fraud detection, including the difficulty in obtaining and processing large amounts of data, the high rate of false positives, and the need for real-time processing. In this paper we are primarily using Artificial Neural Networks (ANN) to analyze the dataset.

Artificial Neural Networks (ANNs) have emerged as a promising solution for credit card fraud detection due to their ability to learn patterns and make predictions based on large amounts of data. ANNs have been shown to outperform traditional statistical methods in detecting fraudulent transactions, making them an attractive option for financial institutions looking to enhance their fraud detection capabilities. This paper aims to explore the use of ANNs for credit card fraud detection, examining their strengths and limitations and exploring the different approaches that can be taken to optimize their performance. Through this research, we hope to provide insights into the potential of ANNs for credit card fraud detection and contribute to the ongoing efforts to combat financial fraud. This information will be valuable for practitioners and researchers who are seeking to develop more effective and efficient fraud detection methods. Ultimately, our hope is that this paper will contribute to the ongoing effort to prevent and combat credit card fraud and protect individuals, financial institutions, and merchants from its devastating effect

II. LITERATURE REVIEW

In the banking sector, credit card fraud is a major issue, and machine learning algorithms have been widely utilized to spot fraudulent transactions. Traditional rule-based methods and machine learning-based methods can be broadly categorized in the literature on credit card fraud detection.

Rule-based techniques rely on a predetermined set of rules to find fraud. The amount of the transaction, the location of the transaction, and the time of day are only a few examples of the regulations that are often based on professional knowledge. Unfortunately, these techniques have limits when it comes to spotting novel and unheard-of fraud kinds, and they might not work against sophisticated fraud operations.

Hybrid strategies that mix rule-based and machine learning-based techniques have gained popularity in recent years. These strategies can combine the advantages of the two approaches and offer more effective fraud detection. Understanding the technologies involved in identifying credit card thefts and recognizing the various forms of credit card frauds are prerequisites for effectively combating credit card fraud. [5] [6] [7] For the purpose of detecting credit card fraud, various algorithms exist. [7] These are artificial neural network models that are based on machine learning and artificial intelligence [8][9], distributed data mining systems [10] [11], and a sequence alignment technique that takes into account the cardholder's spending history [1] [6], artificial intelligence-based intelligent decision engines [12], meta learning agents, and fuzzy based systems. [13] Using a random sample methodology, [18, 20] reports experimental findings showing that classifiers with the highest true positive rate and the lowest false positive rate are produced by intentionally distributing training data in a 50:50 ratio between fraud and non-fraud.Studies on a variety of strategies have been conducted in an effort to solve the problem of credit card fraud detection. These methods include, but are not limited to: decision trees, neural network models (NN), Bayesian networks (BN), expert systems, meta-learning agents, machine learning, pattern recognition, rule-based systems, logic regression (LR), support vector machines (SVM), and k-nearest neighbor (KNN). [17]

A fusion method based on Bayesian learning and the Dempster-Shafer theory FDS of Bayesian learning and Dempster-Shafer theory For the identification of credit card fraud, Dempster-Shafer theory and Bayesian learning incorporate data from both past and present behavior. [26][12][15] Every cardholder has a particular shopping style. The feedforward network is a popular neural network for pattern classification and consists of a linked set of artificial neurons. [26][27] Input, hidden, and output layers make up its three layers. The entering transaction sequence travels from the input layer via the concealed layer and out to the output layer. The term "forward propagation" refers to this. The training data for the ANN is compared to the incoming transaction sequence. The neural network is initially trained using a cardholder's typical behavior. The neural network then classifies the suspicious and non-suspicious transactions based on the suspicious transactions that have been transmitted backwards through it.

The network's generalization capabilities are provided via hidden layers. [16] Neural networks with one, and rarely two, hidden layers are frequently employed and have shown excellent performance. The computation time and risk of overfitting also rise as the number of hidden layers is increased. Overfitting results in subpar out-of-sample forecasting performance. Here, we examined a single hidden layer neural network structure.Decision tree, neural network, and naive bayes classifiers are the strategies that have been assessed. According to reports, neural network classifiers operate best with larger databases and require a lot of time to train the model. Although Bayesian classifiers are slower when used on new instances, they are more accurate, faster to train, and

adaptable for various data sets. The method uses a decision tree, naive Bayesian, and k-nearest neighbor algorithm to build three base classifiers. The performance was improved by 28% when the naive Bayesian algorithm was used as the meta-level algorithm to integrate the basis classifier predictions. [17]

