IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 4, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004106|

Credit Card Fraud Detection Using ML

Prof. Kadam P. N, Vijaykumar Shete, Meghraj Fand, Vaibhav Kale, Saurabh Pawar

Professor, Department of Computer Engineering, SVPM's College of Engineering, Malegaon Bk, India

Department of Computer Engineering, SVPM's College of Engineering, Malegaon Bk, India

Department of Computer Engineering, SVPM's College of Engineering, Malegaon Bk, India

Department of Computer Engineering, SVPM's College of Engineering, Malegaon Bk, India

Department of Computer Engineering, SVPM's College of Engineering, Malegaon Bk, India

ABSTRACT: In today's world credit card fraud is the biggest issue and now there is a need to combat 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, financial transactions are made on a huge amount in the global market, and hence detecting credit card fraud activity is a challenging task. As earlier (Anti-credit card fraud Suite) is introduced to detect the suspicious activities but it is applicable only to individual transactions not to other bank account transactions. 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 transactions from a large volume dataset is difficult, so we propose case reduction methods to reduce the input dataset and then find pair of transactions with another bank account with common attributes and behavior.

KEYWORDS: Structural similarity, machine learning.

I. INTRODUCTION

Credit card fraud scrubbed as much as 5 of the world's GDP (Gross Domestic Product) every year. Combating credit card fraud using AI is to detect suspiciousactivities. 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, trans action records are checked to detect credit card fraud activity if the suspicious data is detected. Here we use Artificial Intelligence and Machine Learning Algorithm to detect Algorithms them suspicious activities and solve them by training the data of that activity. We are going to use supervised and unsupervised algorithm techniques.

II. THE RESEARCH METHOD

1.Financial Fraud Detection with Anomaly Feature Detection

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 example, credit card fraud is defined as the process of using trades to move money/goods with the intent of obscuring the true origin of funds.

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

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 instrument

3. Prevention of Credit Card Fraud Detection based on HSVM

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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004106|

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

III. METHODOGY

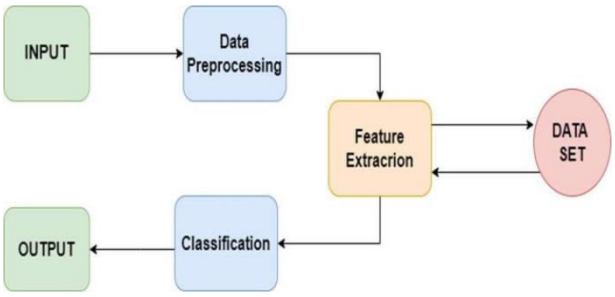

Fig.1. Block Diagram

At The Balance, we are dedicated to giving you unbiased, comprehensive credit card reviews. To do this, we collect data on hundreds of cards and score more than 55 features that affect your finances, such as interest rates, fees, and rewards.We score each attribute on a scale of 0 to 5. We then weight these scores to determine the star ratings you see on our review pages. The following elements are generally ordered from highest to lowest in how heavily they factor into our overall evaluation of credit cards.

Clearly, credit card fraud is an act of criminal dishonesty. This article has reviewed recent findings in the credit card field. This paper has identified the fraud, and dis- cussed measures to detect them. Such measures have included clustering techniques algorithms. From an ethical perspective, it can be argued that banks and credit card companies should attempt to detect all fraudulent cases. Yet, the unprofessional fraudster is unlikely to operate on the scale of the professional fraudster and so the costs to the bank of their detection may be uneconomic. The bank would then be faced with an ethical dilemma. Should they try to detect such fraudulent cases or should they act in shareholder interests and avoid uneconomic costs? As the next step in this research program, the focus will be upon the implementation of a 'suspicious' scorecard on a real data-set and its evaluation.

The main tasks will be to build scoring models to predict fraudulent behavior, taking into account the fields of behavior that relate to the different types of credit card fraud identified in this paper, and to evaluate the associated ethical implica- tions. The plan is to take one of the European countries, probably Germany, and then to extend the research to other EU countries.

