Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Artificial Neural Network–Based Modelling for Credit Card Fraud Analysis

Ms. Shweta Anil Kanojia[1], Dr. R.N. Jugele[2]

[1]Research Scholar, Department of Computer Science, Science College, Nagpur.
[2]Professor, Department of Computer Science, Science College, Nagpur.

Abstract

The growing use of digital payment systems has also been a witness to the emergence, leading to a rise in credit card fraud cases. Thus, this accentuates the need for the use of effective and efficient methods for the detection of financial fraud. This paper outlines the employment of an Artificial Neural Network technique to detect fraud in the use of credit cards. The proposed ANN system uses data collected from the previous use of the credit cards and, therefore, can detect patterns that exist in the data, thus separating fraud from actual transactions. In an effort to increase the suggested ANN system's accuracy and effectiveness, the usage of data pre-processing techniques, such as normalisation and class balancing, has also been included. The proposed ANN system will mainly be evaluated using the accuracy level of the system. As required, the proposed system has proven effective in detecting fraud in the use of credit cards with high levels of precision.

Keywords: ANN, Machine Learning, Classification Accuracy, Financial Transactions, Credit Card Fraud Detection.

1. Introduction

The growing usage of digital payment systems and other financial services has greatly impacted the way financial transactions are processed. Credit cards have emerged as one of the major tools for performing transactions, particularly online, thus leading to a substantial increase in the number of transactions being processed daily [1]. However, the growing usage of digital financial systems also poses a significant threat to financial organisations, primarily because of the growing number of fraudulent transactions being processed through the digital financial system [5]. Building an effective credit card system for fraud detection has thus become an essential aspect of securing financial transactions because the traditional system, which used if-then statements for processing transactions, had its glitches in the case of high transaction volumes [2]. These techniques operate on pre-defined rules, making their detection capabilities for complex and novel fraud behaviours difficult. Since fraudsters change tactics over time, there has been a growing call for smart techniques capable of learning from past experiences with improved performance over time. Machine learning techniques have become indispensable in recent times in addressing these issues by enabling automated data-driven fraud detection systems. Machine learning techniques can scan

past transaction data and differentiate genuine behaviours from fraudulent ones. These techniques learn patterns from data and, therefore, respond better to dynamic fraud behaviours than rule-based techniques [4].

ANNs are some of the most common machine learning algorithms employed in fraud analysis, as they are believed to perform a nonlinear relation between variables, which is common in transactional data. Further, it is possible to train ANNs on past transactional data to identify the fraud patterns, which generalise well to new transaction data. As such, ANNs are ideal algorithms in classification tasks such as fraud detection between legitimate and illegitimate.

In this paper, an ANN-based system will be proposed that focuses on the identification of credit card fraud in terms of past transaction patterns. The proposed system will be trained on the way to tell apart unique patterns that correspond to Credit Card Fraud patterns. Some pre-processing methods, including normalisation and class imbalance methods, will be included in this proposed system to enhance performance. The accuracy rate will mainly be tested on the proposed scheme with respect to classifications.

2. Literature Review

The increasing trend of relying on credit cards for online transactions has also been associated with rising fraud cases, which have resulted in substantial losses to the customer as well as to the financial institution.

393,207 of approximately 1.4 million identity theft incidents are classified as CCF. Currently, benefit and document-related fraud is at the top of identified cases of identity theft, and this is followed by CCF. The number of new incidents of credit card account fraud is 365,597 as of 2020. Nevertheless, the number of identity theft incidents cumulatively increased by 113% from 2019 to 2020, with an increase of 44.6% in credit card identity theft claims on a claim basis. Payment card theft resulted in a loss of a total of $24.26 billion in the global economy last year. With 38.6% of reported card fraud cases in 2018, it is apparent that the United States is the most exposed nation to credit card fraud incidents because, by arming themselves with auto fraud protection systems, financial institutions can make combating credit card fraud their number one concern [9].

