International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 02, 2020
ISSN: 1475-7192

Detection of credit card fraud using Data Mining technique

[1]Neha Bagoria ,[2]Dr. Vishal Kumar Goar

Abstract: *The credit card is an easy and efficient way of shopping. Credit cards can be used physically and online. The number of credit card holders is increasing around the globe, in proportion hackers' opportunities are also getting an increase. In the case of fraud transactions, the risk of credit cards has also been increasing. So, It has become mandatory to find a solution to the credit card information security system 's fraud transaction problems, as well as to find out how to detect fraudulent credit card transactions. The main purpose of this paper is to identify the type of fraud and to review alternative techniques used in fraudulent behavior. Here, Hidden Markov Model (HMM) is one of the common methods used for detecting or identifying the fraud for any credit card that allows the purchase. HMM is one of the Data Mining techniques. Several other data mining methods are Machine Learning, Artificial Intelligence, Neural Network, Genetic Engineering, Data Mining, etc. to detect the fraud.*

Keywords: *Data Mining, Credit Card, Detection Tool, Fraud, Hidden Markov Method,*

I. INTRODUCTION

Detection of credit card fraud in the context of e-payments is nowadays an old but hottest subject. The fraud should be detected by a good fraud detection system, should be identified as soon as possible. For online transactions (online shopping or e payment), the credit card is the common and simple way of paying. Sadly, credit card abuse has also become an important revenue stream for offenders. In this paper, we explore one of the data mining techniques used for credit card detection and the use of data mining to detect intrusion fraud, as well as. The main challenges associated with fraud detection in credit cards are in Real-world fraud data or fraud transactions.

In 2007-2008, Nielsen organizes a study where 28% population of the world has been using the internet [1]. According to the Global Nelson Consumer Report, 83% of people to make payment for online shopping has used the internet, these shopping rate increased by 40% from 2005 to 2008. The most common way of e-payment is the Credit Card. A total transaction of 60 percent has been completed[2]. As the number of users of credit cards increases, the chances of fraud offenders also increase, attackers, steal credit card information, and then fraud also increases. Many different techniques are suggested for detecting credit card fraud. Several data mining techniques like the Hidden Markov process, neural network, and artificial intelligence, etc are provided for the performance of the fraud detection systems.

[1] *Shri Jagdishprasad Jhabarmal Tibrewal University,Jhunjhunu(Rajasthan) nehabagoria06@gmail.com*

[2] *Govt. Engineering College,Bikaner(Rajasthan.) , dr.vishalgoar@gmail.com*

Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020

II. LITERATURE REVIEW

HMM usually separates and divides the difficult issue into many different parts and solves all sub-problems so it's easy to handle. [9] Download: [9]. The researcher proposed the detection of credit card fraud using a Hidden Markov Model. HMM-built detection system simplifies the huge amount of data[7]

Using the Secret Markov Model to detect credit card fraud during fraud transactions[9] in this research paper.

This paper Data mining system holding all related transactions and information and using statistical data methods to identify fraud. Based on the Hidden Markov Model, this system provides a medium to a variety of external l databases[10].

According to this paper, All operations are performed sequentially by using HMM in credit card transactions, detect fraud[11].

This paper detecting credit card fraud is very beneficial for credit card companies and their customers (credit card customers) both. The business must acknowledge the transaction 's financial expense as it does not prevent fraudulent transactions from being cleared. The interest rate costs are higher, and their charges are lower.[12].

III. HIDDEN MARKOV MODEL

Hidden Markov Model (HMM) is a perfect and best solution to the issue of credit card fraud detection. Hidden Markov Model (HMM)- based on the FDS credit card, where it does not require signatures from a scammer. And easily classify the deceptions using behavior sequences of a cardholder. Here, we use Hidden Markov Model (HMM) for all sequence transaction operations. And demonstrate how this can be used in the transaction to identify frauds.

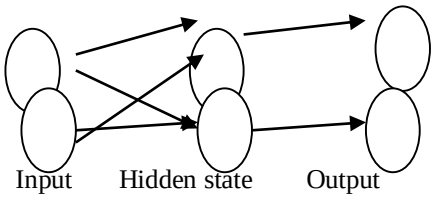
To figure out the secret Markov model of fraud translations, using sequential data with simple data dynamics is very useful, so HMM is the easiest and simplest method.

HMM lowers the maximum false positive transactions, so that's the most significant benefit. [3]. [12].

Hidden Markov Model works according to the user's spending habits. HMM, therefore, categorizes users into three categories: low, medium, and high. Markov model (HMM) helps us to identify both observed occurrences and hidden occurrences.

If the Hmm is not accepting the transaction that means the transaction is fraudulent. If the transaction is fraudulent, then it raises an alarm and declined the transaction by bank.

HMM has a finite set of the state where each state produces an output with a probability distribution method. The final out is only visible to the user, not the process. To identify the fraud transaction made by a credit card, HMM use the cluster set which helps to identify the card holder's profile. Data in HMM is stored in the form of clusters



Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020

Figure 1. Representation of HMM in "Credit Card Transaction"

The Hidden state is hidden for the external users, Only Input and Output states are visible [4].

