International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Fraud Detection System using SVM

Ms. Madhuri B. Thorat[1], Purva D. Netke[2]

1. Assistant Professor, Department of Information Technology, AISSMS's Institute of Information Technology, Pune-411001, INDIA
2.TE. (Information Technology), AISSMS's Institute of Information Technology, Pune-411001, INDIA

A B S T R A C T

As the online transaction is becoming more popular the use of credit/debit cards are also increasing. the types of online transaction fraud associated with this increase in the use of online transactions. Fraud is one of the important ethical issues in electronic payment Gateway. This fraud detection system has the ability to control and obstruct the transaction performed by the attacker from genuine users' credit card details. these fraudulent transactions need to be found. Frauds can be detected through various approaches. Machine Learning consists of many algorithms which will be employed in fraud detection like Support Vector Machine (SVM

Keywords: credit card frauds, fraud detection, fraudulent, Support Vector Machine (SVM), One Time Password (OTP), Security questions.

1. Introduction to Fraud Detection System using SVM.

The paper presents the increase the bank fraud in online transactions with the help of a Support Vector Machine (SVM). Support vector Machine (SVM) is a Supervised Machine Learning Algorithm that is used for classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning This paper uses SVM to estimate the data for fraud detection.

The aim of the SVM algorithm is to create the best line or decision boundary that can isolate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future.

1.1 Motivation

- Online fraud is one of the major problems in the modern world.
- Fraud Detection is a collection of processes and techniques designed to recognize, monitor, and avert fraud.
- In the online, business world fraud, scams and corrupt agents are damaging in a number of ways. Companies have to concentrate in place to ensure that fraud is detected and stopped.

1.2 Aim and Objective

Aim

The aim of the project is to detect the Online transaction fraud detection system by using a Support Vector Machine (SVM).

Objectives

- To Develop a system which can efficiently detect online transaction frauds.
- To Reduce Online Transaction frauds by using SVM.
- To Monitor the Transactions carefully.

2. Literature Review

The paper presents the increase the bank fraud in online transactions with the help of a Support Vector Machine (SVM). In noisy and complex domains, classification problems can be solved by using SVM. The behavior-based classification method using SVM is used in this project. within the type of threshold for separating the data, the SVM gains adaptability. These qualities make SVM carry out the problem of classification in this complex domain

and also generate an honest result. In SVM, the minimal issue and curse of dimensionality occasionally arise. SVM comes from the theory of mathematical learning.[1]

In this paper, the authors analyze the different types of frauds during to which the bank data processing tools are exposed during these definitions, enabling their early detection data already collected by the bank. Support vector machines with spark (SVM-S) is used by the author to create models that represent normal and abnormal customer activity and then use it to calculate the validity of recent transactions.

Also, the rest of the paper is organized as follows: the kind of fraud detection will be first presented as well as indices used to discover it, then we discuss the types of big data solutions that can be used as well as discuss the use of support vector machine in spart to meet the needs of detection of fraud then, next section presents the validation of proposed solutions by testing them on bank database.[2]

The history of past transactions of users is maintained in the payment engine's database. Analysis of real data at the payment engine's database and data obtained from users is done by an algorithm described in this Paper for fraud detection and possibly fraudulent is detected in real-time.

This paper uses outlier analysis for detecting fraud in which the behavioral pattern of the customers along with their social and financial status is considered. Various rules for fraud detection are examined which if not followed can lead to a suspicious transaction. The history of past transactions of users is maintained in the payment engine's database. Analysis of real data at the payment engine's database and data obtained from users is done by the algorithm described in this paper for fraud detection and a possible fraudulent transaction is detected in real-time.[3]

Fraud is any malicious activity that aims to cause financial loss to the other party. Frauds caused by Credit Cards have cost consumers and banks billions of dollars globally. Even after numerous mechanisms to stop fraud, fraudsters are continuously trying to find new ways and tricks to commit fraud. Thus, in order to stop these frauds. we need a powerful fraud detection system that not only detects the fraud but also detects it before it takes place and in an accurate manner. We need to also make our systems learn from past committed frauds and make them capable of adapting to future new methods of fraud. In this paper, we have introduced the concept of fraud related to credit cards and their various types. The paper explained various techniques available for a fraud detection system such as Support Vector Machine (SVM), Artificial Neural Networks (ANN), Bayesian Networks, K-Nearest Neighbor (KNN), Hidden Markov Models, Fuzzy Logic Based Systems, and Decision Trees. An extensive review is done of the existing and proposed models for credit card fraud detection and has done a comparative study of these techniques on the basis of quantitative measurements such as accuracy, detection rate, and false alarm rate. The conclusion of our study explains the drawbacks of existing models and provides a better solution in order to overcome them.[4]

One of the noteworthy difficulties in the classification of portable data is handling data with class imbalance. Unbalanced data possess the characteristics of having a lot of samples of one class than the other. It, thusly, results in the biased accuracy of a classifier in favor of a majority class. Streaming data may have inherent imbalance resulting from the nature of dataspace or extrinsic imbalance due to its nonstationary environment. In streaming data, timely varying class priors may lead to a shift in the imbalance ratio. The researchers have contemplated ensemble learning, online learning, the issue of class imbalance, and cost-sensitive algorithms autonomously.[5]

3. Algorithm

Support Vector Machine (SVM)

SVM is a Supervised machine learning algorithm that can be used for both classifications and regression problems. It's often used in classification issues, however. In this algorithm,

we plot each data item in an "N" dimensional space to some degree, with the price of each function being the price of a chosen coordinate showing the hyper-plane differentiating the 2 groups from the hyper-plane. During this algorithm, we take the shopping data item of each consumer to some degree in an 'n-dimensional space (where n is the number of features you have) with the price of each function being the price of a chosen coordinate.

