

Credit Card Fraud Detection using AI

Mr. Vaibhav Shende¹, Prof. Sunita Nandgave² and Prof. Mansi Bhonsle³

¹⁻³G.H. Raison College of Engineering Management, Wagholi, India
vaibhavshende54@gmail.com

Abstract—In today's world the credit card fraud is the biggest issue and now there is need to combat against the credit card fraud. "credit card fraud is the process of cleaning dirty money, thereby making the source of funds no longer identifiable." On daily basis, the financial transactions are made on huge amount in global market and hence detecting credit card fraud activity is challenging task. As earlier (Anti- credit card fraud Suite) is introduced to detect the suspicious activities but it is applicable only on individual transaction not for other bank account transaction. To Overcomes issues of we propose Machine learning method using 'Structural Similarity', to identify common attributes and behavior with other bank account transaction. Detection of credit card fraud transaction from large volume dataset is difficult, so we propose case reduction methods to reduces the input dataset and then find pair of transaction with other bank account with common attributes and behavior.

Index Terms— Machine Learning, fraud detection, AI, Algorithm.

I. INTRODUCTION

credit card fraud scrub as much as 5 of the world's GDP (Gross Domestic Product.) every year. Combating credit card fraud using AI is to detect the suspicious activities. Combating credit card fraud typically requires most entities that complete financial transactions to keep thorough records of their clients' accounts and activities. If they come across any information that appears to be suspicious, they are required to report it to the government for further investigation. In this Transaction records is check to detect credit card fraud activity if the suspicious data is detected. Here we use Artificial Intelligence and Machine Learning Algorithm to detect the suspicious activities and solve it by training the data of that activity. We are going to use supervised and unsupervised algorithm techniques.

II. LITERATURE SURVEY

1. Paper Name : Financial Fraud Detection with Anomaly Feature Detection

- Authors :Dongxu Huang, Dejun Mu, Libin Yang, Xiaoyan Cai
- Description :In recent years, financial fraud activities such as credit card fraud, credit card fraud, increase gradually. These activities cause the loss of personal and/or enterprises' properties. Even worse, they endanger the security of nation because the profit from fraud may go to terrorism [1][25]. Thus, accurately detecting financial fraud and tracing fraud are necessary and urgent. However, financial fraud detection is not an easy task due to the complex trading networks and transactions involved. Taking credit card fraud as an •

2. Paper Name :A New Algorithm for credit card fraud Detection Based on Structural Similarity

- Author :Reza Soltani, Uyen Trang Nguyen, Yang Yang, Mohammad Faghani, Alaa Yagoub, Aijun

- Description : There are many methods of credit card fraud. Criminals can hide the source of money by using the funds in casinos or real estate purchases, or by overvaluing legitimate invoices. In general, a credit card fraud procedure is composed of three major steps: placement, layering and integration [2]. Placement is the process of introducing the dirty money into the financial system by some mean. Layering is the processing of carrying out complex transactions to hide the source of the funds. Finally, integration is to withdraw the proceeds from a destination bank account. The purpose of performing complex layering is to confuse anti-credit card fraud instruments.

3. Paper Name : Prevention of Credit Card Fraud Detection based on HSVM

- Author : V. Mareeswari

- Description : Specific crime in the banking system is credit card fraud. Credit card usage has been increased due to the rapid growth of E-commerce techniques. Credit card fraud also increased at the same time. Prevention is better than detection. So the existing system prevented the credit card fraud by identifying fraud in the application of the Credit card. Due to the limitation of the existing system, this paper proposed new algorithm along with the existing algorithm. Scalability issues, extreme imbalanced class and time constraints are the limitation of existing systems. Those limitations are overcome by hybrid support vector machine (HSVM) along with communal and spike detection for credit card application fraud detection. HSVM is the most used method for the pattern recognition and classification.