Clustering techniques for behavioral fraud. The peer group analysis is a system that allows identifying accounts that are behaving differently from others at one moment in time whereas they were behaving the same previously. Those accounts are then flagged as suspicious. Fraud analysts have then to investigate those cases. The hypothesis of the peer group analysis is that if accounts behave the same for a certain period of time and then one account is behaving significantly differently, this account has to be notified. Breakpoint analysis uses a different approach.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004106|

IV. RELATED WORK

A. System Architecture

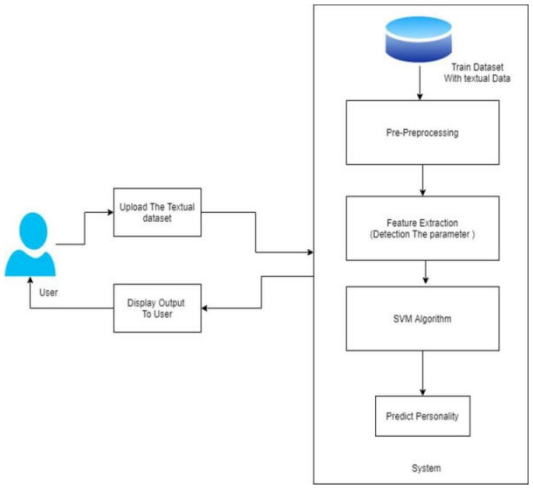

Fig.2. System Architecture

The system architecture includes the User and the System and there is one bridge between that two parameters i.e., Data. After uploading the textual data by the user, the system will train that dataset, after trained dataset that textual data will get preprocessed by the system and it will send to the Feature Extraction module and that module will detect the parameters from the Textual data and compare it with Dataset.

After that the SVM Algorithm will perform on that Textual Data, and that will predict the personality of the user and display the output to the User.

B. SVM Algorithm

SVM is a supervised machine learning algorithm that can be used to classify and predict data. Though we could also say regression problems, classification is the best fit. The goal of the SVM algorithm is to find a hyperplane in an N-dimensional space that categorizes data points clearly. The size of the hyperplane is determined by the number of features. The hyperplane is just a line if there are only two input features. When there are three input features, the hyperplane becomes a two dimensional plane. It becomes tough to imagine when the number of features exceeds three.

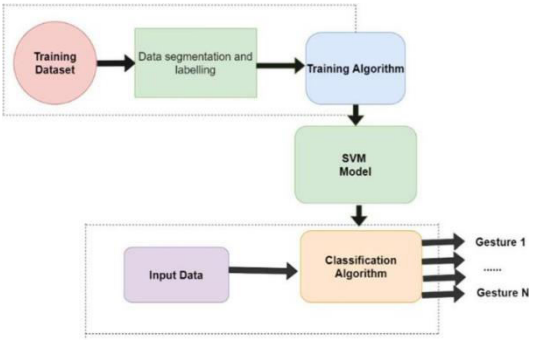

Fig. 3. SVM

V. FUTURE SCOPE

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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004106|

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.

VI. CONCLUSIONS

We use Kaggle online dataset for credit card transaction for anomaly detection, where the fraudulent transactions are considered as anomalies. Using this project we can detect the online fraud transaction.

REFERENCES

1. Ahmed Al Marouf, Md. Kamrul Hasan and Hasan Mahmud “Comparative Analysis of Feature Selection Algorithms for Computational Personality Prediction from Social Media” IEEE Transactions on Computational Social System
2. Aditi V. Kunte, Suja Panicar “Using textual data for personality prediction: A machine learning” 2019 4th International Conference on Information System and Computer Networks (ISCON) GLA University, Mathura, UP,
3. India. Nov 21-22,2019
4. Ange Tato, Roger Nkambou, Claude Frasson, “Predicting Emotions from Multimodal Users’ Data”, UMAP 18, Singapore, July 8-11, 2018.
5. Tuan Tran, Dong Nguyeny, Anh Nguyeny, and Erik Golenz, "Sentiment Analysis of Emoji-based Reactions on Marijuana Related Topical Posts on Facebook", IEEE International Conference on Communications (ICC), 2018.
6. Dany Azucar, Davide Marengo, Michele Settanni, “Predicting the Big 5 Personality traits from digital footprints on social media: A meta-analysis”, Personality and Individual Differences, Computers in Human Behavior, pp. 150-159, August 8, 2018.
7. Bayu Yudha Pratama, Riyanarto Sarno “Personality Classification Based on Twitter Text Using Naive Bayes, KNN and SVM”, 2015 International Conference on Data and Software Engineering.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details