S. Bhattacharyya et al. developed a model for the identification of credit card fraud using SVM, RF, and LR classifiers. They compared the output produced by the various classifiers and discovered that Random Forest was the model that performed the best. [21] Syeda, M., et al. (2002) separated the dataset into three sections: one for training, one for prediction, and one for fraud detection. They then attempted the Granular Neural Network (GNN) for accelerating the data mining process of fraud detection in order to provide successful results. [22] In order to identify fraudulent transactions, Jurgovsky, J., et al. (2018) developed a sequence classification system using Long Short-Term Memory (LSTM) networks. They discovered that the LTSM model outperformed the standard Random Forest classifier approach at spotting fraud. [23] AdaBoost and majority voting were utilized by Randhawa et al. (2018) [24] for all 12 of the models they used, however this did not address the issue of imbalanced data, which resulted in skewed accuracy of above 98% for the majority of the model

III. PROPOSED METHODOLOGY

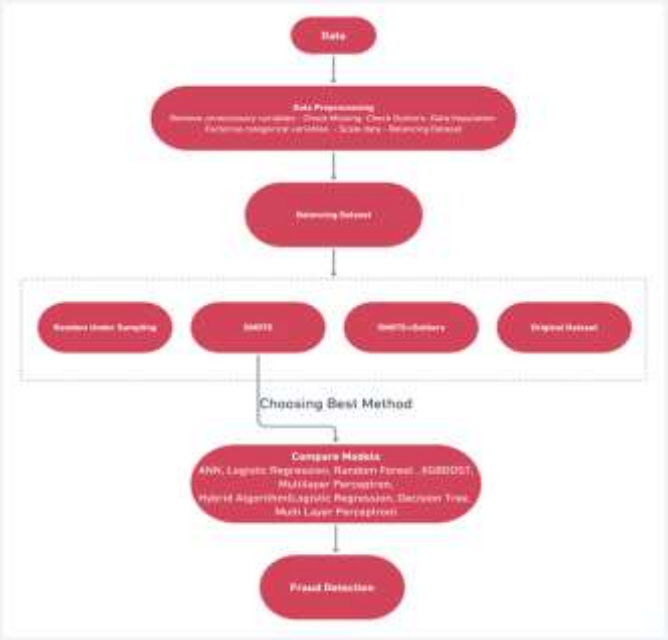

Fig. 1. Proposed Methodology

The proposed methodology for credit card fraud detection using SMOTE (Synthetic Minority Over-sampling Technique) + Outlier Analysis and ANN (Artificial Neural Network) can be outlined as follows:. Data Collection: Collect a large amount of credit card transaction data, which includes both legitimate and fraudulent transactions. This dataset should have a balanced distribution of fraud and non-fraud transactions.

Data Preprocessing: Clean the data and remove any missing or irrelevant data. Then, perform feature engineering to extract relevant features from the data. Feature engineering involves selecting the most important features that are likely to contribute to the detection of fraud.

Data Balancing: Since fraud transactions are typically a minority class, we need to balance the dataset. We can use SMOTE to generate synthetic data points for the minority class. This will help to balance the dataset and improve the performance of the model.

Balancing Dataset

Random Under Sampling

In machine learning and data analysis, random under-sampling is a method for balancing class distributions in a dataset. To match the size of the minority class (fraudulent transactions), it entails choosing at random a subset of instances from the majority class (in this case, non-fraudulent transactions).Because there are far less fraudulent transactions in our dataset than there are non-fraudulent transactions, we used random under-sampling to address the problem of class imbalance. Machine learning models trained on the data may perform poorly if there is a class imbalance because the models may get biassed in favour of the majority class and have trouble detecting instances of the minority class.Prior to randomly choosing the same number of examples from the majority class (i.e., non-fraudulent transactions), we would first determine the total number of instances in the minority class (i.e., the number of fraudulent transactions). Equal numbers of instances would be present in both classes in the resultant dataset, which can enhance the precision of machine learning models developed using the data.

SMOTE

To address the issue of data imbalance, the SMOTE approach is applied.

The data, which are simply the transactions, are trained using the smote approach.

