WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Analysis of Credit Card Fault Detections Using Convolutional Neural Networks and Transfer Learning

Aparna Dayyala[1] , Ramu V[2]

[1]Assistant Professor in CSE Department Balaji Institute of Technology and Science Narsampet, Warangal Rural
[2]Assistant Professor in CSE (ALML) Department Balaji Institute of Technology and Science, Narsampet, Warangal Rural

ABSTRACT

Recognition of credit card fraud in actual-life scenarios. One of the significant ethical issues in the credit card industry is fraud. Many modern financial services, including ATMs and online banking, are currently accessible. In addition, using credit cards has evolved into a valuable and essential aspect of daily economic activity due to the rapid advancements of e-commerce. Clients get provided with credit cards as a means of payment. Credit card fraud is using an individual's credit card or information without the owner's authorization. People frequently get tricked and pay the price in significant fraud methods, which include application and behavioral fraud. Multiple applications received by the same people may result in identical copies. Application fraud happens when cybercriminals use fraudulent data to apply for new cards from banks or card issuers. In this assignment, we will classify the credit card dataset using supervised and unsupervised methods. To assess the model's accuracy, we will use CNN to correlate with the training collection of data.

Keywords: convolutional neural networks, Transfer learning

I. INTRODUCTION

Credit card usage for online transactions and purchases has gradually grown due to the rise of the E-commerce industry. The number of credit card fraud problems is rising along with using credit cards. Credit card frauds are actions taken with a view of performing financial offenses without the cardholder's authorization. Since the use of credit cards has risen substantially, it is essential to recognize the procedure for identifying and ending credit card fraud. The reality exists that inconsistent data are insufficient for correctly recognizing fraud. The central practical arrangement is based on computer robotization. Through simple factual procedures, the PCs may be used to classify credit card exchanges as "suspicious." Therefore, conventional methods must be revised and changed with advanced techniques like machine learning and artificial intelligence (AI). The choice and categorization depend on a wide variety of features. Transactions cannot be classified just as either legally false [1]. However, it can be detected via an in-depth analysis of client conduct, defrayment patterns, and pre-fraud behavior. The requirement of recognizing fraud rapidly, as well as the need to process multiple variables while training, presents several challenges with fraud detection techniques. The "suspicious" trade is stamped, followed by being physically examined by human administrators for the final decision to disambiguate suspicious cases in current frameworks for fraud identification. Based on historical data, we will use machine learning algorithms to forecast the possibility that a transaction will be false. The practice of employing a credit card when making a purchase online has become common. We will use specific machine learning techniques, like CNN, to fix this issue. There will be a training set and test set created from the dataset. The study makes use of CNN techniques. We need to execute and use advanced techniques and functions to detect fraud in a transaction [2].

II. RELATED WORK

It focuses on credit card fraud and the techniques used to identify it. When someone uses another person's credit card without the owner's consent for personal use, it is called credit card fraud. This study identifies fraud using credit cards using machine learning algorithms. The model's effectiveness is assessed using a publicly accessible credit card data set. Its primary objective is implementing and evaluating the framework as a tool for credit card fraud detection. An innovative fraud detection technique that analyzes current transaction data intending to recognize customer spending patterns using historical transaction details[3]. Where cardholders are separated based on the value of their activities, then, using the technique of sliding windows, combine the transactions made with cards from different groups to extract the correct behavioral patterns for every category. The groups are subsequently taught separately with various classifiers later. The classifier with a perfect score may be chosen as one of the most efficient methods to detect fraud. Therefore, after a system for feedback to deal with the issue of concept drift, the researchers utilized a European credit card fraud dataset for their research.