4. Paper Name : Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme

- Author : Arun Kumar Rai , Rajendra Kumar Dwivedi

- Description : Development of communication technologies and ecommerce has made the credit card as the most common technique of payment for both online and regular purchases. So, security in this system is highly expected to prevent fraud transactions. Fraud transactions in credit card data transaction are increasing each year. In this direction, researchers are also trying the novel techniques to detect and prevent such frauds. However, there is always a need of some techniques that should precisely and efficiently detect these frauds. This paper proposes a scheme for detecting frauds in credit card data which uses a Neural Network (NN) based unsupervised learning technique. Proposed method outperforms the existing approaches of Auto Encoder (AE), Local Outlier Factor (LOF), Isolation Forest (IF) and K-Means clustering. Proposed NN based fraud detection method performs with 99.87% whereas existing methods AE, IF, LOF and K Means gives 97, 98, 98 and 99.75 accuracy respectively.

5. Paper Name : Analysis on Credit Card Fraud Identification Techniques based on KNN and Outlier Detection

- Author : N. Malini, M. Phil

- Description : Popular payment mode accepted both offline and online is credit card that provides cashless transaction. It is easy, convenient and trendy to make payments and other transactions. Credit card fraud is also growing along with the development in technology. It can also be said that economic fraud is drastically increasing in the global communication improvement. It is being recorded every year that the loss due to these fraudulent acts is billions of dollars. These activities are carried out so elegantly so it is similar to genuine transactions. Hence simple pattern related techniques and other less complex methods are really not going to work. Having an efficient method of fraud detection has become a need for all banks in order to minimize chaos and bring order in place. There are several techniques like Machine learning, Genetic Programming, fuzzy logic, sequence alignment, etc are used for detecting credit card fraudulent transactions. Along with these techniques, KNN algorithm and outlier detection methods are implemented to optimize the best solution for the fraud detection problem. These approaches are proved to minimize the false alarm rates and increase the fraud detection rate. Any of these methods can be implemented on bank credit card fraud detection system, to detect and prevent the fraudulent transaction.

6. Paper Name : Real-time Credit Card Fraud Detection Using Machine Learning

- Author : Anuruddha Thennakoon, Chee Bhagyan , Sasitha Premadasa, Shalitha Mihiranga, Nuwan Kuruwitaarachchi

- Description : Credit card fraud events take place frequently and then result in huge financial losses [1]. The number of online transactions has grown in large quantities and online credit card transactions holds a huge share of these transactions. Therefore, banks and financial institutions offer credit card fraud detection applications much value and demand. Fraudulent transactions can occur in various ways and can be put into different categories. This paper focuses on four main fraud occasions in real-world transactions. Each fraud is addressed using a series of machine learning models and the best method is selected via an evaluation. This evaluation provides a comprehensive guide to selecting an optimal algorithm with respect to the type of the frauds and we illustrate the evaluation with an appropriate performance measure. Another major key area that we address in our project is real-time credit card fraud detection. For this, we take the use of predictive analytics done by the

implemented machine learning models and an API module to decide if a particular transaction is genuine or fraudulent. We also assess a novel strategy that effectively addresses the skewed distribution of data. The data used in our experiments come from a financial institution according to a confidential disclosure agreement. 2.1 Research Gap Identify.

