International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi :https://doi.org/10.32628/IJSRCSEIT

Credit Card Fraud Detection Using DNN

Prajakta Bartakke, Nakshatra Garad, Omkar More, Rutuja Nigade
Department of Computer Engineering, ZCOER, Pune, Maharashtra, India

ABSTRACT

Article Info
Volume 8, Issue 2
Page Number : 409-412

Publication Issue :
March-April-2022

Article History
Accepted: 10 April 2022
Published: 22 April 2022

Frauds in credit card transactions are common today and most happening as most of us are using the credit card payment methods more frequently. The reason behind it is the advancement in technology and surge in number of online transactions and corresponding financial loss. Therefore, there is need for effective and higher accuracy methods to reduce the loss. Moreover, fraudsters find ways to steal the credit card information of the user by sending fraud or fake SMS and calls, also through malicious attack, identity theft attack and so on. This paper aims in using the Deep Neural Networks algorithm of Deep Learning in predicting the occurrence of the fraud transaction. Further, we conduct a variation of the accomplished training and testing in deep learning techniques using balanced and imbalanced datasets to differentiate between fraud and non-fraud transactions and to acquire enough accuracy effectively.

Keywords: Deep-Learning, Machine-Learning, Tensor Flow, Deep Neural Network, Long-Short Term Memory, Recurrent Neural Network, Random Forest.

I. INTRODUCTION

In recent years, with the advent of technology, more and more people are using credit cards to meet their needs, and fraud has been steadily rising. Nowadayss almost every business be it small to large, uses a credit card as a means of payment. Oorganizations such as the telecommunication industry, the mechanical industry, banks, etc. often encounter credit card frauds. Many procedures such as data extraction, algorithmic machine learning techniques are used to detect credit card fraud but have not yielded significant results. Therefore, there is a need for more efficient and effective algorithms to be developed that are more efficient. we try to avoid fraud by using our credit card before the transaction is secured well by using deep neural network algorithm and compared to a few other machine learning algorithms.

Overview of credit card fraud detection:

Fraud is an aggressive act, performed by an unauthorized person by cheating an innocent person. Credit card fraud involves the theft of important card holders' information and the unauthorized use of fraudulent means by telephone or SMS. These credit card frauds may occur using other fraudulent software applications.

Credit card fraud occurs when the user or customer enters the information required to make any transaction using a credit card and the transaction should only be authorized when checking for fraudulent act. For any transaction to happen in a correct way, we first transfer the contents of the transaction to the verification module there, which is then classified into fraudulent and non-fraud. Any transaction that is entered under the fraud category is prohibited and is a punishable offence. If not, work will be allowed.

II. LITERATURE SURVEY

In “Credit Card Fraud Detection using Machine Learning” paper they have used machine learning algorithm for fraud detection but has a limitation regarding handling meta classifiers. In “Credit Card Fraud Detection using Python” paper they have used all the observations in datasets but has a limitation during handling big dataset. In “A Credit Card Fraud Detection using Naïve Bayes” paper, they have used Naïve Bayes Algorithm but has very low accuracy. In “Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria”, paper they have designed and coded a model for fraud detection but resampling techniques are not taken in consideration. In “Credit Card Fraud Detection” using hidden Markov Model” paper they have used HMM algorithm but target function and predicted target function doesn’t match.

III. METHODS AND MATERIAL

The proposed system uses the Deep Neural Network to detect fraud in credit card operations. Performance is measured and accuracy is calculated based on forecasts. Also, with developed learning algorithms such as deep neural networks and Recurrent Neural Networks are used to build a credit card detection model. We compare the machine learning algorithm used in the test and determine which deep neural networks predict it better than the system developed using Random Forest algorithms. The data set used in the model contains 31 of the 30 attributes that include information related to name, age, account information and more and the last attribute gives the result of activity 0 (fraudulent) or 1 (non-fraud).

IV. RESULTS AND DISCUSSION

A. Background Study

A neural network is a system which is designed to mimic human brain, consisting of an input layer, several inner layers and an output layer. The data is fed as input of the neural network. The information is then passed to the next level using appropriate weights or values and biases. The outcome of the network is the final value predicted by the artificial neuron.