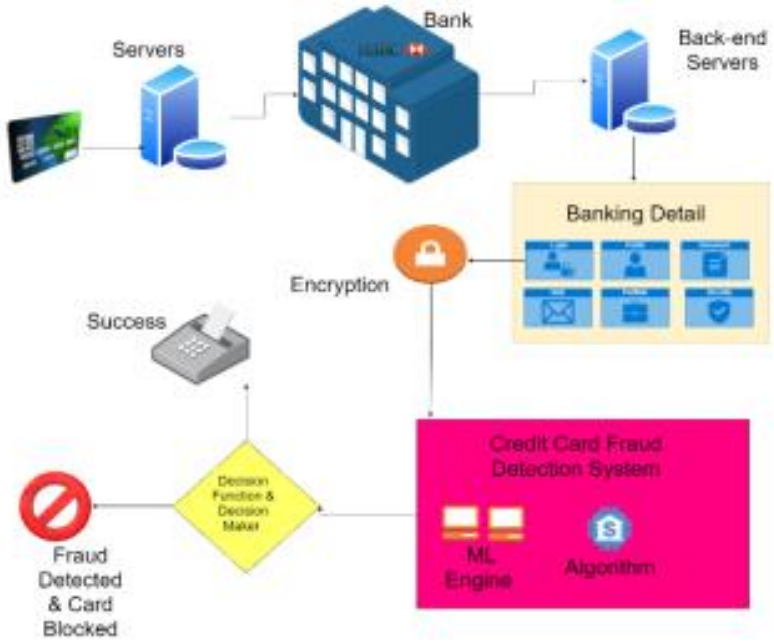

Figure 1: Overview Of Fraud Detection

TYPES OF FRAUD

1. **Bankruptcy Fraud**

It uses a credit report from an approved agency as a source for data examining the candidates' open records, just as a potential implementation of a bankruptcy model educates against bankruptcy fraud. It constitutes one of the most significant forms of fraud because using a credit card if in debt can be inferred through the expecting bankruptcy deception[4].

2. **Theft Fraud/Counterfeit Fraud**

The offender will take another person's card and use it as frequently as it is wise until it is blocked. The sooner the owner reacts and contacts the bank, the sooner the bank can move to put an end to the crime. Sometimes, someone will copy your card number and codes and use them on particular websites where a physical card signature is not required[5].

3. **Application Fraud**

In numerous places, applicants must complete an application process to be qualified for a credit card. While looking for copies, any of those attributes could be employed. Cross-coordinating is a straightforward alternative to using factual techniques. On the other hand, personality misconduct, as it is known, is carried out by real fraudsters purposely completing out application information improperly[5].

4. **Behavioral Fraud**

It occurs when authentic card details are acquired knowingly, and purchases occur with the belief that the cardholder will be present. These organizations engage in phone and online commercial transactions, where just card details are required.

III. METHODOLOGY

1. **Convolutional Neural Network**

Convolutional neural networks. Convents mirror typical neural networks in many ways, which can be visualized as a group of neurons arranged in an acyclic graph. A hidden layer neuron is only connected to a portion of the neurons in the preceding layer, which constitutes the fundamental difference from a neural network. The operation of each component can be seen in the following figure [6].CNN is a model generating interest due to its contextual information-based categorization abilities. Consider trying to determine whether a photograph of a bird depicts a bird or another object. You start by feeding the input layer of the neural network (multi-layer network used to classify things) the image's pixels in arrays. The hidden layers perform feature extraction through various calculations and manipulations. Several hidden layers, including the convolution, ReLU, and pooling layers, extract features from the image. The object in the image is identified at the very end by the fully connected layer[7].