4 Detection of Credit Card fraud using HMM:

Here we present how fraud can be identified using a Hidden Markov Model. FDS verifies every bank-issued transaction. This program gets card information and verifies whether the transaction is real or not[5]. In that, we can HMM be used to detect credit card fraud.

HMM is:

- N no. of states, and S states.

Where 1,2,3…..N;

These are individual states.

Time denoted by T

- M define number of Input/ Output states

V is Input/ Output

V=Vi;

i= 1,2,3,…M;

In the case of pre-approved and authorized transactions, it doesn't require transmitting the data to the system who are known by use.

IV. METHODOLOGY FOR IMPLEMENTATION

Simplest dynamic Bayesian network represents the HMM. We purchase X values into N price ranges A1, A2 . . . AM, form the issuing by the bank. The original price value is based on the incidental charges. These methods find out the price value of different cardholders by using the clustering algorithm. It uses symbol Ak for clustering algorithm where k = 1, 2. . . . M, and price value (k) and range (M) which can be represented observations on k, M.

Here, we consider three types of prices- L, M, H. Low, Medium, High. Here, V ={ l,m,h} where v is the observation symbol making M = 3. For example, let l = (0,$100], m = ($100; $500], and h=($500] ; credit card limit]. If a card holder's transaction, performed by the user is $190, then the m[6] is the related observation symbol.

In the very early stage, the last 10 transactions, in that case, do not have data of model, the model asks to perform the validation steps continuously and confirm the basic information of cardholder while the transaction is in progress. This information could be related to the cardholder's secondary name, his date of birth, his spouse or mother's median name, communication email address or alternate contact numbers, etc. As such feeding of information is available, the HMM model learned the relative data of transaction for the next level of verification for in the transaction which is being made on cardholders profile [7].

By this calculation, HMM perform the statistic and probability calculation to decide that performed the transaction is real or not i.e. fraud. In case the handler believes that the transaction is fraudulent then the user needs

security details to be entered. For example, Card Holder's PAN no., specified security question with an answer or account number entered at the time of registration, this given information is fully related to a specified credit card. If the transaction is real without any fraudulence then it will allow the transaction to be completed directly. Otherwise, there would be the Security Information Form that has specific quirks. To complete the transaction the user must answer this security question correctly.

V. DESCRIPTION OF THE MODEL

All credit card details will be checked with the program database (Credit card 16 digit numbers and 3 digit CVV number, Expiry mm/yy, name of the cardholder, etc.) If the data given is entered correctly by the end-user, then ask in the next step about Personal Identification Number (PIN). If the Personal Identification Number (PIN) matches the real banking database, it checks the user's credit card account balance. Once this is validated the module will trigger the fraud exam. These verification steps are checked before loading the page for the initiation of payment.

Using the AI and data from many users, the system is trained for each cardholder and keeps an HMM. Some of the past transactions are performed dynamically for observation purposes. These transactions and their data are normally stored in the database of the bank which contains all the data, transaction attributes. Here the bank knowingly invests the amount the cardholder has previously paid on this work[6,8].

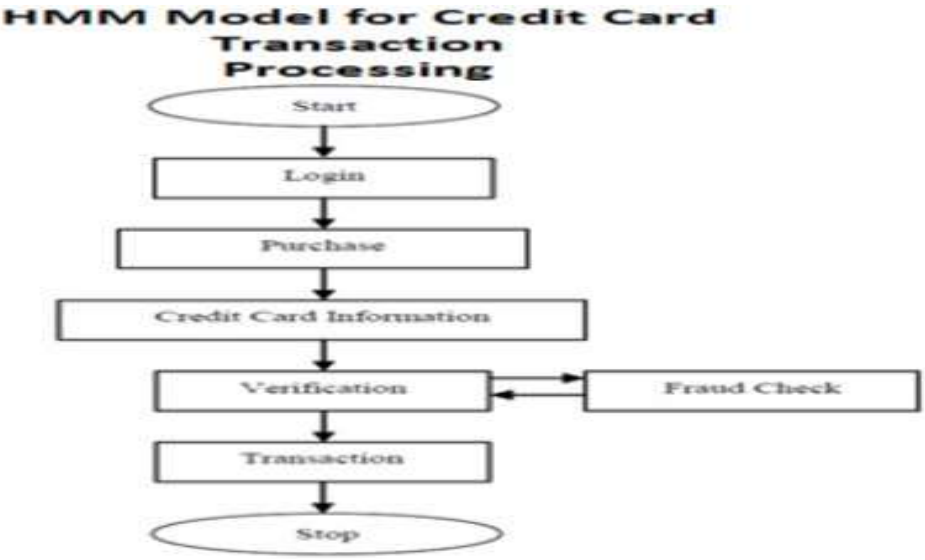


Figure 2. DFD for credit card fraud detection

VI. RESULTS AND DISCUSSION

Credit card bank does not provide real-time data or information about the transaction so it is very difficult to find out the fraud or emulate. In figure 1, we categorized all random data set according to their transition of purchase. With the help of an algorithm, we also calculate the spending profile percentage of each (L, M, and H)

that is based on a total number of fraud transactions. The last 10 transactions will be checked by the incoming transactions in fraud detection.

