JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Optimization Accuracy of Credit Card Fraud Prediction using Deep Learning Neural Network

Kumar Ujjawal[1], Prof. Suresh. S. Gawande[2]
M. Tech. Scholar, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal[1]
Guide, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal[2]

Abstract: **Cloud computing and mobile computing have increasing its performance with rapid manner through numerous area of applications, these are extending such as digital payments, storage and confidential information accessing. Current technology offers several internet applications by using cloud based electronic payment methods, therefore security and confidentiality is necessary. According to national herald in India 42% frauds are identified in various fields from 1990 to 2020. Like "no fraud" agency in USA identified around 30% frauds since 1990, every year these frauds are increases with high ratios. Frauds did not have particular patterns, also change their behavior at every time. These frauds are most probably recognized at cloud based e-commerce and trade business websites. In order to decrease this frauds ratio, we need to develop a real and accurate fraud detection system. In this research with the help of deep and machine learning optimization methods has been used to detect the cloud based frauds. So many, existed works solve this issue but accuracy, F-score, recall and precession are very less. Because of this limitation, in this work is introduced deep learning mechanisms like fully Edited Nearest Neighbor (ENN) and deep neural network (DNN). The DNN with ENN is best technique for credit card fraud prediction and achieve good accuracy.**

Index Terms **– Credit Card, Deep Learning, ENN, DNN, Accuracy**

I. INTRODUCTION

Now a day's virtual companies and the internet are changing the scenario of traditional commerce. As the internet provide a global market, more flexibility and more competition in market, e-commerce value is increased. E-commerce also provides easier and wide range of innovation in the field of banking and payment. It plays a main role in global and competitive market. Is global market increasing people is diverting toward digital market instead of traditional market. As it gives facilities to customer, it has number of limitations also. Online payment is the vital thing for Ecommerce or Digital market. As universal market increasing the demand for Financial and Banking sector for payment is become standard in present days. Online payment gives you benefits to perform transaction from anywhere, anytime and anyplace with the help of smart devices like laptop, mobile, desktop, PDA, etc. The main objective behind electronic payment growth is it removes the limitations of traditional commerce. A user does not have to stand in long queue and personally visits the Bank to settle transaction. It gives many benefits like transactions are become faster that are done in few minutes, no need to visits banks and stand in queue. There are two ways to performed Electronic payment that are either online or offline. Online payment can identify as virtual payment. In online payment, it requires account holder name, PIN, card number, expiry date, etc. sensitive information. Offline payment can identify as physical payment. For offline payment, presence of card holder and PIN are required [1, 2].

For online payment frauds first thing is required is credit card number of some card holder. There is a many way to accomplish these scams. Some popular methods for online credit card frauds are phishing, identity theft, skimming, lost or stolen card use, card cloning, etc. Apart from these methods some another mechanism that allow credit card scams such as, malware or key loggers who can hack credit card details while online transaction, scanning devices are used to read tour credit card details [3, 4].

While online payment does not require signature or PIN number of your card, it makes process easier. Most of the websites are stealing card details and selling them to third party, number of the fraudsters are available on dark web so difficulty to trap. For offline payment frauds two mechanisms are most important that are ATM system and POS system. Fraudsters are creating clone card, card trapping, forged ATM or POS devices, identity theft, lost or stolen card, suspicious system, network or device [5].

In online transaction that stops consumer scam due to copy of payment card numbers, this creation includes at least one reliable card host. Payment card processing steps are as follow:

- Customer choose host, and place online order. While placing online order payment card number is not sended.
- Merchant allocates an OrderID for the placed order.
- Customer verifies payment details via host using private key, merchant also request for payment verification via host. Customer and merchant both verify payment with the same orderID.
- Host compares orderID and improve private key. The host combine it with the set of private key to fetch payment card number.
- After that host sends request for payment verification of card holder through payment network.
- When card holder sends back the response of payment verification, response sends back to the merchant.
- Merchant completes the order and Send for payment via the host.
- During the online transaction, all information are transfer through the SSL in an encrypted form, and when recipient receives it in decrypted form.

II. TYPES OF CARDS

Payment cards are the part of payment system i.e. issued by payment organization or bank. There are number of different type of cards available in market. But most common card used by customer is either credit card or debit card. Consumer used it for payment purpose. It can be used either for physical payment or virtual payment. It removes the concept of carry paper money. Advantage of digital cash is no need to carry cash and merchant cannot refuse to accept it. Following chart shows the various types of card available in Mauritius market. Each and every card has its unique features. Customer can issue card from legal organization as per their needs.

