As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(04):106-109, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0804019
Available online at: http://www.ijmtst.com/vol8issue04.html

Credit Card Fraud Detection using Hidden Markov Model

Sharayu Pradeep Gulhane | Nitin N. Mandaogade

Department of Embeded System and VLSI Design, G.H. Raisoni University,Amravati.
*Corresponding Author Email ID: sharayugulhane59@gmail.com

To Cite this Article
Sharayu Pradeep Gulhane and Nitin N. Mandaogade. Credit Card Fraud Detection using Hidden Markov Model. International Journal for Modern Trends in Science and Technology 2022, 8(04), pp. 106-109. https://doi.org/10.46501/IJMTST0804019

Article Info
Received: 03 March 2022; Accepted: 4 April 2022; Published: 07 April 2022.

ABSTRACT

It is very important for credit card companies to detect the transactions that are not from a genuine buyer. Also to avoid transactions that are carried out by unauthorised person who is not the owner of the credit card or who is carrying out the transaction without the knowledge of the owner of the card. These problems can be worked out with data science and machine learning technology. It is very important to get a control over such frauds and it cannot be skipped. This project aims to use modelling data set along with machine learning for credit fraud detection. In order to find the credit card frauds, we need to analyse all the past transaction data and patters of the card user. And also need the data of transactions that appear to be fraudulent. This model will therefore be used to determine if an ongoing transaction is fraudulent or not. With this implementation, our goal is to get 100% fake jobs while minimizing the false alarms for genuine transactions. Credit Card Fraud Detection is a common sample of segmentation. In this process, we focused on analyzing data sets and using multiple algorithms detecting ambiguities such as Local Outlier Factor and the Isolation jungle algorithm in PCA that converted Credit Card Making data.

KEYWORDS: Credit Card Fraud, Machine Learning, Data Science, Forest separation algorithum, external feature, automated fraud detection.

1. INTRODUCTION

Growing credit card fraud is nothing but an unauthorized transaction carried out by an unauthorized person without the knowledge of card owner. The necessary precautionary measures can be taken to prevent this abuse and the behavior of those fraudulent activities can be investigated to reduce and prevent similar incidents in the future. Use of card for personal reasons while the owner and issuing authorities of the card are unaware of the fact that the card is in use is considered as a fraud transaction. Fraud detection involves monitoring the activities of the majority of users in order to measure, detect or avoid undesirable behavior, including fraud, interference, and error. This is a very relevant problem that needs the attention of communities such as machine learning and data science where the solution to this problem can be automated. This problem is especially challenging in view of the learning environment, as it is characterized by a variety of factors, including class inequality. Not all transactions are fraud and very less amount of transaction are actually fraud, therefore a real buyer should not face a false alarm experience. Also, practical patterns often change their mathematical features over time.

These are not the only challenges in using the real-world fraud detection system. However, in real-world examples, most payment applications are quickly scanned with automated tools that determine which payments should be approved. Machine learning algorithms are used to analyze all authorized transactions and to report suspicious activity. These reports are investigated by experts who contact cardholders to verify that the activity was genuine. Investigators provide a response to an automated system used to train and update the algorithm to ultimately improve the performance of fraud detection over time. Fraud detection methods are constantly being developed to prevent criminals from adapting to their fraudulent tactics.

These crimes are classified as:

- Credit Card Fraud: Online and Offline
- Card theft
- Account Loss
- Device Login
- Application Fraud
- Fake Card
- Communication Fraud

2.RELATED WORK

I. Online fraud acts as an illegal scam or a crime aimed at making money or personal gain. It is a deliberate act contrary to the law, the law or the policy for the purpose of obtaining unauthorized financial gain. precisely the counterfeit function in the simulation test of a credit card transaction set of a particular commercial bank. Outlier mining is a data mining industry that is primarily used in the financial and online sectors. It is responsible for obtaining items extracted from the main system i.e. non-actual actions. They take the values of the customer behavior and based on the number of those attributes they calculated that distance between the specified value of that attribute and its predetermined value. Unusual techniques such as multimedia data mining / sophisticated network split algorithm can detect illegal events in real-time card-based data set, based on a network redesign algorithm that allows to create single event diversion presentations from a reference group for online online transactions. . There have also been attempts to improve from a completely new feature. Efforts have been made to improve warning-response interaction in the event of fraudulent activity. In the event of a fraudulent activity, the authorized system will be notified and a response will be sent to deny further work.

