



Credit Card Fraud Detection System

Shubham Jadhav, Siddhant Karale, Omkar Pawar, Sujit Pisal, Gajanan Arsalwad

Student, Student, Student, Student, Professor
Information Technology,
Trinity College of Engineering and Research Pune, India

Abstract: Today's society has a number of problems, but the biggest one is credit card fraud, which needs to be addressed. In order to make the source of cash untraceable, "credit card fraud is the process of cleaning dirty money." Due to the massive quantity of financial transactions that take place on a daily basis in the worldwide market, it might be difficult to identify credit card fraud. To identify suspicious activity, the (Anti-Credit Card Fraud Suite) has been introduced; however, it is only relevant to individual transactions and not to other bank account transactions. By identifying shared characteristics and behavior's with other bank account transactions using structural similarity, we offer a machine learning solution to address these difficulties.

Keywords – credit, credit card, fraud, SVM, system, authentication, live camera.

I. INTRODUCTION

At a time when the entire planet was under lockdown and travel was only permitted in the event of an absolute emergency, millions of people were introduced to the world of online shopping. The ease of online shopping allowed e-commerce platforms to set new sales records. It is not unexpected that at the same time, the prevalence of financial fraud on the internet surged. Online fraud involving credit and debit cards significantly increased by 225 percent during the COVID-19 epidemic in 2020 as compared to 2019. In 2020, there were 1194 occurrences of credit and debit card fraud, up from 367 in 2019, according to the NCRB research. Millions of people were introduced to the world of internet shopping during a time when the entire planet was on lockdown and travel was only permitted in extreme cases. The ease of online shopping helped e-commerce platforms to generate record sales. It is not unexpected that the rate of online financial fraud increased at the same period. There was a 225 percent rise in online fraud occurrences involving credit and debit cards during the COVID-19 epidemic in 2020 compared to 2019. According to the NCRB research, there were 1194 occurrences of credit and debit card theft in 2020, up from 367 in 2019.

II. LITERATURE SURVEY

Paper Name : Credit Card fraud Detection Using AI

Authors : Dongxu Huang, Dejun Mu, Libin Yang, Xiaoyan Cai

Description : Financial fraud activities, such as credit card fraud, have gradually grown in recent years. These activities lead to the loss of personal and/or commercial property. Worse, they jeopardise national security by diverting profits from fraud to terrorists [1][25]. Thus, accurately detecting and tracing financial fraud is both necessary and urgent. However, because of the intricate trade networks and transactions involved, detecting financial fraud is a difficult process. As an illustration, credit card fraud is described as the practise of moving money or products via exchanges while concealing the real source of the funds.

Paper Name : Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering Neural Network

Authors : Tanmay Kumar Behera, Suvasini Panigrahi

Description : The usage of credit cards has significantly expanded, which has resulted in a high number of fraud instances, as a result of the quick development of e-commerce and online banking. In this study, we provide a unique method for identifying credit card fraud that involves three stages of fraud detection. The first user authentication and card information verification are done in the first step. If the check is successfully cleared, the transaction moves on to the following stage, where a fuzzy cmeans clustering method is used to determine the typical credit card usage patterns of consumers based on their prior behaviour. The degree of divergence from the norm determines a suspicion score, which determines if the transaction is lawful, suspicious, or

fraudulent. Once a transaction is flagged as suspicious, a neural network-based learning process is used to ascertain if the behaviour in question was indeed fraud or only a rare error made by a genuine user. Numerous experiments with stochastic models demonstrate that the effective detection of fraudulent activities while reducing the creation of false alarms is made possible by combining the clustering approach with learning.

Paper Name : Credit card fraud detection based on whale algorithm optimizHG BP neural network

Authors : Dongxu Huang, Dejun Mu, Libin Yang, Xiaoyan Cai

Description : In order to address the issues of slow convergence rate, easy to fall into local optimum, network flaws, and poor system stability resulting from BP neural network, this research offers a credit card fraud detection technology based on whale algorithm optimised BP neural network. We first utilise the whale swarm optimization algorithm (WOA) to acquire an ideal beginning value, and then we use the BP network method to correct the incorrect value in order to obtain the ideal value.

Paper Name : Credit Card Fraud Detection Using RUS and MRN Algorithm • **Authors :** Anusorn Charleonnann

Description : Currently, organizations and other stakeholders are focusing on credit card expenditure services in general because it is a quick and efficient way to pay for items and services. Thus, this study focuses on detecting credit card payment fraud using the RUSMRN machine learning technique. The suggested method makes use of three fundamental classifiers: MLP, NB, and Naive Bayes algorithms. In addition, it can analyze the correctness to work with the unbalance datasets. Additionally, it can evaluate the correctness of working with unbalanced datasets. As a result, this study focuses on the information of Taiwan's credit card firm in order to collect data on behavior of customers in credit card payment. Following that, it has brought the information to build a prediction for correctness whether it has payment hazards. In accordance with the results, the suggested methodology has the best classification performance in terms of accuracy and sensitivity.

