CENTRAL ASIAN JOURNAL OF INNOVATIONS ON TOURISM MANAGEMENT AND FINANCE

Volume: 04 Issue: 08 | Aug 2023 ISSN: 2660-454X

https://cajitmf.centralasianstudies.org

Analysis of Credit Card Fraud Detection Model Using Convolutional Neural Network

[1] P. Deekshith Chary
[2]Balusupati Anil kumar

Received 16th Jun 2023,
Accepted 19th July 2023,
Online 30th August 2023

[1] *Computer science Engineering (Data Science) Assistant professor, CMR Institute of Technology, Hyderabad, Telangana*
[2]*Computer science Engineering (Artificial Intelligence & Machine Learning) Assistant professor, CMR Institute of Technology, Hyderabad, Telangana*

Abstract: *The usage of credit cards has increased significantly in everyday circumstances as a result of the Internet's rapid expansion and the simplicity of electronic the purpose of transmission. A credit card allows the individual using it to pay for goods or services purchased from a merchant, but because it operates on a cash-in-advance basis, the cardholders must return the funds that they have already spent after a brief amount of period. Credit cards are vulnerable to an array of threats, such as identity theft, phishing, skimming, and card absence before transaction. We can use systems that detect fraud to predict scams well in advance to enable to use credit cards securely and fraud free. Researchers have been using a number of credit card fraud detection techniques, include rule-based systems, internal fraud detection systems, and neural networks. Credit card fraud is the fraudulent use of an individual's credit card or other data without the permission of the owner. People frequently get scammed and ripped off through significant fraud techniques such as application and behavioral fraud. Multiple applications produced by the same someone might result in identical fraud. Application fraud happens when scammers use fraudulent to apply for new cards from the bank.*

Keywords: *Convolutional Neural Network, Logistic Regression*

I. Introduction

The purchase of goods via e-commerce websites has become widespread in the present. Several companies have created an online payment method that accepts credit cards for the purpose to track down all the different kinds of credit card fraud that are occurring and to explore alternative fraud detection techniques. On the foundation of previous transactions, we are employing Deep learning algorithms to forecast the possibility a transaction will be a fraud. A fraud the inquiry team has established departments and groups that are in responsible for analyzing any potentially suspicious transactions that the detection system identifies as a means to stop credit card losses. A fraud analyst's computer screen showing flagged accounts and the transactions connected to those was displayed in real time. Fraud analysts examined over the red flagged transactions to determine the potential risk connected regarding them based on client backgrounds and experiences.

Fraud must be minimized order to minimize these losses. Various frauds of different kinds are taking place as technology develops quickly. Therefore, a variety of machine algorithms are utilized nowadays for recognizing fraud, include hybrid algorithms and artificial neural networks since they perform better. When a cardholder refuses to authorize a transaction, there are two possible outcomes: either the card stolen, or it could be counterfeit, in which case the cardholder made the purchase but later denied the transaction by reporting the card as stolen[1].