Due to these requirements, the automation of the installation of credit card fraud detection systems has become an integral part of modern financial security systems [5],[4]. Traditional approaches in the field of fraud detection methods have gained popularity in the form of rule-based systems, as well as manual human-operated transaction monitoring systems. However, these approaches are found to be less effective in real-world applications pertaining to larger transaction datasets and mounting patterns of fraud in recent times. In addition to that, the requirement to entirely rely on pre-built rules causes these approaches to be less effective in identifying complex and unidentified patterns of transactions, thereby mounting further restrictions on their long-term applicability [5]. In an attempt to address these ineffectivenesses, current research developments on the topic have received widespread momentum in adopting advancements in machine learning algorithm approaches to carry out the task of detecting fraud. This allows for automatic and intensive processing of previously performed transactions to efficiently distinguish between honest and fraudulent transactions. In addition to that, these approaches are less reliant on rules and can be adapted more efficiently to the approaches of fraudsters in recent times [4], [3]. For the effective detection

of credit card fraud, there have been some recent efforts by several studies to compare the performance of various machine learning techniques, viz., Logistic Regression, Decision Trees, Support Vector Machine Methods, K-Nearest Neighbours, Random Forest Modelling, and Artificial Neural Networks. The results from the aforementioned studies clearly show the effectiveness of ensemble models and Artificial Neural Networks over the classification approach for the detection process [4]. Artificial Neural Networks have been one of the most popular techniques used in the study of fraud detection because of their ability to capture the non-linear patterns that exist in the transaction process [3], [4]. Apart from the techniques mentioned above, the importance of data preprocessing as an approach to improve the ability of artificial neural networks for functionality in fraud detection systems has been expounded by various researchers [4], [5]. The current literature also supports the importance of conducting a thorough assessment of the models on the following parameters, including the Confusion Matrix, F1-Score, Accuracy, Precision, and Recall. Among these, Accuracy as a factor for the performance of the models has been extensively used as an indicator in the current literature for the detection of credit card fraud using ANNs [3].

In 2022, Jain et al. [6] introduced the use of the R environment to apply Logistic Regression, Decision Trees, Artificial Neural Networks (ANN), and Gradient Boosting methods to discover credit card fraud. The experimental results revealed that the ANN and Gradient Boosting models were more accurate than other models in identifying fraud, establishing the efficacy of the two models in identifying fraud. In 2023, Prateeksha et al. [7] described a technique to discover credit card fraud by applying the machine learning technique to the three classifiers: Artificial Neural Network, Decision Tree, and Logistic Regression.

These classifiers have been trained using the publicly available credit card transaction dataset for the identification of patterns of valid as well as fraudulent transactions. Parameters of accuracy, precision, and recall have been taken into consideration for the identification of the most accurate approach for the identification of fraudulent transactions. It was found in the experiment that the ANN approach is the most accurate approach of the various approaches applied. This research work aims at the design of a system for the detection of fraudulent transactions at an initial stage to avoid the losses faced by the banking sector.

3. RESEARCH METHODOLOGY:

Artificial Neural Network (ANN): A specific type of Artificial Neural Network (ANN) is that of a model designed on the structure and functioning of the human brain [8]. “An ANN is composed of ‘interconnected processing units called neurons that work in collaboration with each other for learning complex patterns from the datasets.' Artificial neural networks are extensively applied in various machine learning models, such as classification, forecasting, or identifying patterns in datasets, because of their effectiveness in handling ‘modelling nonlinear relationships.' There are three layers in an Artificial Neural Network, namely, ‘the input layer, hidden layers, and output layers.' Regarding this, ‘the input layers receive the ‘set of features of the datasets, whereas the ‘hidden layers carry out ‘weighted calculations and transformations by means of ‘activation functions.' Further, ‘the output layers create the final ‘predictions or ‘classification output.' Every connection between the ‘neurons is formed in relation to their ‘weights that symbolise the degree of ‘influence between the ‘neurons. “The training phase of ANN, its weights are adapted or adjusted for optimising the error that exists between the predicted results and actual results through backpropagation.” This process of training would go on till the model achieves optimal results. It

is highly beneficial for fraud detection as it is capable of handling large, high-dimensional, and imbalanced data, including the complex patterns existing between the transactions identified as fraud, compared to the transactions identified as legitimate.