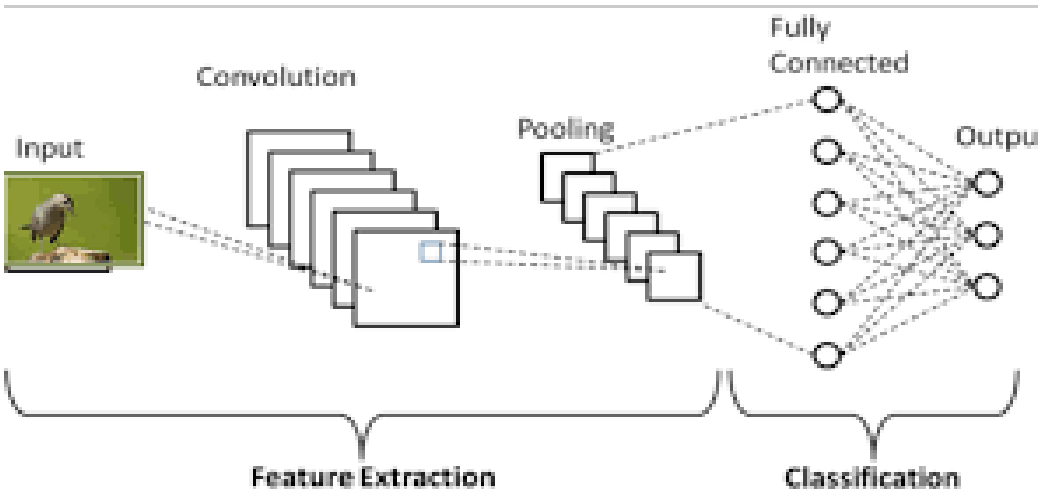

Figure 2: **Typical CNN structure**

ReLU Layer

Substitute all negative values with zeros and remove all negative values from the modified images. This stops the values from adding up to zero. When applying the ReLU transform function, a node is only activated if the input is throughout an established threshold; alternatively, the output is zero. But if the input increases above the point, there is a linear relationship between the input and the dependent variable[8].

Pooling Layer

After non-linear activation, pooling is carried out. The pooling layer helps in reducing the number of parameters and prevents overfitting. It also functions as a smoothing tool to get rid of undesirable noise. There are numerous varieties of pooling, including minimum, maximum, average, and others. Pooling is primarily used with filters and strides to shrink the image size [9]. In the future, the network will look at more significant parts of the image at a time due to max pooling, which reduces the number of parameters in the network and subsequently lowers the computational burden. Max pooling diminishes the resolution of the supplied output of a convolutional layer. In addition, max pooling might lessen over fitting[10].

2. Long Short Term Memory systems

Standard RNNs suffer from evaporating or detonating inclination problems. The Long Short-Term Memory architecture was suggested as a solution to these problems. A memory cell found in LSTMs maintains its state over time. Additionally, gating devices control data flow into and out of the memory cell. More specifically, an input entrance can make it possible for the info sign to alter the cell state or reverse it (by setting the input gates to 0). An output gate allows the cell state to either square or influence neurons in the surrounding layers. An overlook door gives the cell the ability to remember or ignore. Its previous state. Initially. It is still being determined what each component's proportional relevance is. The number of neurons in the hidden layers, the activation function, the inner activation function, and the dropout rate are significant LSTM parameters influencing the output's quality [11].

3. Recurrent Neural Network

The output from the previous step is used as input to the next step in recurrent neural networks (RNNs), a form of neural network. It can manage sequential data, consider the present information and any past inputs received, and memorize previous inputs thanks to internal memory [12]. The activation function, dropout rate, and loss function are significant variables that influence how well RNNs operate.