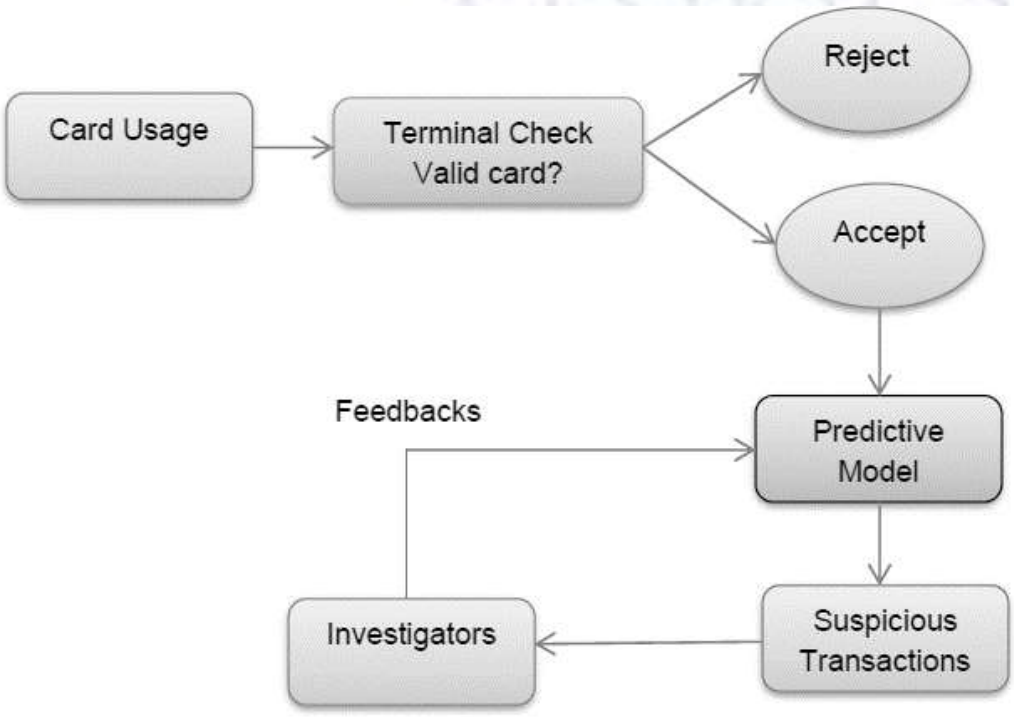

Figure 1: Fraud detection process

Multiple Types of Credit Card Fraud

The distribution of ignorance through the world with deceptive fortune and major negative impacts is caused by data innovation development coupled with upgrading in the relevant channels. Researchers have

identified and illustrated that there are many different types of credit card fraud, including phony cards, web or electronic extortion, simple burglary, never got issued, application deception [2].

1. **Card Not Present Transaction**

When a consumer decides to make a purchase without a credit card, the shipper is mostly dependent on the cardholder who provides card information inadvertently by phone, mail, or the internet.

2. **Identify Theft**

This can be divided into two different groups: account takeover and application fraud. When a guy succeeds in using a stolen document to open a record in someone else's name, application fraud occurs. The records can be stolen by the offenders, for example: the construction of useful personal information through justifications of bank and service bills.

3. **Skimming**

It is an electronic technique where personality criminals collect data on a casualty close to home and use it to their advantage. The skimmer is nothing more than a little device that outputs a Visa Card and stores the information of the magnetic stripe it contains. It may have happened as a result of financial skimming.

II. Literature Review

Fraud types and conduct vary frequently. It's essential to understand the technology used in fraud detection. The models, algorithms, and fraud detection tools utilized in earlier inquiries are discussed here. Deep learning techniques are explained in and this method requires time to process large amounts of data. Another issue with the preparation of credit card transaction data is repetition.

In order to do this, Zahra Kazemi (2021) recommended applying a deep auto-encoder to extract the most useful characteristics from the data on credit card transactions, and then combining it with a soft max network to determine the labels for the various classes [3]. Regarding these impacts of features, data was used to overcome fully automatic decoding, which maps data into a high dimensional space through sparse models and results in discriminative space for classification. In the classification problem is sorted using the Logistic Regression algorithm (LR). Fraudulent case discretization is done using Gaussian Mixture Models. Synthetic minority oversampling is used to balance the data. Economic value is calculated via sensitivity analysis.

The most common form of payment that is accepted for both online and offline cashless purchases is the credit card. As a result, all transactions and payments now follow the newest, most practical method. The advancement of technology has led to an increase in credit card theft, which indicates that economic fraud is rising due to improved global communication. It was originally worked on by N. Malini (2021), and the results indicate that false alarm rates decrease and fraud detection rates rise. On bank credit card fraud detection systems, any of these techniques can be used to detect and prevent fraudulent transactions [4]. Used a customized Bayesian Network Classifier (BNC) method to find actual instances of credit card theft. The Hyper-Heuristic Evolutionary Algorithm (HHEA), which organizes the suggested algorithm information into taxonomies and searches for the optimal combination of such components for a given dataset, was used to automate the process of constructing Fraud-BNC[5]. Suresh Kumar (2019) has worked on a practical issue involving the identification of credit card fraud based on fraudulent transactions. The majority of the time, credit card fraud can take place both online and offline, although at the moment, online fraud transactions are on the rise. Therefore, many methods are used in the current system to identify online

fraud transactions. The Random Forest Algorithm (RFA) has been utilized by Suresh Kumar to identify fraudulent transactions and their accuracy [6]. Decision trees are used in their approach to categorize datasets, which are based on supervised learning. After classifying the dataset, a confusion matrix was obtained, and it was used to assess the effectiveness of RFA. 90% accuracy is provided by the results obtained after dataset processing.

III. Methodology

1. Convolutional Neural Network

A CNN is a specific kind of deep neural network that is employed in deep learning to evaluate visual pictures. CNN employs a range of layer types, and we used 18 layers in our CNN model. The input layer, which is the first layer employed by our model, comprises the image data. A three-dimensional matrix is used to describe image data, and this layer does normalization. Our model uses a convolutional 2D layer as its second layer. Convolution is done on this layer. The image is divided into perceptron segments using an algorithm, local fields are generated, and perceptron segments are compressed into feature maps using a m*n matrix. The batch normalization layer is the third layer that our model uses. Between convolutional layers and nonlinearities layers, such as ReLU (Rectified Linear Units) layers, we employ batch normalization layers[7].