It is used for complex classification tasks, which explains its relevance in a two-class classification scenario, such as credit card fraud analysis, as it can treat complex patterns associated with a transaction identified as potential fraud, thereby resulting in better outcomes. For fraud analysis, the pattern of data is non-linear as well as dynamic.

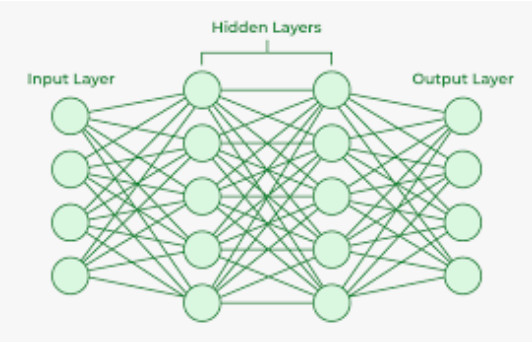

Fig 1: ANN Model

Algorithm: Training and Classification Using Artificial Neural Network

Step 1: Network Initialisation
Some small random initialisation values are employed to initialise the weights and biases of all artificial neurons in the neural network. The activation functions are selected for the hidden layers as well as the output layers to achieve nonlinear learning.
Step 2: Data Preprocessing
All the attributes of the input data are normalised, thereby increasing the efficiency of the learning process. Finally, the data set is split into a training set and a test set.
Step 3: Model Training
The training will employ a fixed number of epochs.
Step 4: Model Evaluation
The trained ANN model is then tested on the test data set. Accuracy, precision, recall, and F1-scores are the measures for classification that are generally employed for evaluating the model's performance.
Step 5: Output
The trained neural network model and classification result are returned.

4. RESULTS AND DISCUSSION

A. DATASET: Data sourced from the Kaggle site and used in the analysis includes credit card transactions carried out by European card-users and their corresponding results. Data is presented in a CSV file, and loading and processing the data for analysis becomes quite easy. The dataset has approximately 550,000 transactions, and each is regarded as a distinct dataset. To ensure anonymity and also for uniformity, the dataset underwent feature scaling by using Principal Component Analysis. This

created 28 numeric features, which describe different aspects of the transactions, like their timing, amount, and even minute behaviours. Another feature is the identification number given to each transaction so as to track and refer to it later. The "Amount" feature describes the amount in a credit card transaction. The target variable of the model is revealed by the "Class" feature, showing whether the transactions are genuine and original, also considered authentic, and otherwise as forgery, marked as 0 and 1, respectively. Such a dataset gives a significant foundation to build and develop different machine learning models to recognise and detect credit card transactions as forgery.

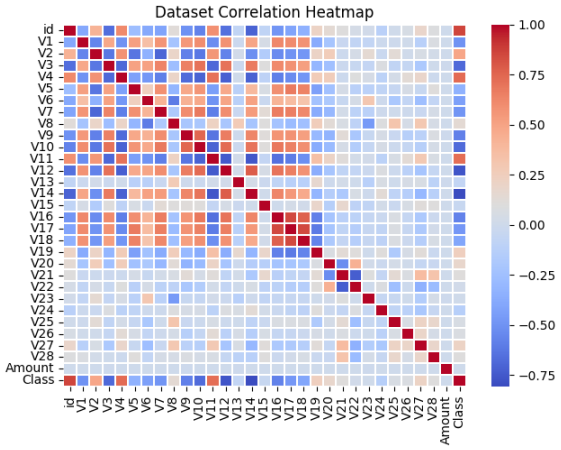

Fig 1: Heatmap showing correlation among features in the credit card transactions dataset.

B. PERFORMANCE METRICS: Performance measures are known as the quantitative measures by which the accuracy, goodness, as well as the ability to generalise models for performing the process of machine learning is evaluated. In the above research work, a data set consisting of a collection of credit card transactions along with actual as well as fraudulent payments is taken into consideration. Each transaction is labelled with a binary label based on which the payment associated with the fraudulent transaction is represented with the digit 1, while the other payments are actual payments, which are denoted by the digit 0. The performance paradigm associated with the new classification technique is tested by taking the parameter such as F1 score, recall, accuracy, and precision values that are calculated based on a mathematical expression. Accuracy is a common parameter taken into consideration for testing the performance associated with models.