II. Ghosh and Reilly [5] have proposed a neural network approach to detect credit card fraud. They built a recovery system, trained with a large sample of credit card account operations. These samples contain an example of fraudulent cases due to lost cards or stolen cards.

III. Application fraud, stolen card details, fraudulent fraud etc. They check the data set for all credit card transactions for the next time. Bayesia networks are also one way to detect fraud, and they are used to detect fraud in the credit card industry [6]. These methods give better results but have a longer cycle time to detect fraud. However, time delays are one of the major disadvantages of this approach, especially when compared to neural networks.

IV. Another algorithm proposed by Bentley [7] is based on the genetic system. Genetic algorithm is used to establish logical rules that can divide credit card transactions into suspicious and non-suspicious categories. Basically, this method follows a points-out process in which the overdue payment overlooked the previous three-month payment. If it is larger than the previous three months, it will be considered suspicious or even non-suspicious.

3. METHODOLOGY

Markov Model Hidden is probably the simplest and most convenient model that can be used to create a sequential data model, i.e. data samples are dependent on one another. HMM is a randomly embedded process with two different levels, one hidden and the other open to all. The Hidden Markov Model is a set of limited circuits, each of which is associated with the distribution of opportunities. Transitions between regions are governed by a set of opportunities called transition probabilities. In some cases the effect or perception can be made, depending on the a situation that is visible to the outside viewer and therefore the regions are "hidden" on the outside; hence the name Hidden Markov Model.

A HMM has a finite set of states which is governed by a set of transition probabilities. In a particular state, an outcome or observation can be generated according to an associated probability distribution. It is only the outcome and not the state that is visible to a next observer.

In order to define an HMM completely, following elements are needed.

- The number of states of the model, *N*. We denote the set of states $S = \{S_1; S_2; S3; \ldots S_N\}$, where i =1; 2; . . .; N, is a number of state and S_i, is an individual state. The state at time instant t is denoted by q_t.
- The number of observation symbols in the alphabet, *M*. If the observations are continuous then *M* is infinite. We denote the set of symbols $V = \{V_1; V_2; \ldots V_M\}$ where V_i, is an individual symbol for a finite value of M.

$$\Lambda = \{a_{ij}\}$$

- A set of state transition probabilities.

$$a_{ij} = P\{q_{t+1} = S_j \mid q_t = S_i\}, 1 \le i, j \le N,$$

where q_t denotes the current state,

Transition probabilities should satisfy the normal stochastic constraints,

$$a_{ij} \ge 0, 1 \le i, j \le N$$

And

$$\sum_{j=1}^{N} a_{ij} = 1, \ 1 \le i \le N,$$

- The observation symbol probability matrix B,

$$B = \{b_j(k)\}$$

A probability distribution in each of the states,

$$b_j(k) = P\{a_t = V_k \mid q_t = S_j\}, 1 \le j \le N, 1 \le k \le M$$

Fig. 1: Catagorization of HMM.

HMM has been used successfully in many applications such as speech recognition, robots, bio-informatics, data mining etc.

Fraud Detection System runs at the bank where credit card was issued. For every incoming transaction FDS runs verification. FDS receives the card details and the amount of purchase to verify whether the transaction is genuine or not. The types of goods purchased in that transaction are not known to the FDS. It tries to find any odd factor in the transaction based on the spending profile, of the cardholder, shipping address, and billing address etc. If the FDS confirms the transaction to be fraudulent, it raises an alarm, and the issuing bank declines the transaction. The concerned cardholder may then be contacted and alerted about the possibility that the card is compromised.