Batch normalization is a two-step process that involves first normalizing the input and then rescaling and offsetting. Convolutional neural network training will be accelerated as a result, and sensitivity to network initialization will be decreased. ReLU layer is the fourth layer that our model employs. It is a typical neural network default activation function that enhances model performance and training. It is a CNN layer that combines rectification and non-linear layers. The threshold operation is carried out in this, making negative values equal to zero. Contrarily, ReLU has no impact on the input size. Then, for the purpose to fully comprehend our original data, we will pre-process our data. We'll use 10% of the data from the pre-processing as the original data variable. We will choose the input and output features for our model. The Infinite Feature Selection Algorithm is now used. The best features available for predicting fraud will be chosen using an infinite feature selection algorithm. We'll use a convolutional neural network and train our model. The two components of fraud detection are training and prediction.

2. Logistic Regression

That the sigmoid function could potentially employed for categorizing the output that is a dependent feature and because it employs probability for doing so, sigmoid function and logistic regression operate together. Because of the usage of the sigmoid function, which produces a value of 1 if the output is more than 0.5 and a value of 0 if the output is less than 0.5, this technique performs well with small data sets. While this sigmoid function wouldn't be suitable for deep learning since, in that case, updating the weights to reduce update error is necessary while going backwards from output to input. We must differentiate the sigmoid activation function in intermediate layer neurons, which yields a value of 0.25 and affects the module's accuracy in deep learning [8].

3. ANN Model

Artificial neural networks often appear as heavily connected systems of "neurons" that can derive values from inputs. A neural network is equivalent to a web of connected neurons, which can be estimated in the millions. The body provides all parallel processing with the aid of these connected neurons, and an individual or animal's body is the most exquisite example of parallel processing. Artificial neural networks

have evolved into a clustering of early artificial neurons. By generating layers that are subsequently linked to one another, this clustering takes effect.

Thus, patterns and trends that are too complex to be observed by people or other computer approaches can be extracted using neural networks, which have a higher capacity to infer meaning from complex or imprecise data. The kinds and range of artificial neural networks that can be implemented in silicon are constrained by this physical fact. At the moment, neural networks are only a basic grouping of artificially rudimentary neurons. By building layers and connecting them, this clustering takes place. The other aspect of "art" of designing networks to address issues in the actual world is how these levels link to each other.