This method is primarily employed to distinguish between legitimate cardholder transactions and fraud activities. The transaction data are initially kept in confluence form. As a result, the SMOTE method has trained the confluence data to distinguish between legal and fraudulent transactions. The synthetic minority oversampling method reduces the difference between fraudulent and legitimate transactions. Confluenced transactions are synthesized by the SMOTE()function parameters.

SMOTE + Outliers

SMOTE was used in this case, but only after the outliers had been eliminated. Note verification was crucial because most outliers are found in rows that are positive for fraud.Using SMOTE+Outliers was therefore necessary to determine whether eliminating the outliers would indeed improve model prediction.

Original Dataset

We also found out the precision-recall curve for the original dataset without performing any pre-processing to analyze if without performing any kind of balancing techniques could we use the original dataset

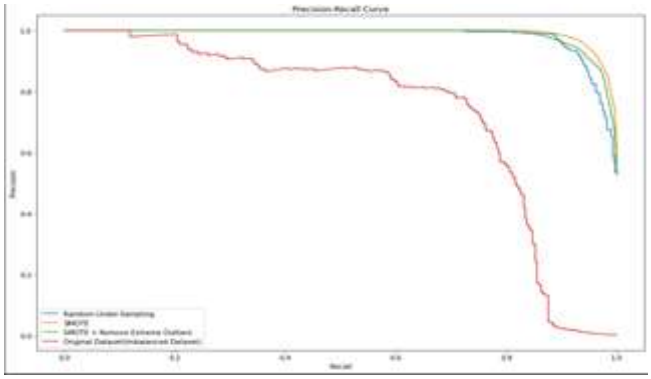

Fig. 2. Precision-recall curve

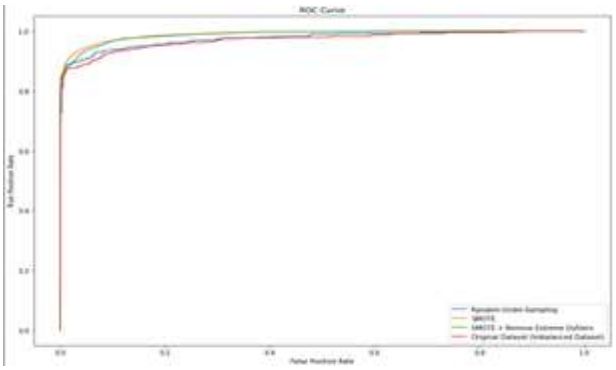

Fig. 3. ROC curve

We will utilize the dataset with SMOTE Method because it fits both the Precision-Recall and ROC-AUC curves the best.

Compare Models

Logistic Regression:

The supervised machine learning method known as the Logistic Regression (LR) classifier, also referred to as the Logit classifier, is frequently used for binary classification tasks. LR is a particular kind of linear regression in which the logit function is fed a linear function.

$$y = \alpha 0 + \alpha 1X1 + \alpha 2X2 + \cdots + \alpha nXn \quad (1)$$

$$p = 1/(1 + e{-}y) \quad (2)$$

where the range of p's value is 0 to 1. The probability, or q, is what defines how well a specific class will do in a prediction. The more closely q approaches 1, the better it predicts a given class.

Random Forest:

A machine learning technique called Random Forest is used for classification, regression, and other tasks. Multiple decision trees are combined in this ensemble method to increase forecasting accuracy and avoid overfitting.

The fundamental principle of a Random Forest is to aggregate the predictions made by various decision trees after they have been trained on various random samples of data. To avoid overfitting, each decision tree is constructed independently, utilising a different subset of the data and a unique set of characteristics. Each decision tree in the forest is constructed during training using a subset of the training data that is randomly selected with replacement (this process is known as "bootstrap aggregating" or "bagging"). Additionally, only a randomly chosen subset of the available features is taken into account at each split in the tree.

The Random Forest aggregates all of the decision trees' forecasts to arrive at a prediction. Each tree in a classification job predicts the input's class label, and the final prediction is formed by considering the vote of the majority of the tree predictions. When performing regression tasks, each tree forecasts a continuous value, and the final forecast is calculated by averaging the tree forecasts.

XGBoost:

Extreme Gradient Boosting, or XGBoost, is an ensemble learning technique that generates predictions using a number of decision trees. Sequential tree construction is used by XGBoost, where each tree is built to fix the flaws of the one before it.

The key difference between random forest and XGBoost is that random forest can handle missing values in the data, while XGBoost requires imputation of missing values prior to training. Random forest tends to have lower variance but higher bias compared to XGBoost, while XGBoost can be prone to overfitting if not regularized properly.