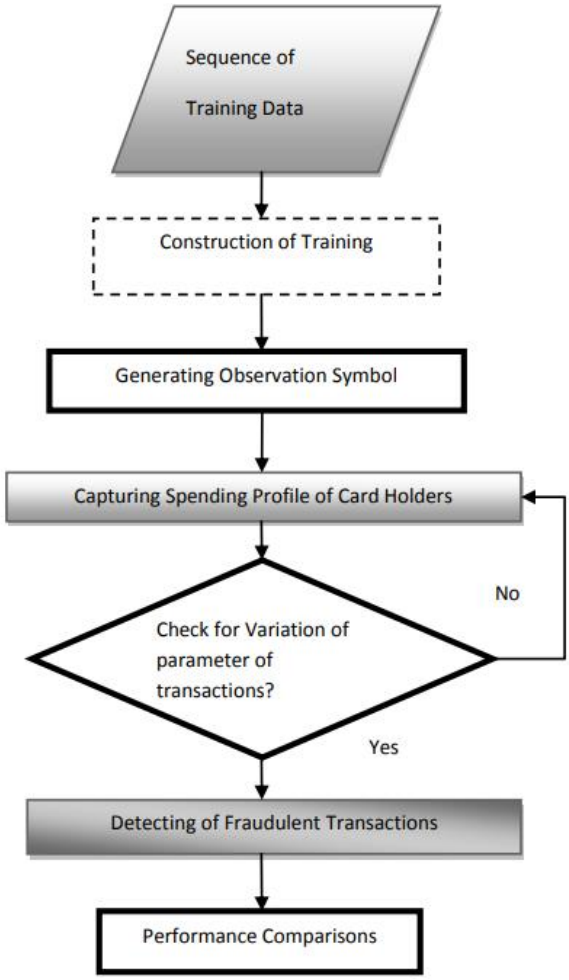

Fig . 2 : System flow diagram for incoming transaction.

4. FUTURE SCOPE AND CONCLUSION

Credit card has become a new trend and so the fraud happening has also increased. Therefore we need a firm and robust mechanism in order to detect such scams without hurting the genuine customers. I am tring to implement such system with minimal false alarms from my proposed project.

In this paper, we have discussed how the Hidden Markov Model will be helpful in detecting fraudulent online sales with a credit card. The proposed Fraud Detection System is also capable of measuring large amounts of processed data processing. The HMM-based credit card fraud system does not have a complex process to perform fraud testing as an existing system. The proposed fraud detection system provides a real and immediate effect than the existing system. The Hidden Markov Model makes detection processing much easier and tries to remove complexity.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] "Credit Card Fraud Detection Based on Transaction Behavior -by John Richard D. Kho, Larry A. Vea" published by Proc. of the 2019 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8 2017

[2] CLIFTON PHUA1, VINCENT LEE1, KATE SMITH1 & ROSS GAYLER2 " A Comprehensive Survey of Data Mining-based Fraud Detection Research" published by School of Business Systems, Faculty of Information Technology, Monash University, Wellington Road, Clayton, Victoria 3800, Australia

[3] "Survey Paper on Credit Card Fraud Detection by Suman" , Research Scholar, GJUS&T Hisar HCE, Sonepat published by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 3, March 2014

[4] "Research on Credit Card Fraud Detection Model Based on Distance Sum – by Wen-Fang YU and Na Wang" published by 2009 International Joint Conference on Artificial Intelligence

[5] "Credit Card Fraud Detection through Parenclitic Network Analysis-By Massimiliano Zanin, Miguel Romance, Regino Criado, and SantiagoMoral" published by Hindawi Complexity Volume 2018, Article ID 5764370, 9 pages

[6] "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy" published by IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, VOL. 29, NO. 8, AUGUST 2018

[7] "Credit Card Fraud Detection-by Ishu Trivedi, Monika, Mrigya, Mridushi" published by International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016