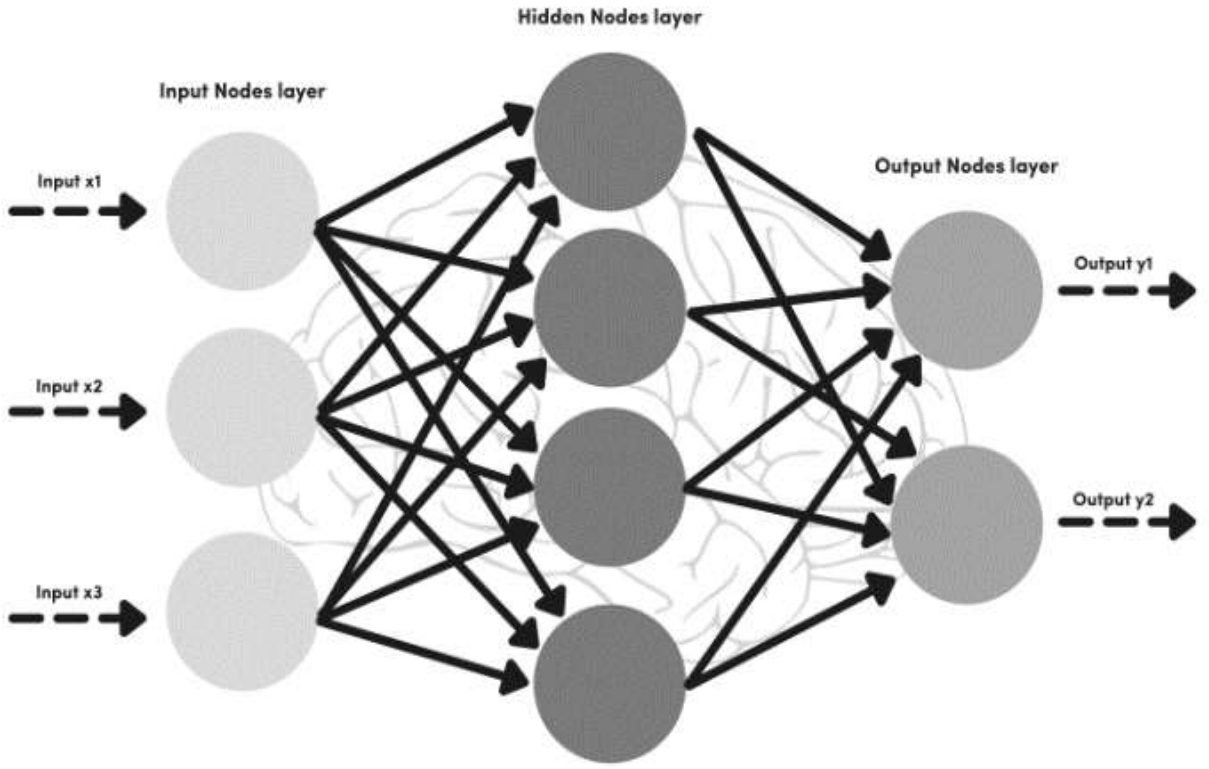

Figure 2: A Simple Neural Network

4. Experimental Results

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 were able to obtain the result of an accurate value of credit card fraud detection, which is 0.9539 (95.3%).The Kaggle data set is utilized, which consists of 284,807 transactions that occurred within the previous two days, of which 492 were fraudulent. Therefore, only numerical input variables that follow PCA transformation are employed in order to secure client privacy[9].

There are 50 values—including amount and time—that are separated by commas. After the data is supplied, the predicted outcome is shown as fraud. These findings, along with the classification report for each algorithm, are provided in the output as follows, where class 0 denotes a transaction that was found to be valid and class 1 denotes a transaction that was found to be fraudulent. The CNN model object function is the Root Mean Square Error (RMSE) with respect to Iterations. The CNN's RMSE value will decrease as

it learns. In our experiment, we took into account 10 epochs, and we discovered that as the number of epochs increased throughout the CNN network's training phase, the RMSE value decreased.

Table 1: Table of accuracy, precision, and recall evaluations for several Algorithms

	Accuracy	Precision	Recall
Logistic Regression	94.84	97.58	92.00
ANN Model	92.78	98.54	91.50
CNN model	98.69	98.41	98.98

The final element in the image shows the weight value of the feature selection method in relation to characteristics. It demonstrates that the loss is proportional to the epoch or iterations that become below 0.0005 after 1000 iterations [10]. Based on feature selection, we took into account 30 features and discovered the credit card fraud, along with its weight, which is indicated in the figure. The increase in attribute count minimizes the weight of the feature.

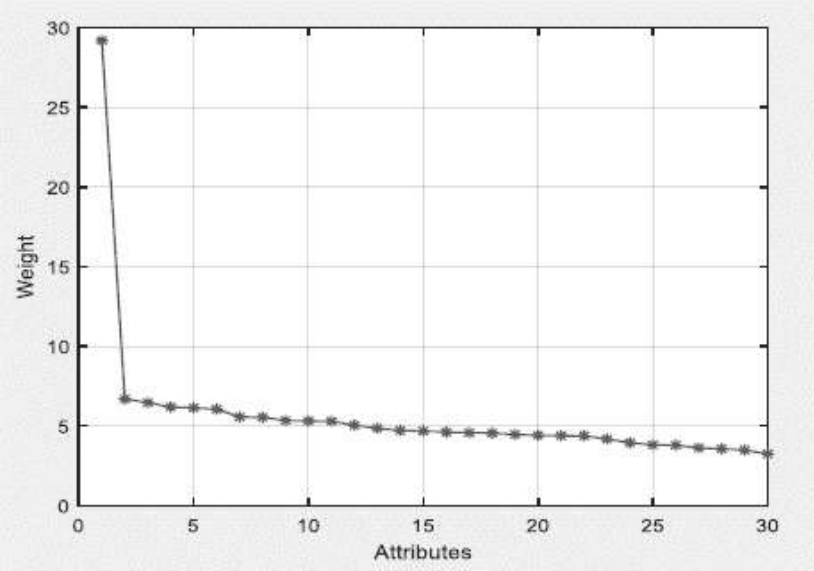

Figure 3: Weighting value for the features in the feature selection algorithm

5. Conclusion

The most frequent issue is credit card fraud, which costs individuals and certain banks and credit card companies a lot of money. In order to prevent consumers from losing their cash, as well as to benefit banked businesses, this project is working to create a model that more effectively distinguishes between transactions that are fraudulent and those that are not fraudulent by leveraging the time and quantity features in the Kegel data set.A financial institution must thus suggest automatic detection techniques to stop fraudulent behavior. Numerous studies have been conducted in this field up to this point using both Deep Learning and conventional statistical techniques while taking into account the sequential structure of transactional data. To be able to do this, we used an infinite feature selection method on a sizable dataset of credit card fraud transactions that comprises both transactions that are genuine. We will thus examine

what might indicate that a transaction to be fraudulently conducted. While the CNN algorithm will perform better, testing and application speed will still be an issue.