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

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

III. FUNCTIONAL REQUIREMENT

System Feature:

1. **Database:** Personal information about the sender and receiver, as well as account information about the sender and receiver, are stored in a database..
2. **User:** User registers on the system for transactions and has account details for their own and receiver accounts. The user conducts the money transaction, and the system records the sender and receiver's information.
3. **System:** The dataset is being pre-processed. Machine learning can also be used to train the machine. and discover account information associated with credit card fraud.

IV. EXTERNAL INTERFACE REQUIREMENT AND FIGURES

User Interface

The system will give a graphical user interface to the user; there will be no command line interface for the product's functions. Population and Sample

Hardware Interface

Because the application must be operated over the Internet, every hardware required to connect to the Internet will be a hardware interface for the system. As for e.g. WAN – LAN, Ethernet Cross-Cable

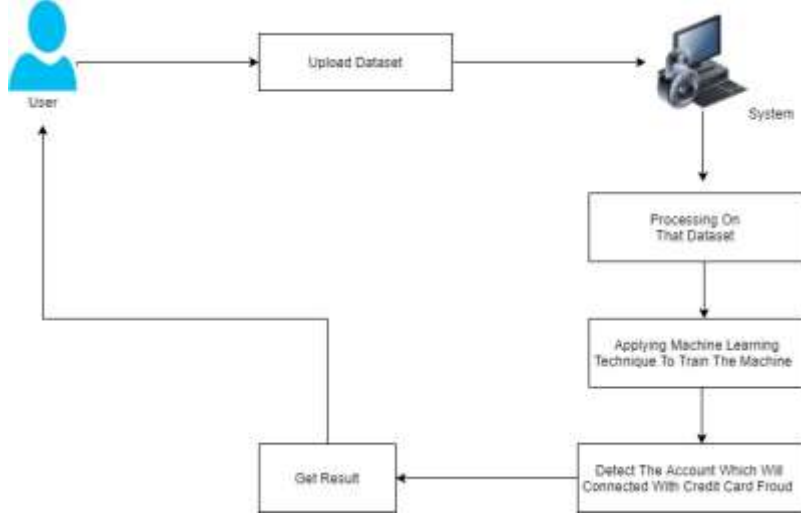
Software Interface

- **PYTHON :** Python is a scripting language that is high-level, interpreted, interactive, and object-oriented. Python is intended to be extremely readable. It commonly uses English terms rather than punctuation, and it includes fewer features formations than other languages. • Python can be interpreted The interpreter processes Python at runtime. It is not necessary to compile your software before running it. This is comparable to PERL and PHP. • Python is an interactive language. To write your programmers, you can actually sit at a Python prompt and interact directly with the interpreter.
- Python is Object-Oriented Python supports Object-Oriented style or technique of programming that encapsulates code within objects.

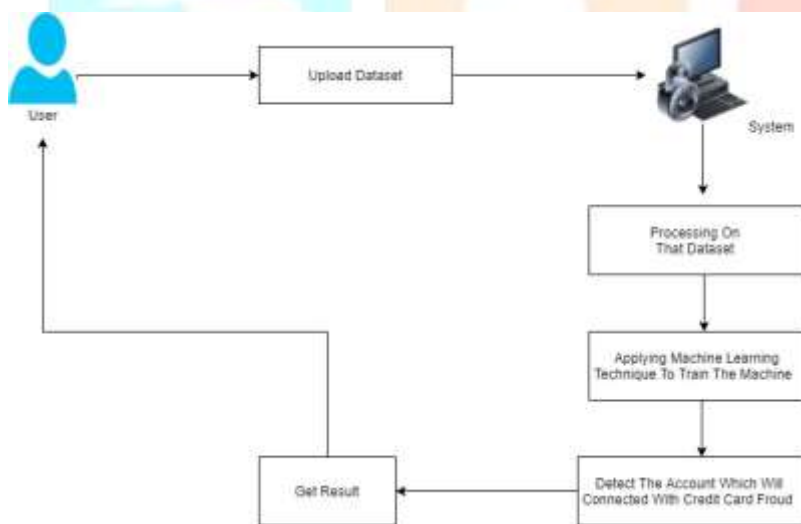
- Python is a language for beginners. Python is an excellent language for beginning programmers, as it allows for the creation of a wide range of applications, from simple text processing to web browsers to games.
- **Pycharm** : Pycharm are usually developed in the python language.