Multi-Layer Perceptron:

For supervised learning tasks like classification and regression, a multi-layer perceptron (MLP) kind of neural network is used. It is made up of several interconnected layers of neurons, each of which performs a weighted sum of its inputs before executing a nonlinear activation function. The network is able to learn progressively complicated representations of the input data because the output of one layer serves as the input to the following layer.

- **Input layer:** The input layer receives the input data, which is usually represented as a vector of features. Each neuron in the input layer corresponds to a single input feature.
- **Hidden layers:** The hidden layers of an MLP consist of multiple layers of interconnected neurons.
- **Output Layer:** The output layer of an MLP produces the network's final output. It consists of one or more neurons, depending on the number of output classes or the type of regression task.
- **Activation functions:** The activation functions used in an MLP introduce nonlinearity to the model, allowing it to learn complex patterns in the data.
- **Training:** The weights and biases in the network are changed during the training of an MLP in order to reduce the cost function, which calculates the discrepancy between the anticipated output and the actual output for a particular input.

ANN:

A supervised machine learning technique called an artificial neural network (ANN) draws inspiration from the inner workings of the human brain. The fundamental components of the simplest ANN are an input layer, a hidden layer, and an output layer.

- **Input Layer:-** The input layer is in charge of accepting input features. This layer does not do any calculation; rather, nodes merely transfer data (features) to the hidden layer. It provides data from the outside world to the network.
- **Hidden Layer:-** Nodes in the hidden layer are part of the abstraction that any neural network provides and are invisible to outside observers. The output layer receives the results after the hidden layer has processed the features entered through the input layer in a variety of ways.
- **Output Layer:-** This layer transmits the knowledge that the network has learned to the outside world.

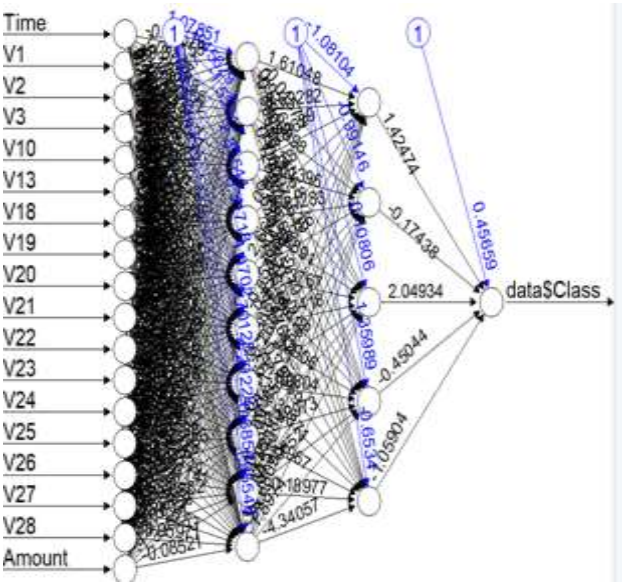

Fig. 4. ANN Architecture

Hybrid Algorithm(Logistic Regression, Decision Tree, Multi Layer Perceptron):

A hybrid algorithm combining logistic regression, decision tree, and multilayer perceptron (MLP) using a voting classifier can be created. The voting classifier is an ensemble learning technique that uses a majority vote system to integrate the predictions of various independent models.

The Voting Classifier is an ensemble classifier that combines multiple machine learning models to make a prediction. It takes a list of estimator objects as input and uses their predictions to make the final prediction by majority vote or weighted vote. In this case, we can use the Voting Classifier to combine the decision tree, logistic regression, and neural network

classifiers. By using the Voting Classifier, we can improve the accuracy and stability of the predictions made by our hybrid algorithm. The Voting Classifier considers the predictions of each classifier and combines them to make a final prediction. This approach can help us to reduce the bias and variance of our predictions, as well as to provide better performance on unseen data. One important consideration when using a Voting Classifier is to ensure that the base classifiers are diverse and complementary.