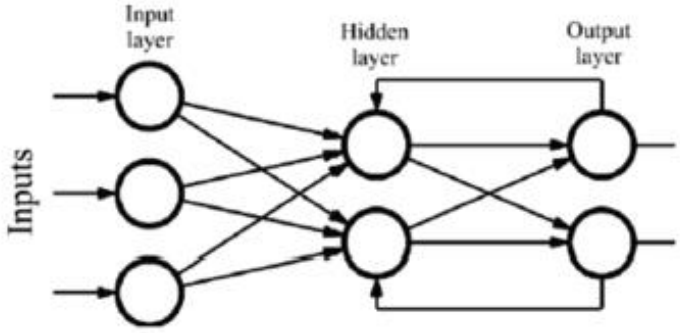

Figure 3: With hidden layer RNN

4. Transfer learning

Convolutional neural networks (CNNs) constitute a technique for transfer learning which allows the knowledge acquired from one activity to be applied to another related task. In computer vision applications like image categorization and object recognition, CNNs are frequently employed. Transfer learning uses the generic properties that CNNs trained on massive datasets, like Image Net, have discovered and which are pertinent to many visual applications. Transfer learning uses a pre-trained CNN as a starting point and refines it on the new dataset instead of training a CNN from scratch on a fresh dataset. A feature extractor, the pre-trained CNN, gathers high-level visual representations. Then, new layers created for the particular task receive these features.

5. Feed Forward Neural Network

A viral AI algorithm known as the perceptron gave rise to neural networks. The fundamental Deep learning models are deep feed-forward systems, often called feed-forward neural networks or multi-layer perceptrons (MLPs). Multi-layer perceptrons, called feed-forward neural systems, are perceptrons connected in multiple layers. Data streams ahead with this type of engineering in just one direction. In other words, the data streams begin at the information layer, travel through the "enclosed up" levels, and finally arrive at the yield layer. The framework lacks a circle. At the end of the yield layers, data ends.

IV. RESULTS

Our dataset has 492 frauds out of 284,807 transactions over two days. The dataset is very skewed, with frauds making up 0.172% of all transactions in the positive class. It solely has numeric input variables, a PCA transformation's output. Unfortunately, we cannot offer the original features or additional context for the data due to confidentiality concerns. The PCA's primary components are features V1, V2,..V28. The model is trained using the training dataset which is given to it. The model's precision is projected and printed. By creating and training a Convolutional Neural Network model with additional upgrades, we obtained the result of an accurate credit card fraud detection value, which is 0.9539 (95.3%). Compared to the current model, the proposed model can produce more accurate results with a larger dataset.

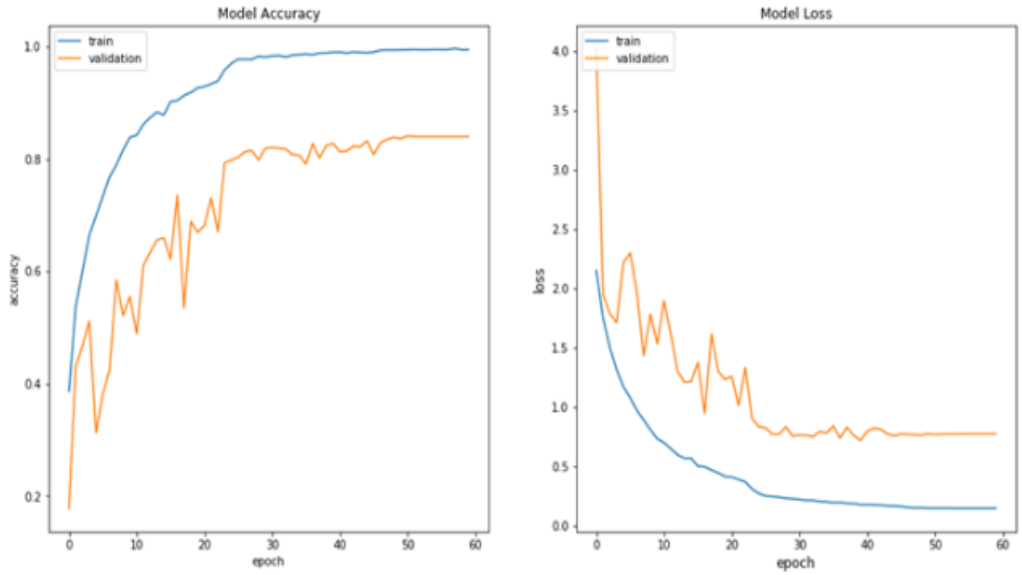

Figure 4: Loss and accuracy of the model

V. CONCLUSION

A standard instance of fraudulent deceit is credit card fraud. This article has examined recent charge card late findings. The many types of fraud, including bankruptcy, counterfeit, theft, application, and behavioral fraud, were distinguished in this piece, along with methods for spotting them. Convolutional neural networks, genetic algorithms, and pair-wise coordinating are examples of such techniques. From a moral perspective, one may argue that banks and credit card issuers should try to identify every instance of fraud. Different methods for machine learning are primarily influenced by the type of data that arrives.