B. Components

Each neuron in a neural network performs the following operations:

The product of each input and the weight or values of the channel through which it passes is observed. The sum of the weighted products is calculated or generated, which is called the weighted sum.

An random value is added to the same weighted sum.

The final addition is then fed as special function called the activation function (specific type).

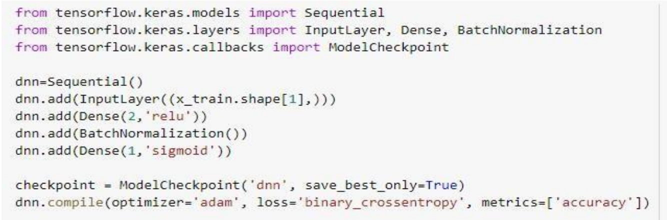
V. IMPLEMENTATION DETAILS

A. Activation Function:

The decision whether the neuron should be continued in the same way or kept suspended by setting a weighted value and adding bias to it. The main motivation of the activation function is to constitute the outcome of neuron along with the non-linearity. It is a function used to calculate the result of node. It is also called as Transfer function.

B. Callbacks:

Classes with certain set of instructions are call backs. When the model is being trained, the call backs have the admittance to the total content inside the neural net. These techniques can be used for the following: Adaptive adjustment of the learning rate. Early stoppage. Performance of the monitor Model's checkpoints. Terminating on NaN Writing the meta data of training to external files. Custom call backs can also be specified.



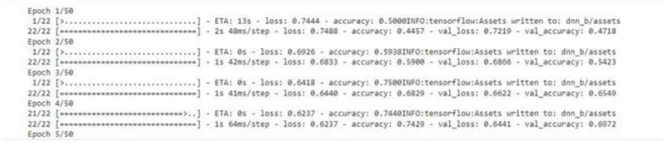
```
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import InputLayer, Dense, BatchNormalization
from tensorflow.keras.callbacks import ModelCheckpoint

dnn=Sequential()
dnn.add(InputLayer((x_train.shape[1],)))
dnn.add(Dense(2,'relu'))
dnn.add(BatchNormalization())
dnn.add(Dense(1,'sigmoid'))

checkpoint = ModelCheckpoint('dnn', save_best_only=True)
dnn.compile(optimizer='adam', loss='binary_crossentropy', metrics=['accuracy'])
```

Figure 1: Implemented Algorithm

C. Epochs:

It defines the number of times that the learning algorithm will run through the dataset. This allows the model to run until the error or area of improvement within the model has been identified or sufficiently optimized.

Processing is done on Credit card data set again and again (50 Epoch) to develop accuracy and attain better results.



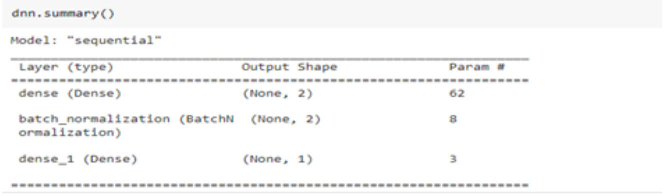
```
Epoch 1/50
 1/22 [>.............................] - ETA: 13s - loss: 0.7444 - accuracy: 0.5000INFO:tensorflow:Assets written to: dnn_b/assets
22/22 [==============================] - 2s 48ms/step - loss: 0.7488 - accuracy: 0.4457 - val_loss: 0.7219 - val_accuracy: 0.4718
Epoch 2/50
 1/22 [>.............................] - ETA: 0s - loss: 0.6926 - accuracy: 0.5938INFO:tensorflow:Assets written to: dnn_b/assets
22/22 [==============================] - 1s 42ms/step - loss: 0.6833 - accuracy: 0.5900 - val_loss: 0.6866 - val_accuracy: 0.5423
Epoch 3/50
 1/22 [>.............................] - ETA: 0s - loss: 0.6418 - accuracy: 0.7500INFO:tensorflow:Assets written to: dnn_b/assets
22/22 [==============================] - 1s 41ms/step - loss: 0.6440 - accuracy: 0.6829 - val_loss: 0.6622 - val_accuracy: 0.6549
Epoch 4/50
21/22 [===========================>..] - ETA: 0s - loss: 0.6237 - accuracy: 0.7440INFO:tensorflow:Assets written to: dnn_b/assets
22/22 [==============================] - 1s 64ms/step - loss: 0.6237 - accuracy: 0.7429 - val_loss: 0.6441 - val_accuracy: 0.6972
Epoch 5/50
```

Figure 2: Epochs

D. DNN Summary - Sequential

Batch normalization

To synchronize the detailed layers along with the inside layers by making modifications in the scaling and mean of the activation is termed as normalization. Result of using this normalizing effect in deep neural networks along with the additional layer gives the higher rate of learning without disappearing or exploding elements.