Figures

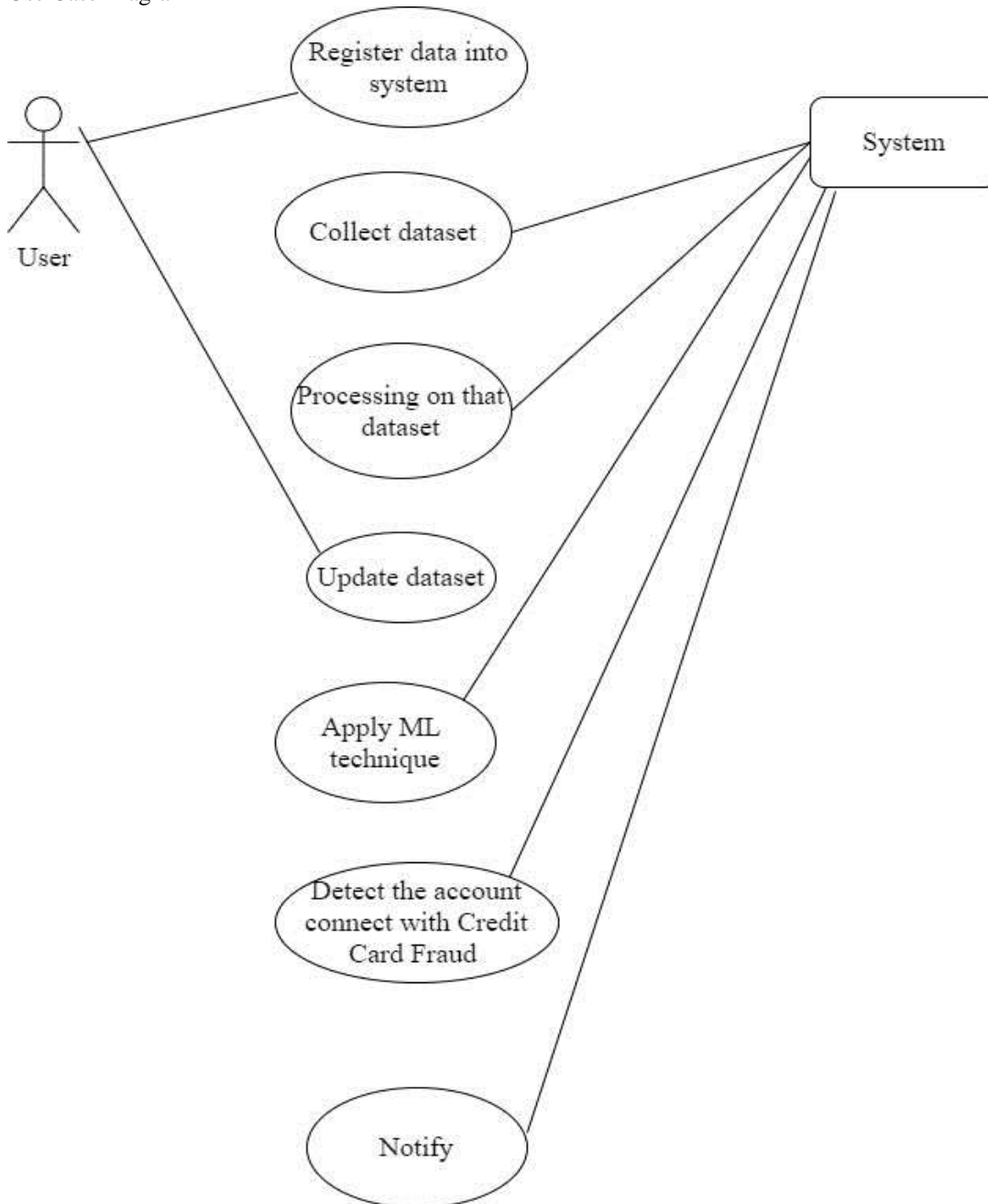
System Architecture



DFD Level 1



Use Case Diagram



V. CONCLUSION AND FUTURE WORK

The suggested machine learning approach seeks to identify possible money-laundering groups among a huge number of financial transactions. Case reduction approaches such as matching transaction detection and balance score filter are used to restrict the list of prospective ML accounts in order to increase the framework's efficiency. Next, we may identify and group possible credit card fraud accounts using structural similarity. Our preliminary experimental findings demonstrate that we can detect ML accounts with a high degree of accuracy.

REFERENCES

- 1 [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 [2] Fatf-gafi.org, 'credit card fraud - Financial Action Task Force (FATF)', 2014. [Online]. Available: <http://www.fatfgafi.org/faq/moneylaundering/>. [Accessed: 22Dec- 2015].
- 3 [3] Neo4j Graph Database, 'Neo4j, the World's Leading Graph Database', 2014. [Online]. Available: <http://neo4j.com/>. [Accessed: 22- Dec- 2015].
- 4 [4] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten. Improving credit card fraud detection with calibrated probabilities. In SDM, 2014.
- 5 [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.