REFERENCES

1. D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic and A. Anderla, "Credit Card Fraud Detection - Machine Learning methods," 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, published on 22 March 2019
2. Hema Gonaboina Appala Srinuvasu Muttipati, DEEP LEARNING METHODS FOR DISCOVERING CREDIT CARD FRAUD published on 12, January 2021.
3. Zahra Kazemi , Adriano C.M. Pereira, Gisele L. Pappa, "A customized classification algorithm for credit card fraud detection", Engineering Applications of Artificial Intelligence, pp. 21-29, Volume 72, 2018.
4. N.Malini, Xianwei Li, Yiyang Dong, Ruizhe Zheng, "A Deep Neural Network algorithm for detecting credit card fraud", International Conference on Big Data,39 Artificial Intelligence and Internet of Things Engineering (ICBAIE), pp. 181-183, 2020.
5. 10. Fabrizio Carcillo, Yann-Aël Le Borgne, Olivier Caelen, Yacine Kessaci, Frédéric Oblé, Gianluca Bontempi , "Combining unsupervised and supervised learning in credit card fraud detection", Information Sciences, pp. 1-15, Volume 557, 2019.
6. Suresh Kumar, Jehyuk Lee, Hunsik Shin, Hoseong Yang, Sungzoon Cho, Seung-kwan Nam, Youngmi Song, Jeong-a Yoon, Jong-il Kim, "Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning", Expert Systems With Applications, pp. 214-224, Volume 128, 2019.
7. Gabriele Gianini, Leopold Ghemmogne Fossi, Corrado Mio, Olivier Caelen, Lionel Brunie, Ernesto Damiani, "Managing a pool of rules for credit card fraud detection by a Game Theory based approach", Future Generation Computer Systems, pp. 549-561, Volume 102, 2020.
8. Yvan Lucas, Pierre-Edouard Portier, Léa Laporte, Liyun He-Guelton, Olivier Caelen, Michael Granitzer, Sylvie Calabretto, "Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs", Future Generation Computer Systems, pp. 393-402, 2020.
9. Yvan Lucas, Pierre-Edouard Portier, Lea Laporte, Sylvie Calabretto, Liyun He-Guelton, Frederic Oble, Michael Granitzer, "Dataset shift quantification for credit card fraud detection", IEEE Second International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), pp. 97-100, 2019.
10. Chunzhi Wang, Yichao Wang, Zhiwei Ye, Lingyu Yan, Wencheng Cai, Shang Pan, "Credit card fraud detection based on whale algorithm optimized BP neural network", The 13th International Conference on Computer Science & Education (ICCSE), pp. 614-617, 2020.
11. Swathi, P. (2021). Industry Applications of Augmented Reality and Virtual Reality. *Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172*, *1*(02), 14-18.
12. Swathi, P. (2013). Scope of Financial Management and Functions of Finance. *International Journal of Advanced in Management, Technology and Engineering Sciences. ISSN NO-2249-7455*, *3*, 109-116.

13. Pothuganti, K. (2021). Long Short-Term Memory (LSTM) algorithm based prediction of stock market exchange. *International Journal of Research Publication and Reviews*, *2*(1), 90-93.
14. Swathi, P. (2022). Implications For Research In Artificial Intelligence. *Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM) ISSN: 2799-1156*, *2*(02), 25-28.
15. Ramana, S., Bhaskar, N., & Murthy, M. R. (2020). Three Level Gateway protocol for secure M-Commerce Transactions. *Solid State Technology*, *63*(6), 11155-11174.
16. Swathi, P. (2022). A Study On The Restrictions Of Deep Learning. *Journal Of Artificial Intelligence, Machine Learning and Neural Networks, ISSN-2799-1172*, *2*(2), 57-61.
17. Bhaskar, N., Ramana, S., & Kumar, G. M. (2023, January). Internet of Things for Green Smart City Application Based on Biotechnology Techniques. In *2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF)* (pp. 1-7). IEEE.
18. Ramana, S., Bhaskar, N., Murthy, M. R., & Sharma, M. R. (2023). Machine Learning for a Payment Security Evaluation System for Mobile Networks. In *Intelligent Communication Technologies and Virtual Mobile Networks* (pp. 347-356). Singapore: Springer Nature Singapore.