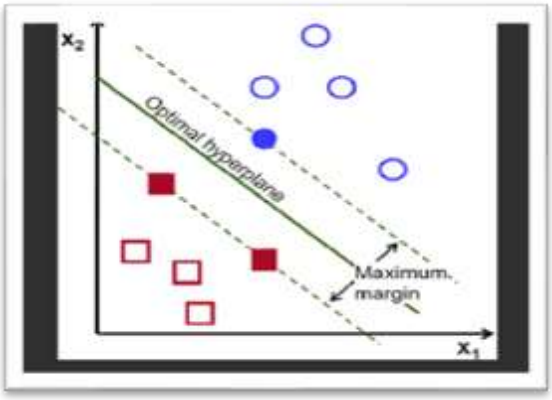

Figure3.1: Graph of SVM

4. Experimental Methodology

In methodology, This paper contains total of five steps, firstly, If the user is a new user then the system will ask for registration. The user will register herself or himself with the help of a name. city, mobile number, and email Then the system will ask for login details such as username and password.

To enroll for the security questions verification, the login user selects several questions and supplies confidential answers that only the user knows.

One Time Passwords (OTP) also play an important role in this whole system. OTP can be used once and then expires. The user needs to prove his or her identity with the help of OTP. To Predict or classify patterns SVM Classifies into fraudulent or non-fraudulent

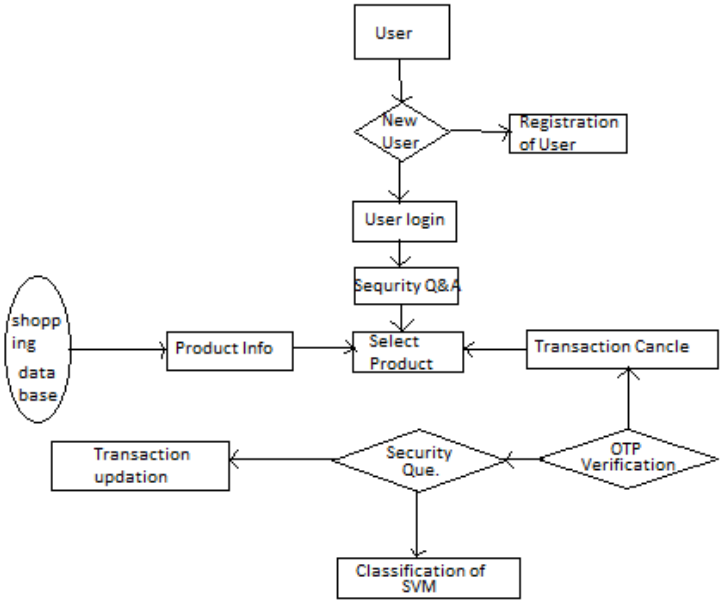

Figure 4.1: Flowchart of proposed Methodology [1]

5. Performance Evaluation

It Concludes that each system faces its own problems while dealing with dataset description. The proposed system come with the SVM model of real databases system come with the SVM model of real database which helps in acquiring a maximum of 99.9% accuracy.

The Artificial Neural Network (ANN) comes with 97.32% accuracy while Hidden Markov Model(HMM) has 94.7% accuracy. ANN has a high processing time and excessive training for large neural networks, difficult to set up and run. Also, Bayesian Networks need excessive training and have 96.52% accuracy.

6. Conclusion

This project presents a classification of online credit / open-ended credit the challenges faced by cardholders also because of the card issuer, the variety of fraud implemented by the persons who commit the fraud. The behavior-based classification method using SVM is used in this project. Effective performance in fraud detection is often given using SVM. SVM typically provides a creative solution. Within the type of threshold for separating the data, the SVM gains versatility. These qualities make the SVM carry out the problem of classification in the complex domain and also generate an honest result. The suggested approach offers greater identification precision and is also scalable for managing larger quantities of transactions.[1]

References

[1]. Mettildha Mary, M. Priyadharsini, Dr. Karuppasamy."Online Transaction Fraud Detection System" In: 2021 International conference

[2] Bank Fraud Detection Using Support Vector Machine 1.Nana Kwame Gyamfi Computer Science Dept. Kumasi Technical University Kumasi, Ghana 2.Dr Jamal-Deen Abdulai Computer Dept. University of Ghana

[3]Fraud Detection in Online Credit Card Payment Aishwarya Kaneri1, Anugrah S2, Isha Bharti3, Samruddhi Jadhav4, Mitali Kadu5 1,3,4,5 Cummins College of Engineering, Pune University 2Army Institute of Technology, Pune University

[4]A comparative analysis of various credit card fraud detection techniques January 2019 Authors: Y. Jain N. Tiwari S. Dubey Sarika Jain National Institute of Technology.

[5] Parallel and incremental credit card fraud detection model to handle concept drift and data imbalance Akila Somasundaram & Srinivasulu Reddy

Neural Computing and Applications volume 31, pages3–14 (2019).

[6] A.S.Wheeler R, " Multiple algorithms for fraud detection. Knowledge-Based Systems," no. S0950-7051(00)00050-2, 2000

[7] E. Aji M. Mubarek, "Multilayer perceptron neural network technique for fraud detection," in International Conference on Computer Science and Engineering(UBMK), 2017.

[8] E. D. Yusuf Sahin, "detecting credit card fraud by ann and logistic regression," 2011.

[9] S. k. A. K. M. Ayushi agarwal, "Credit card fraud detection: A case study," in IEEE, New Delhi, India, 2015.

[10]]. R. M. jamail esmaily, "Intrusion detection system based on multilayer perceptron neural networks and decision tree," in International conference on Information and Knowledge Technology, 2015.