III. FIGURES

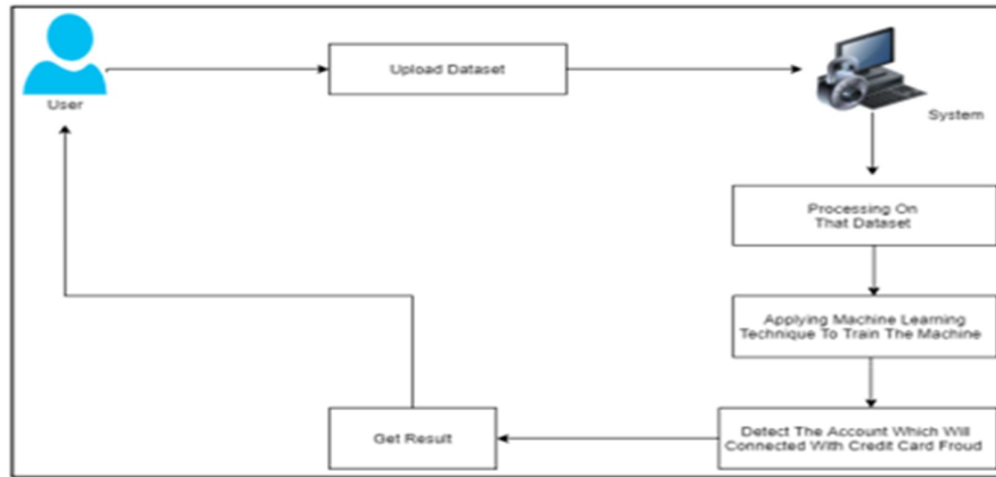


Figure 1. System Architecture

Expert commentary based on algorithms developed by Cnn Model (ConvNet/CNN), this algorithm can classify images by assigning relative importance to various aspects and objects within the image. Neural pathways are assumed to be familiar to the reader. In the deep learning, Ai - based Neurons are the best. Techniques is used to classify the image, audio, and words. LSTMs and CNNs, 2 types of neural networks, can still be used to predict word sequences and classify images, respectively. We're going to lay the groundwork for CNN's infrastructure in this document. Before diving into the Deep Multilayer Perceptron, a refresher in neural concepts is in order. Neural networks typically have three layers.

There are three levels of input: That's the layer where we put the data that we'll be feeding into our model. Neurons in this layer correspond to each feature in our dataset. It's worth listening to the hidden neuron to process data that's coming in through the Input layer. There may well be a plethora of layers depending on our model and data size. The total of hidden neurons increases of features increases. In order to make the network nonlinear, the previous layer's output is multiplied by the previous layer's learnable weight training but then learnable biases are added. It is possible to modify the hidden layer's output into the probability score for every class using an algorithm like sigmoid or softmax.

A. Motivation

We can identify and group potential credit card fraud accounts.

Modelling past credit card transactions with the data of the ones that turned out to be fraud.

Credit Card Fraud Detection is a typical sample of classification SVM (support vector machine) machine learning algorithm.

B. Objective

To identify suspicious events and report them to an analyst while letting normal transactions be automatically processed.

To detect card fraud using Support vector machine learning algorithm.

C. Problem Statement

The aim of this project is to detect the suspicious activities of bank transaction to identifying the Credit card Fraud . Also to reduces the amount of criminal activities. The people involved in Credit card obviously try to conceal the real purpose of money transfer used in this process.

IV. CONCLUSIONS

The proposed ML framework aims to find potential money-laundering groups among a large number of financial transactions. In order to improve the efficiency of the framework, case reduction methods such as matching transaction detection and balance score filter are used to narrow down the list of potential ML accounts. Next by taking advantage of structural similarity, we can identify and group potential credit card fraud accounts. Our preliminary experimental results show a high degree of accuracy in detection of ML accounts.

REFERENCES

- [1] "Fatf-gafi.org - Financial Action Task Force (FATF)", Fatf-gafi.org, 2016. [Online]. Available: <http://www.Fatf-gafi.org>. [Accessed: 22-Dec- 2015].
- [2] Fatf-gafi.org, 'credit card fraud - Financial Action Task Force (FATF)', 2014. [Online]. Available: <http://www.fatfgafi.org/faq/moneylaundering/>. [Accessed: 22- Dec- 2015].
- [3] Neo4j Graph Database, 'Neo4j, the World's Leading Graph Database', 2014. [Online]. Available: <http://neo4j.com/>. [Accessed: 22- Dec- 2015].
- [4] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten. Improving credit card fraud detection with calibrated probabilities. In SDM, 2014.
- [5] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han. Outlier Detection for Temporal Data. Synthesis Lectures on Data Mining and Knowledge Discovery, Morgan Claypool Publishers, 2014.