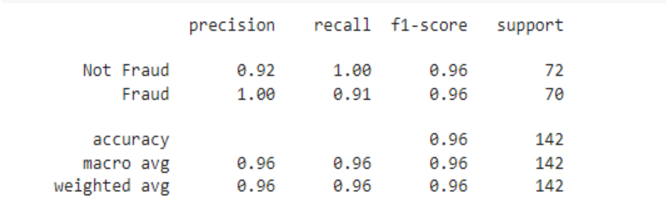
```
dnn.summary()

Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 dense (Dense)               (None, 2)                 62

 batch_normalization (BatchN  (None, 2)                8
 ormalization)

 dense_1 (Dense)             (None, 1)                 3

=================================================================
```

Figure 3: DNN Summary

OPTIMIZERS

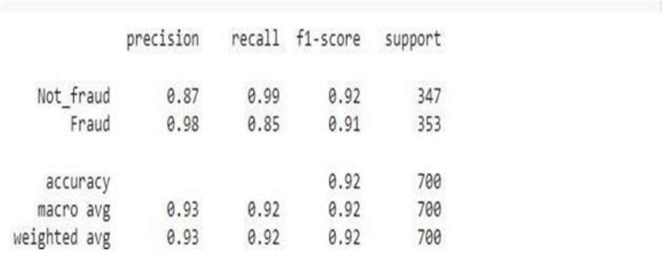
The function or an algorithm that modifies the factors and attributes of the neural network such as weights and the rate of learning is termed as optimizer in deep learning terms. As the overall loss is reduced, i t helps in improving the efficiency.

E. Final Output



```
              precision    recall  f1-score   support

   Not Fraud       0.92      1.00      0.96        72
       Fraud       1.00      0.91      0.96        70

    accuracy                           0.96       142
   macro avg       0.96      0.96      0.96       142
weighted avg       0.96      0.96      0.96       142
```

Figure 4: Classification Report for DNN



```
              precision    recall  f1-score   support

   Not_fraud       0.87      0.99      0.92       347
       Fraud       0.98      0.85      0.91       353

    accuracy                           0.92       700
   macro avg       0.93      0.92      0.92       700
weighted avg       0.93      0.92      0.92       700
```

Figure 5: Classification Report for Random Forest

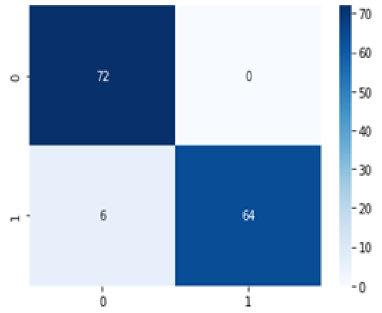


Figure 6: Configuration Matrix

VI. CONCLUSION

From our approach we can conclude that, Keras based Deep Learning Neural Network proves to be a great alternative to other classifiers mentioned above. Also, no matter how accurate the trained model of the network might be, it will not show accurate results unless the skewness of the data is reduced. It can be inferred that Under- Sampling works better in this case because the smaller number of observations help in training the network efficiently When we consider the precision, recall, and the F1-score the DNS algorithm has the highest value than the Random Forest algorithm.

VII. REFERENCES

[1]. Inc. US Legal. Internet fraud law and legal definition

[2]. U.S. payment card fraud losses by type 2018 | statistic

[3]. Mohammed, M., Khan, M.B., Bashier, E.B.M.: Machine Learning: Algorithms and Applications. Crc Press, Boca Raton (2016)

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

[5]. Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., Beling, P.: Deep learning detecting fraudin credit card transactions. In: Systems and Information Engineering Design Symposium (SIEDS) (2018)

[6]. Machine Learning: the Power and Promise of Computers That Learn by Example. The Royal Society, Machine Learning: the Power and Promise of Computers That Learn by Example.