1. Accuracy: Measures overall correctness.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

2. Precision: Measures how many predicted positives are actually correct.

$$\text{Precision} = \frac{TP}{TP+FP}$$

3. Recall (Sensitivity / True Positive Rate): Measures how many actual positives are correctly identified.

$$\text{Recall} = \frac{TP}{TP+FN}$$

4. F1-Score: Harmonic mean of precision and recall.

$$\text{F1 Score} = 2* \frac{Precision*Recall}{Precision+Recall}$$

5- AUC Score: The AUC score measures a model's ability to distinguish between classes, particularly in binary classification problems.

6-ROC Curve: The ROC curve illustrates the trade-off between sensitivity and false alarm rate over varying classification thresholds.

7- Confusion Matrix: A confusion matrix is a table used to evaluate the performance of a classification model by comparing the predicted labels with the actual labels. It helps to understand how many predictions are correct and where the model makes mistakes.

PARAMETERS	ANN
RECALL	0.9992
PRECISION	0.9994
F1-SCORES	0.9993
AUC SCORE	0.9999
ACCURACY	0.9993

Table 1: Performance Metrics of ANN

C.TRAINING AND VALIDATION ACCURACY

```
# Training vs Validation Accuracy
plt.figure(), plt.plot(history.history['accuracy'], label='Training Accuracy')
plt.plot(history.history['val_accuracy'],label='Validation Accuracy')
plt.xlabel("Epochs"),plt.ylabel("Accuracy")
plt.title("Training vs Validation Accuracy (ANN)"), plt.legend(),plt.show()

# Training vs Validation Loss
plt.figure(), plt.plot(history.history['loss'], label='Training Loss')
plt.plot(history.history['val_loss'], label='Validation Loss')
plt.xlabel("Epochs"), plt.ylabel("Loss"),plt.title("Training vs Validation Loss
(ANN)"),plt.legend(),plt.show()
```

