A New Model for Detecting Fraudulent Credit Card Transactions Using Deep Learning Algorithms

Dr.D.J.Samatha Naidu,

Principal, Annamacharya PG College Of Computer Studies, Rajampet, Annamayya Dist, AP, 516126.

Tugutla Sainath

MCA, Annamacharya PG College Of Computer Studies, Rajampet, Annamayya Dist, AP, 516126

Abstract

Fraudulent credit card transaction is still one of problems that face the companies and banks sectors; it causes them to lose billions of dollars every year. The design of efficient algorithm is one of the most important challenges in this area. This project aims to propose an efficient approach that automatic detects fraud credit card related to insurance companies using deep learning algorithm called Autoencoders. The effectiveness of the proposed method has bee. n proved in identifying fraud in actual data from transactions made by credit cards. In addition, a solution for data unbalancing is provided in this paper, which affects most current algorithms. The suggested solution relies on training for the autoencoder for the reconstruction normal data. **Keywords:**

| Date of Submission: 26-08-2022 | Date of acceptance: 10-09-2022 |
|--------------------------------|--------------------------------|

I. INTRODUCTION

The Association for Payment Clearing Services (APACS) has estimated that total losses through credit card fraud in the United Kingdom have been growing rapidly from £122 million in 1997 to £440.3 million in 2010 [1]. According to the Nelson report [2], the losses on global credit and prepaid cards reached \$ 24.71 billion in 2016, up 11.2 percent from 2015. Gross fraud losses are absorbed by card issuers and merchants as well as by acquirers of transaction from ATMs and Merchant. A central feature of the report, the LexisNexis Fraud Multiplier [3], estimates the total amount of loss a merchant incurs, based on the actual dollar value of a fraudulent transaction. According to the Fraud Multiplier tool, In 2016, every dollar of fraud cost merchants \$2.40, up from \$2.23 a year ago. Also, the report finds that the volume of fraud raised sharply in the last year, from a monthly average of 156 to 206 successful fraudulent transactions, and from 177 to 236 prevented fraudulent transactions, while the level of fraud as a percentage of revenues also inched upward from 1.32 percent to 1.47 percent.

Objective

In this paper we are training Auto Encoder and Decode deep learning model on credit card dataset to predict normal and fraud transaction. To train model we have normalized the dataset and then split dataset into train and test and then by using TRAIN dataset we have trained AUTOENCODER and DECODER model.

II. RELATED WORK

Some techniques of machine learning treat transaction fraud as a problem of supervised classification. In this manner, together with annotations, we can train a classifier based on training data, then classify test transaction data into normal and abnormal classifications. Fraud Credit card is not restricted to transactions only, but to transactions and the features in which they occur

SCOPE

To find the frauds in the credit card business by using the algorithms which adopted machine learning techniques. Two algorithms are used viz Fraud Detection in credit card using Decision Tree and Fraud Detection using Random Forest. Then, an actual world credit card facts group from a financial institution is examined.

III. METHODS

1.Auto encoder Classifier Method

Auto encoder learn is a unsupervised learning seeking to be output corresponding to their income and therefore can be considered the network as a supervised learning, the output is the result of reconstruction the original income x. An autoencoder learns to map from input to output through a pair of encoding and decoding phases.

The encoder maps from the input to hidden layer, the decoder maps from the hidden layers to the output layer to reconstruct the inputs

2.Auto Encoders architecture consists Method

Encoder: it is the part in which the model learns how to reduce the input dimensions and compress the input data into an encoded representation.Bottleneck: it is the layer that contains the compressed representation of the input data. This is the lowest possible dimensions of the input data.

3.Decoder: it is the model that learns how to reconstruct the data from the encoded representation to be as close to the original input as possible .



IV. SAMPLE SCREENS

Screen : Credit Card Datase

Description: In above screen click on 'Upload Credit Card Dataset' button to upload dataset.



Screen :upload dataset



Screen:MAE histogram on Non-Fraudulent TransactionScreen :.

Description: In above text area we can see testing accuracy is 0.97 and in above non-fraud transaction MAE graph x-axis represents number of test records and y-axis represent MAE values and MAE got decrease when test data records increase and now close above graph and then click.

| | | S Figure 1 | | | | | | 2 X | | |
|--|----------------|---|------------|-------|---------|-----|-----|-----------|-----------|--|
| | | | | | | | | | | |
| Auto Encoder Decoder Accuracy on Test Data: 0.9760366560162915 | | MAE histogram on Fraudulent Transaction | | | | | | | | |
| | | 70 - | | | | | | | | |
| | | 60 - | | | | | | | | |
| | | | | | | | | | | |
| | | 50 - | | | | | | | | |
| | | 40 - | | | | | | | | |
| | | 30 - | | | | | | | | |
| | | | | | | | | | | |
| | | 20 - | | | | | | | | |
| | | 10 - | | | | | | | | |
| | | | | - 110 | 200 000 | | | - | | |
| | | | ò | 50 | 100 | 150 | 200 | 250 | | |
| Upload Credit Card Dataset | Normalize & D | | ++ 0 | | 1 | | | x=213.803 | v=51.8784 | |
| Train AutoEncoder & Decoder Model | Extract Encode | r & Decoder | for Predic | tion | 9 | | | | - | |
| | | | | | | | | | | |
| MAE Histogram on Fraud Transaction | | | | | | | | | | |

Screen : Graph Showing on Fraudulent Transaction

Description: In above graph for each fraud transaction we got MAE values and plot in histogram where x-axis represents test record number and y-axis represent MAE value for that record.

V. CONCLUSION

In this paper, we have proposed a with the large and ongoing financial loss currently being experienced by financial companies, It was necessary to develop more efficient methods on which the electronic systems to detect fraudulent transactions, fraud detection is a very difficult and complex task. Fraudulent activities are rare events that are difficult to model, and the large volume of day-to-day transactions requires automated tools to support the science of fraud verification. In this project, some advanced techniques have been introduced to detect the fraud credit card of the insurance company.