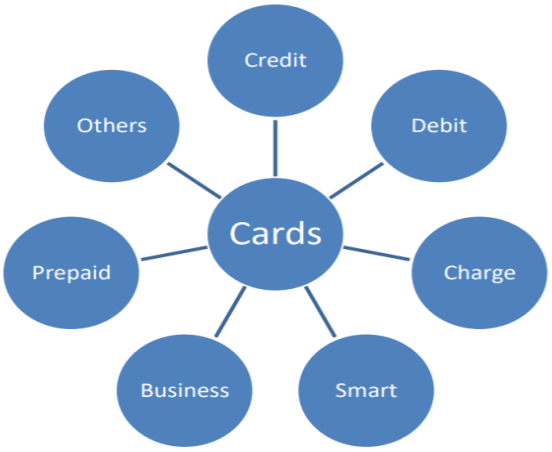


Fig. 1: Type of cards

1. Credit card: It is a plastic material card, issued by bank or payment organization. It gives credit to customer for purchase goods or services. There is spending limit on card.

2. Debit card: It is plastic material card, issued by bank to their account holder. It is different from credit card, it directly withdrawal money from customer account. Normally used for cashless transaction.

3. Charge Card: It is plastic card that is differing from credit card. It is provided by payment organization to consumer and they have to pay for card. It allows customer to do online or physical spending. Card has no credit limit.

4. Smart Card: It is a chip based plastic card provided by bank to their customers. This card has no credit limit. Periodically card holder will pay for their card statement. Customers have to pay fees to card issuing company.

5. Business Card: A business card is similar to plastic material credit card. Card holder name, job title, business address, phone number, etc. information printed on card. Business card is used for business expenses at your home or abroad. It can be business debit card or credit card.

6. Prepaid Card: It is not like credit or debit card. Unlike credit or debit card, for prepaid card u does not require a bank account. The amount in the card must have to fill in advanced. You can spend money that is loaded in your card for payment. It is reusable card; ones loaded amount is used, consumer can reload or throw the card.

7. Other Cards: Apart from all these types of cards, there are many different types of cards like cheque card, gift card, cash card, reward card, etc.

III. PROPOSED METHODOLOGY

An Artificial Intelligence Fraud Detection (AIFD) as an advanced Linear Regression model has been built to analyse a very complex credit card transaction dataset with several fixed features converted to various numerical values, and then the model output determined whether or not that particular transaction was fraudulent: 1.0 or legitimate: 0.0.

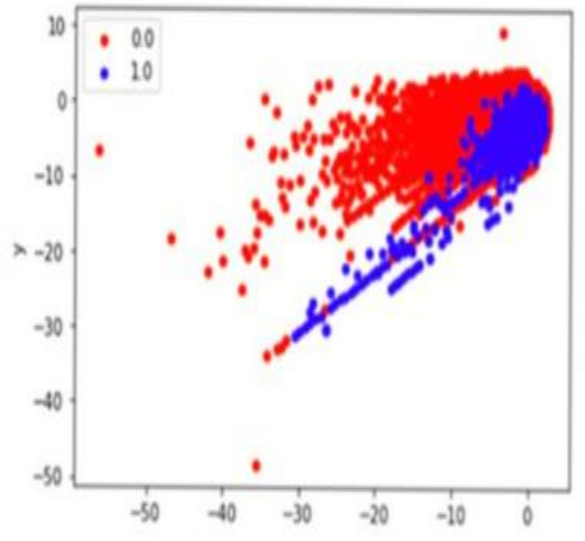


Fig. 2: Credit Card dataset

A given credit card dataset has already undergone some Principal Component Analysis (PCA) and ML technique and contains 284807 transactions and significantly unbalanced with the frauds account of 0.172%, thus the data highly lean towards legitimate 284315, represented by X = 0.0 (red) vs fraudulent 492 transaction represented by y = 1.0 (blue) in order to get the representation of the data. The Credit card dataset has been visualised using scatter graph with x, y features in order observe the compression before and after SMOTE ENN has been applied (Fig. 2).

The AIFD model has been created in order to efficiently test our deep neural network up to 5 layers, and a number of functions in order to improve its accuracy (Fig. 3).