The model's effectiveness for detecting CCF is greatly affected by the number of features, the volume of transactions, and the correlation between the components. We employ a dataset in CSV format. The data is very private. Because of the imbalanced data, it is challenging to identify fraudulent transactions because most transactions are accurate.

REFERENCES

1. 'Machine Learning For Credit Card Fraud Detection System' International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 24 (2018) pp. 16819-16824 © Research India Publications. http://www.ripublication.com
2. Credit card fraud detection using Machine Learning' K. Karthikeyan1, K. P. Sangeeth Raj1, S. Ramaganesh1, P. Parthasarathi2, Dr. N. Suguna3
3. Abakarim, Y., Lahby, M., & Attioui, A.: An Ef□cient Real-Time Model for Credit Card Fraud Detection Based on Deep Learning. In Proceedings of the 12th In International Conference on Intelligent Systems: Theories and Applications (p. 30). ACM, (2018)
4. S. Ramana, S. C. Ramu, N. Bhaskar, M. V. R. Murthy and C. R. K. Reddy, "A Three Level Gateway protocol for secure M-Commerce Transactions using Encrypted OTP," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 1408-1416, doi: 10.1109/ICAAIC53929.2022.9792908.
5. S. Ramana, S. C. Ramu, N. Bhaskar, M. V. R. Murthy and C. R. K. Reddy, "A Three-Level Gateway protocol for secure M-Commerce Transactions using Encrypted OTP," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1408-1416, doi: 10.1109/ICAAIC53929.2022.9792908.
6. N.Bhaskar, S.Ramana, & M.V.Ramana Murthy. (2017). Security Tool for Mining Sensor Networks. International Journal of Advanced Research in Science and Engineering, BVC NS CS 2017, 06(01), 16–19. ISSN Number: 2319- 8346
7. Karunakar Pothuganti, (2018) 'A comparative study on position based routing over topology based routing concerning the position of vehicles in VANET', AIRO International Research Journal Volume XV, ISSN: 2320-3714 April, 2018 UGC Approval Number 63012.
8. Ramana, S., Bhaskar, N., Murthy, M.V.R., Sharma, M.R. (2023). Machine Learning for a Payment SecurityEvaluation System for Mobile Networks. In: Rajakumar, G., Du, KL., Rocha, Á. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. ICICV 2023. Lecture Notes on Data Engineering and Communications Technologies, vol 171. Springer, Singapore. https://doi.org/10.1007/978-981-99-1767-9_26
9. N. Bhaskar, S. Ramana and G. M. Kumar, "Internet of Things for Green Smart City Application Based on Biotechnology Techniques," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10083965.
10. K. Pothuganti, B. Sridevi and P. Seshabattar, "IoT and Deep Learning based Smart Greenhouse Disease Prediction," 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), 2021, pp. 793-799, doi: 10.1109/RTEICT52294.2021.9573794.
11. I. Ahmad and K. Pothuganti, "Smart Field Monitoring using ToxTrac: A Cyber-Physical System Approach in Agriculture," 2020 International Conference on Smart Electronics and Communication (ICOSEC), 2020, pp. 723-727, doi: 10.1109/ICOSEC49089.2020.9215282.
12. Wen, Ying, et al. "Learning text representation using recurrent convolutional neural network with highway layers." arXiv preprint arXiv:1606.06905 (2016).