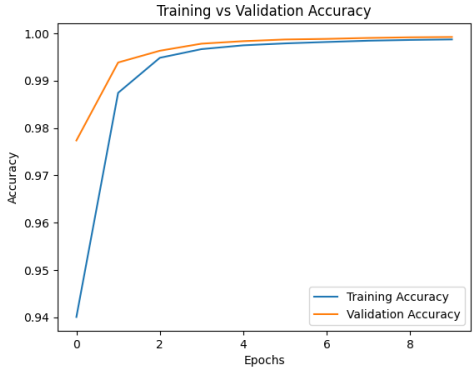

Fig 2: Training and Validation Accuracy for ANN Model

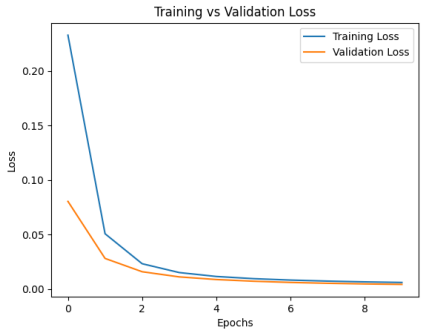

Fig 3: Training and Validation Loss for ANN Model

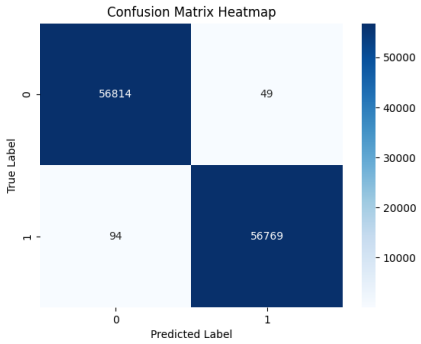

Fig 4: Confusion Matrix of ANN Model

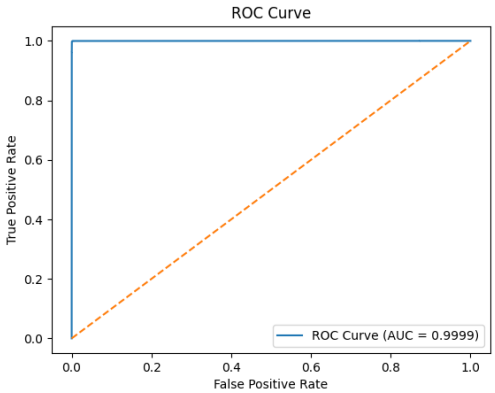

Fig 5: ROC Curve of ANN Model

5. Conclusion

An Artificial Neural Network (ANN) model has been designed and validated for effective credit card fraud detection as a part of this research work. Based on the understanding of complex patterns available within the transactions, the proposed methodology has shown the potential to classify a given transaction as valid or fraudulent. A series of testing criteria, like Accuracy, Precision, Recall, F1-score, and Area Under the ROC Curve, have been considered as a part of this research work for a complete analysis of the efficiency of the proposed methodology. With an accuracy of 99.94% and a value of 0.9999 for AUC, the proposed

Artificial Neural Network method for credit card fraud detection possesses a highly efficient classifying power.

This means there is very little misclassification within the confusion matrix, which in turn effectively reduces the number of false positives and false negatives. Added to that, there is effective generalisation since the training and validation accuracy and loss curves converge rapidly and are very similar in amplitude. Another piece of supportive evidence regarding the robustness of the model refers to the ROC curve that shows a high true positive rate within a wide range of thresholds. Generally, the results of the study prove that the ANN model suggested may significantly enhance the security of electronic payment systems and turn out to be highly feasible for credit card fraud detection tasks.

References

1. P. Y. Prasad, A. S. Chowdary, C. Bavitha, E. Mounisha, and C. Reethika, "A Comparison Study of Fraud Detection in Usage of Credit Cards using Machine Learning," In Proc. 7th Int. Conf. on Trends in Electronics and Informatics (ICOEI), Tirupati, India, 2023, pp. 1204–1209, doi: 10.1109/ICOEI56765.2023.10125838.
2. Y. M. R. Raajha, A. Kavin, D. Rajkumar, R. Reshma, R. Santhosh, and N. Mekala, "An Analytical Approach to Fraudulent Credit Card Transaction Detection using Various Machine Learning Algorithms," In Proc. 2nd Int. Conf. on Electronics and Renewable Systems (ICEARS), Coimbatore, India, 2023, pp. 1400–1404, Doi: 10.1109/ICEARS56392.2023.10085157.
3. K. Annaboina and M. V. P. Rao, "Credit Card Fraud Detection Using Machine Learning and Data Science," International Journal of Computer Engineering and Technology, vol. 12, no. 2, pp. 25–35, 2021.
4. A. Phakatkar, "Credit Card Fraud Detection using Machine Learning Techniques," Journal of Emerging Technologies and Innovative Research (JETIR), vol. 10, no. 6, pp. 192–197, 2023.
5. S. Al Balawi and N. Aljohani, "Credit-card Fraud Detection System using Neural Networks," The International Arab Journal of Information Technology, vol. 20, no. 2, pp. 234–241, Mar. 2023.
6. N. Jain, A. Chaudhary, and A. Kumar, "Credit Card Fraud Detection Using Machine Learning Techniques," Proc. 11th Int. Conf. on System Modelling & Advancement in Research Trends (SMART 2022), IEEE, pp. 1451–1455, 2022. DOI: 10.1109/SMART55829.2022.10047360.
7. P. M. S. Prateeksha, B. N. Swetha, and M. Patil, "Credit Card Fraud Detection Using Machine-Learning," International Journal of Advanced Research, vol. 11, no. 04, pp. 1559–1563, Apr. 2023.
8. H. Chen and L. Chen, "An application of XGBoost algorithm for online transaction fraud detection based on improved sailfish optimiser," 2022 4th International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI), Wuhan, China, 2022, pp. 294–299, doi: 10.1109/MLBDBI58171.2022.00064
9. 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, Apr. 2022.