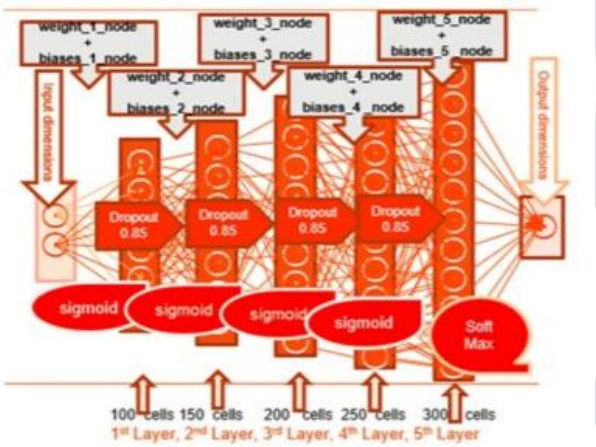


Fig. 3: Visual representation of AIFD

The neural network has been trained and tested first with the unprocessed data then with SMOTE + ENN then each layer has been observed for its accuracy in order to determine the most efficient number of layers required for AIFD efficiency, thus number of cells per each layer (L) has been added: L1=100, L2=150, L3=200, L4=250, L5=300. The dropout function: 0.85, Adam Optimizer: 0.006, number of epochs 1000 has been selected to generate the best results.

Synthetic Minority Oversampling and Edited Nearest Neighbours

The Synthetic Minority Oversampling and Edited Nearest Neighbours (SMOTE ENN) algorithm is a hybrid approach that applies over-sampling (OS) with SMOTE to generate the synthetic samples for the minority imbalanced class: 1.0 (IC) and then applies cleaning techniques to under-sample with ENN to the newly generated instance: imbalanced credit card data (ICCD) plus newly created (NC) data resulting in synthetic credit card (CC) SMOTE ENN dataset (Fig. 4).

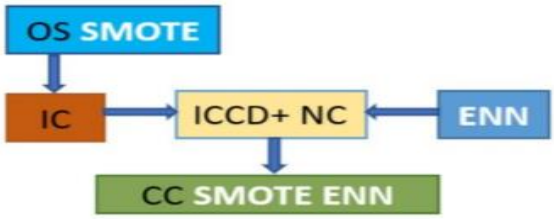


Fig. 4: Visual representation of SMOTE ENN algorithm

The credit card dataset was pre-processed using SMOTE + ENN algorithm with sampling strategy 0.5, where minority examples increased when SMOTE was applied, and the majority examples were removed once the nearest neighbor is applied to generate 284807 transactions: legitimate 268103, represented by: X = 0.0 (red) vs fraudulent 131310 transaction: represented by: y = 1.0 (blue); thus, imbalanced with the frauds account of 0.329% (Fig. 5). It has been observed that AIFD model initial loss (IL) and final

loss (FL), have improved by pre-processing credit card dataset using SMOTE + ENN algorithm, by taking slightly longer in initial elapsed time in seconds (IET/s) and final elapsed time in seconds (FET/S).

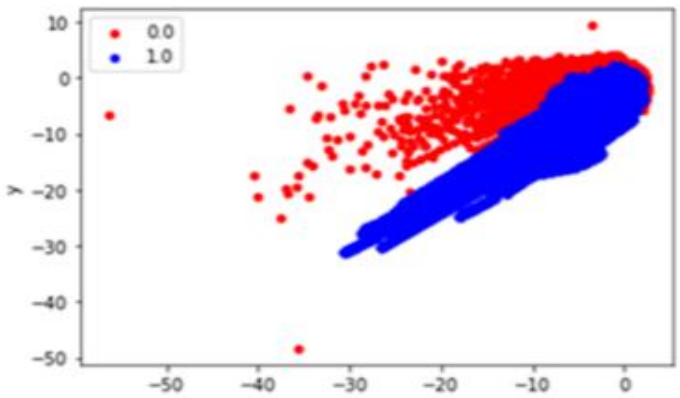


Fig. 5: Credit Card (SMOTE ENN) dataset

IV. SIMULATION PARAMETERS

Dataset was separated into two datasets (70%/30%, preparing/testing) to keep away from any predisposition in preparing and testing. Of the information, 70% was utilized to prepare the ML model, and the excess 30% was utilized for testing the presentation of the proposed movement arrangement framework. The articulations to compute accuracy and review are given in Equations (2) and (3).

Accuracy gives a proportion of how precise your model is in anticipating the real up-sides out of the absolute up-sides anticipated by your framework. Review gives the quantity of real up-sides caught by our model by grouping these as obvious positive. F-measure can give a harmony among accuracy and review, and it is liked over precision where information is uneven.