Table 1 - last 10 transactions of fraud detection

No. of transaction	Amount	No. of transaction	Amount
1	20	11	88
2	44	12	77
3	55	13	67
4	65	14	56
5	43	15	98
6	53	16	87
7	66	17	16
8	45	18	87
9	23	19	68
10	55	20	59

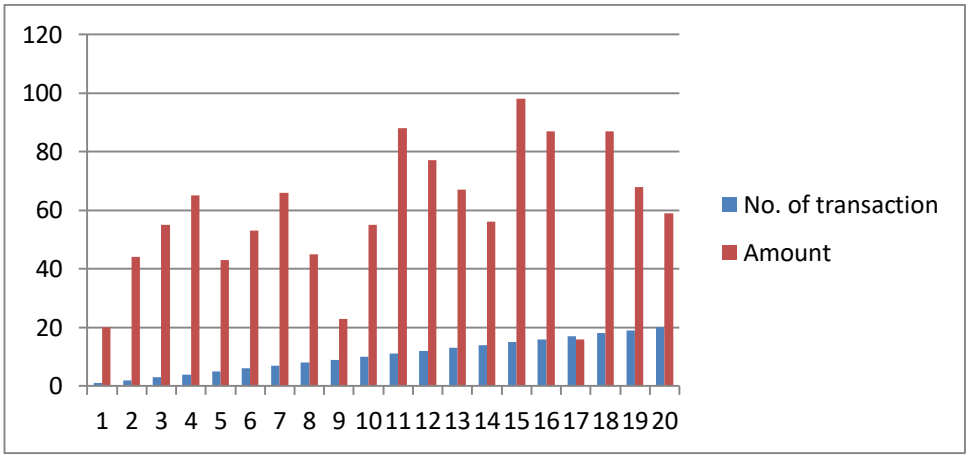


Figure 3 shown pattern of spending profile based on all transactions done[11].

VII. CONCLUSION

The main aim of this study we classify the best user model fraud cases. There are several methods today for identifying credit card fraud. If we applied this algorithm to the credit card fraud detection system, then we can easily predict the likelihood of fraud transactions after credit card transactions, and before anti-fraud series strategies can be adopted with great losses and reduced risks.

Here we discuss in this paper how these models will facilitate the use of credit cards to stop fraud. The Fraud Detection Program is capable of adjusting the large amounts of handling transactions. This "Hidden Markov Model" approach makes the detection operation very relaxed and helps to eliminate the complexity of the transaction.

REFERENCE

Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020

1. Internet usage world statistics. (2011).
2. A Global Nelson Consumer Report, Trends in online shopping (2008).
3. Thosani Jinal C., Bhadane, Chetashri, Avlani, Harsh M., Parekh, Zalak H. "Credit Card Fraud Detection Using Hidden Markov Model" ,International Journal of Scientific & Engineering Research, Volume 5, Issue 1 (2014)
4. R.RAJAMANI, M.RATHIKA "Credit Card Fraud Detection using Hidden Morkov Model and Neural Networks" in International Journal Of Advanced Networking and Applications (IJANA) (2015)
5. Arun K. Majumdar "Credit Card Fraud Detection Using Hidden Markov Model" International Journal of Thesis Projects and Dissertations (IJTPD**)** Vol. 1, Issue 1 ,(2013)
6. Shailesh s. Dhok, "Card Fraud Detection Using Hidden Markov Model" Model ISSN: 2231-2307, Volume-2, Issue-1, March 2012
7. Bilonikar Priya, Deokar Malvika, Puranik Shweta, Sonwane Nivedita, Prof.B.G.Dhake, "Survey on Credit Card Fraud Detection Using Hidden Markov Model" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, (2014)
8. Savitribai Phule(2007), "Global Consumer Attitude Towards On-Line Shopping"
9. Bhusari, V. and Patil, S. "Study of Hidden Markov Model in Credit Card Fraudulent Detection", International Journal of Computer Applications, Vol. 20, No.5 (2011)
10. Gaurav Mhatre et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2053-2055
11. Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar."Credit Card Fraud Detection using Hidden Markov Model" IEEE transactions on depedable and secure computing
12. Vimal Gupta, Surbhi Gupta "Credit Card Fraud Detection & Prevention – A Survey", International Journal for Innovative Research in Science & Technology Volume 4 (20170
13. K.RamaKalyani, D.UmaDevi, " Fraud Detection of Credit Card Payment System by Genetic Algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 7. ,(2012)
14. Bolton, R.J., Hand, D.J, "Statistical fraud detection: A review. Statistical Science " 235–255 (2002)
15. Alfian N, Tarjo T, Haryadi B. "The effect of anti fraud strategy on fraud preventionin banking industry[J]" 2017

Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020