This means that each base classifier should have different strengths and weaknesses, and should be trained on different subsets of the data. By combining classifiers with different characteristics, the Voting Classifier can effectively reduce the overall error rate and improve the robustness of the model.Another important consideration is to use an odd number of base classifiers, so that there are no ties when making predictions. In addition, the base classifiers should not be too similar to each other, as this can lead to overfitting and reduce the performance of the ensemble. Overall, using a hybrid algorithm that combines multiple machine learning models and using a Voting Classifier to combine their predictions can be an effective approach for credit card fraud detection. By leveraging the strengths of each individual classifier, we can improve the accuracy and stability of our predictions, which can lead to better fraud detection and prevention.

IV. RESULTS AND DISCUSSION:

Fig. 5.

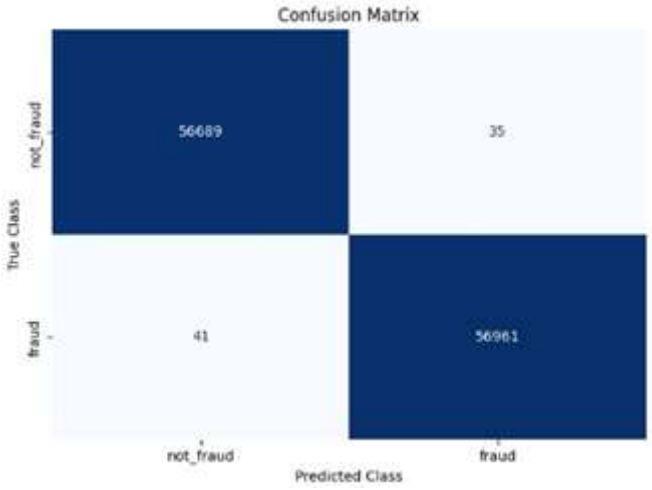

Fig. 6.

The model's performance in correctly categorizing both fraudulent and non-fraudulent transactions is demonstrated by the high number of True Positives (TP) and True Negatives (TN) it attained. Nevertheless, the model also generated a small number of false positives (FP) and false negatives (FN), meaning it misclassified a small number of transactions. The model is able to identify the bulk of fraudulent transactions, as evidenced by the relatively low ratio of False Negatives (FN) to True Positives (TP). The model seems to work well overall, however it may be improved to cut down on the amount of false positives and false negatives.

Model	Precision	Recall	F1-Score	Accuracy
1.Logistic Regression	0.97	0.92	0.95	0.95
2.Random Forest	0.99	1	0.99	0.99
3. XGBoost	0.99	1	0.99	0.99
4. Multilayer Perceptron	0.99	1	0.99	0.99
5. ANN	0.977	0.994	0.985	0.981
6. Hybrid Algorithm	0.99	1	0.99	0.99

The dataset used in this study contained a total of 284808 credit card transactions, with 492 fraud cases and 284315 non-fraud cases , after applying SMOTE there were 284315 fraud and non-fraud transactions in the dataset

The results showed that the ANN achieved an accuracy of 0.981, while the hybrid algorithm had an accuracy of 0.99933172713. This indicates that the hybrid algorithm outperformed the ANN in detecting credit card fraud, achieving a higher level of accuracy.

The results of this study demonstrate the effectiveness of the hybrid algorithm consisting of logistic regression, multi-layer perceptron, and decision tree in detecting credit card fraud. This algorithm combines the strengths of multiple machine learning techniques, resulting in a highly accurate fraud detection system.

The high accuracy of the hybrid algorithm can be attributed to several factors. Firstly, the logistic regression component of the algorithm is well-suited for binary classification problems like credit card fraud detection. Secondly, the multi-layer perceptron component is capable of learning complex relationships between input features and output labels, which can be beneficial in detecting fraudulent transactions. Finally, the decision tree component of the algorithm provides a simple and interpretable model that can help identify key features that contribute to fraud detection.

The results also show that the ANN was effective in detecting credit card fraud, achieving an accuracy of 0.981. However, the ANN was outperformed by the hybrid algorithm, indicating that the combination of multiple machine learning techniques can result in a more accurate fraud detection system.

In conclusion, the findings of this study suggest that the hybrid algorithm consisting of logistic regression, multi-layer perceptron, and decision tree is a highly effective method for detecting credit card fraud. This algorithm could be implemented by financial institutions and credit card companies to enhance their fraud detection systems and reduce the risk of fraudulent transactions.