Accordingly, F-measure was used in this review as a presentation metric to give a decent and fair measure utilizing the equation.

$$\text{Precision} = TP\ TP + FP \times 100$$

$$\text{Recall} = TP\ TP + FN \times 100$$

$$F - \text{measure} = 2 * \text{Precision} * \text{Recall}\ \text{Precision} + \text{Recall} \times 100$$

Where,

TP—True Positive, FP—False Positive, FN—False Negative

V. SIMULATION RESULTS

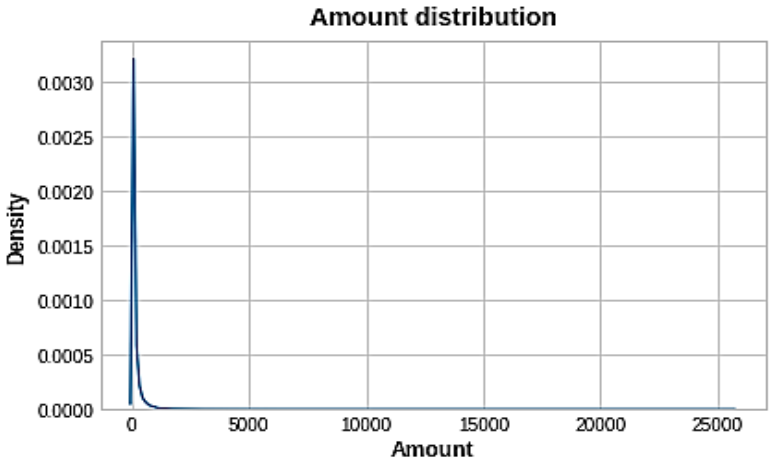
Step1- Dataset gathering and information

The dataset covers credit card transactions done by Mauritius cardholders. In this dataset, we have 492 frauds out of 284,807 transactions that occurred in the last two days. The dataset is heavily skewed, with the positive class (frauds) accounting for only 0.172 percent of all transactions.

The major components derived with PCA are features V1, V2...V28; the only features not changed with PCA are 'Time' and 'Amount.' Feature the seconds elapsed between each transaction and the first transaction in the dataset are stored in the 'Time' field. The transaction Amount is represented by the feature 'Amount,' which can be utilized for example-dependent cost-sensitive learning. Feature the answer variable is called 'Class,' and it has a value of 1 when there is fraud and 0 when there isn't.

Step2 – Data preprocessing

1. Check Duplicate values in pandas data frame and found
2. 8063 duplicate data, all related to non fraudolent transactions. I will drop them.
3. Amount Distribution



4. Box Cox and Log Transformation on Amount

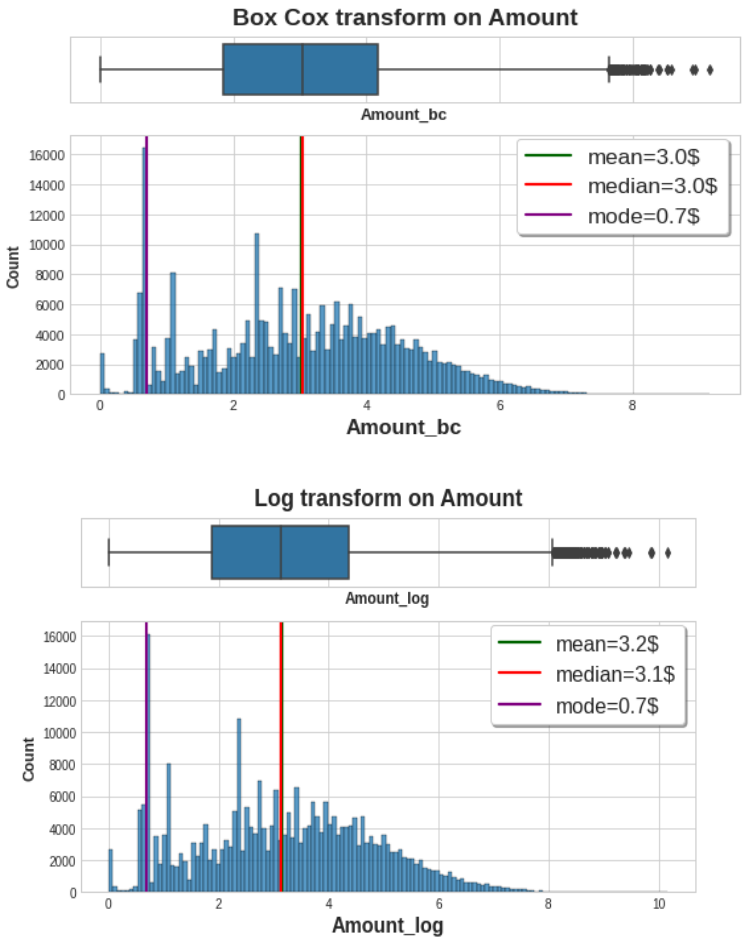


Table 1: Comparison results of Base Algorithms and Proposed Algorithm

Results	Naïve Bayes	Logistic Regression	K-NN	Proposed Algorithm
Recall	0.846	0.612	0.704	0.757
Precision	0.058	0.821	0.861	0.837
F1 Score	0.109	0.701	0.775	0.795
Accuracy	0.976	0.988	0.988	0.999
True Negative	55535	56851	56864	56637
True Positive	83	60	62	72
False Negative	15	38	26	23
False Positive	1329	13	10	14

VI. CONCLUSION

Electronic payment has two options users either choose online or offline. In virtual payment, user have to give account holder name, PIN, card number, expiry date, etc. information. For physical payment, occurrence of card and PIN are required. Online payment having various options, users are using different kinds of payment instruments such as credit card, debit card, net banking, e-wallet, UPI, etc. Credit card is the most common standard and most promising Electronic payment mechanism for online shopping. Use of online payment mechanisms are increasing now days. The credit card can be used as online or offline. From the simple analysis report, the most intended payment method for hacker is credit card.

Today, for the business companies or banking sectors the Credit Card Fraud become one of the biggest issues that requires more safety and security. As technologies are increasing, facilities are increasing with that other hand Credit card fraud scams are also rising. Consumers wants secure channel to complete the transaction. There are many different types of credit card frauds and we can detect the fraud transaction by available different fraud detection techniques.

REFERENCES

[1] *Vipul Jain, H Kavitha and S Mohana Kumar, "Credit Card Fraud Detection Web Application using Streamlit and Machine Learning", International Conference on Data Science and Information System (ICDSIS), IEEE 2022.*

[2] *Yathartha Singh, Kiran Singh and Vivek Singh Chauhan, "Fraud Detection Techniques for Credit Card Transactions", 3rd International Conference on Intelligent Engineering and Management (ICIEM), IEEE 2022*

[3] F. Itoo and S. Singh "Comparison and analysis of logistic regression Naïve Bayes and KNN machine learning algorithms for credit card fraud detection" International Journal of Information Technology vol. 13 no. 4 pp. 1503-1511 2021.

[4] E. S. C. R. S K Saddam Hussain "Fraud Detection in Credit Card Transactions Using SVM and Random Forest Algorithms" IEEE Xplore 2021.
[5] E. Ileberi Y. Sun and Z. Wang "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost" IEEE vol. 9 no. 5 pp. 165286-165294 2021.
[6] D. Tanouz R. R. Subramanian and D. Eswar "Credit Card Fraud Detection Using Machine Learning" IEEE 2021.
[7] S. Khatri A. Arora and A. P. Agrawal "Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison" IEEE 2020.
[8] M. S. Kumar V. Soundarya S. Kavitha E. Keerthika and E. Aswini "Credit Card Fraud Detection Using Random Forest Algorithm" IEEE 2019.
[9] M. K. Dejan Varmedja "Credit Card Fraud Detection - Machine Learning methods" IEEE Xplore 2019.
[10] Vaishnavi Nath Dornadula and S Geetha "Credit Card Fraud Detection using Machine Learning Algorithms" Procedia Computer Science vol. 165 pp. 631-641 2019.
[11] I. Sadgali N. Sael and F. Benabbou "Fraud detection in credit card transaction using neural networks" Proceedings of the 4th International Conference on Smart City Applications (SCA '19) 2019.
[12] G. L. S. Xuan "Random forest for credit card fraud detection" IEEE 15th International Conference on Networking Sensing and Control (ICNSC) 2018.
[13] I. Sohony R. Pratap and U. Nambiar "Ensemble learning for credit card fraud detection" Proceedings of the ACM India Joint International Conference on Data Science and Management of Data Association for Computing Machinery 2018.
[14] J. O. Awoyemi and A. O "Credit card fraud detection using machine learning techniques: A comparative analysis" IEEE 2017.