REFERENCES

1. Burkov A. The hundred-page machine learning book. 2019;1:3–5.
2. Maniraj SP, Saini A, Ahmed S, Sarkar D. Credit card fraud detection using machine learning and data science. Int J Eng Res 2019; 8(09).
3. Dornadula VN, Geetha S. Credit card fraud detection using machine learning algorithms. Proc Comput Sci. 2019;165:631–41.
4. M. Syeda, Y.-Q. Zhang, and Y. Pan, “Parallel granular neural networks for fast credit card fraud detection,” In Proceedings of 2002 IEEE International Conference on Fuzzy Systems. FUZZ-IEEE’02, 2002. doi:10.1109/fuzz.2002.1005055
5. Barry Masuda, “Credit Card Fraud Prevention: A Successful Retail Strategy,” crime prevention, Vol. 6, 1986
6. Tej Paul Bhatla, Vikram Prabhu & Amit Dua “Understanding Credit Card Frauds,” 2003.
7. Linda Delamaire, Hussein Abdou, John Pointon, “Credit card fraud and detection techniques: a review,” Banks and Bank Systems, pp. 57-68, 2009.
8. Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick, “Credit card fraud detection using Bayesian and neural networks,” Interactive image-guided neurosurgery, pp.261-270, 1993.
9. Ray-I Chang, Liang-Bin Lai, Wen-De Su, Jen-Chieh Wang, Jen-Shiang Kouh, “Intrusion Detection by Backpropagation Neural Networks with Sample-Query and Attribute-Query,” Research IndiaPublications, pp.6-10, November 26, 2006.
10. Philip K. Chan ,Wei Fan, Andreas L. Prodromidis, Salvatore J. Stolfo, “Distributed Data Mining in Credit Card Fraud Detection,” IEEE Intelligent Systems ISSN, Vol. 14 , Issue No. 6, Pages: 67 – 74, November 1999.
11. C. Phua, V. Lee, K. Smith, R. Gayler, “A Comprehensive Survey of Data Mining-based Fraud Detection Research,” Artificial Intelligence Review, 2005
12. Russell, Norvig ,” Artificial Intelligence – A Modern Approach,” 2nd Edition, 2003.
13. Peter J. Bentley, Jungwon Kim, Gil-Ho Jung and Jong-Uk Choi, “Fuzzy Darwinian Detection of Credit Card Fraud,” In the 14th Annual Fall Symposium of the Korean Information Processing Society, 14th October 2000
14. Simon Haykin, “Neural Networks: A Comprehensive Foundation,” 2nd Edition, pp.842, 1999.
15. R. Brause, T. Langsdorf, M. Hepp, “Neural Data Mining for Credit Card Fraud Detection, “International Conference on Tools with Artificial Intelligence, pp.103-106, 1999.
16. Leandro S. Maciel, Rosangela Ballini, Neural Networks Applied To Stock Market Forecasting: An Empirical Analysis, Learning and Nonlinear Models (L&NLM) –

Journal of the Brazilian Neural Network Society, Vol. 8, Iss. 1, pp. 3-22, 2010.

17. Credit card fraud detection using machine learning techniques: A comparative analysis. (n.d.). Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis | IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8123782
18. Stolfo, S., Fan, D. W., Lee, W., Prodromidis, A., & Chan, P. (1997). Credit card fraud detection using meta-learning: Issues and initial results. In AAAI-97 Workshop on Fraud Detection and Risk Management.
19. Pun, J. K. F. (2011). Improving Credit Card Fraud Detection using a Meta-Learning Strategy (Doctoral dissertation, University of Toronto).
20. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decision Support Systems, vol. 50, pp. 602–613, 2011. doi:10.1016/j.dss.2010.08.008
21. Ghosh, D.L. Reilly, "Credit Card Fraud Detection with a NeuralNetwork," Proceedings of the International Conference on System Science, pp.621-630, 1994.
22. J. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P.-E. Portier, L. HeGuelton, and O. Caelen, "Sequence classification for credit-card fraud detection," Expert Systems with Applications, vol. 100, pp. 234–245, 2018. doi:10.1016/j.eswa.2018.01.037
23. 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.
24. Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, "BLAST-SSAHA Hybridization for Credit Card Fraud Detection," IEEE Transactions On Dependable And Secure Computing, vol. 6, Issue no. 4, pp.309-315, October-December 2009
25. Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick, "Credit card fraud detection using Bayesian and neural networks," Interactive image-guided neurosurgery, pp.261-270, 1993.
26. Simon Haykin, "Neural Networks: A Comprehensive Foundation," 2nd Edition, pp.842, 1999.