International Journal of Engineering & Technology, 7 (2.32) (2018) 153-157

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Hidden Markov Model Based Fault Tolerance in Credit Card Transaction Security

N.Arunachalam[1], P.Prabavathy[2], S.Priyatharshini[3]

[1]*Assistant Professor, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry,India*
[2]*Student, Department of Information Technology, Sri Manakula Vinayagar Engineering College,Puducherry, India*
**Corresponding author E-mail:* narunachalam85@gmail.com

Abstract

Credit card fake detection has raised unique challenges due to the streaming, imbalanced, and non-stationary nature of the data that has been transacted. It had additionally included an active learning step, since the labeling (fake or genuine) use of a subset on transactions is obtained in near-real time through human investigators contacted the cardholders. In this paper, the Hidden Markov Model (HMM) algorithm has been used for sequence of Credit card operations for transaction processing and the fake can be detected by using the fake detection model during transaction processing. HMM, Fake detection model and image process had played an imperative role in the detection of credit card fake in online transactions. In fake detection, most challenging is a data problem, due to two major reasons – first, the profiles of cardholders are normal and fake lent behaviors changed constantly and secondly, credit card fake data sets are highly changed its position. Using fake detection (FD) algorithm the performance of detection in credit card transactions had highly affected by the sampling approach on dataset, selection of HMM, Fake detection model. Using fake detection (FD) algorithm an image technique had been used. A reliable augmentation of the target scarce population of fakes are important considering issues such as labeling cost; algorithm HMM, fake detection and outlines in the data streamed source. We have approached several scenarios which showed the feasibility of improving detection capabilities evaluated by means of receiver operating characteristic (ROC) curves and several key performance indicators (KPI) commonly used in financial business.

Keywords: *Comparative analysis, Credit card fake, Detector, Fake detection model, Hidden Markov Model And Image processing, Signal processing on graphs*

1. Introduction

Credit card purchasing in online spending split into two such as physical and virtual card. In a physical card, the user-holder grants his card physically to commerce for making an expense through online. An assailant has to give-away the card for transaction which makes fake. If the user-holder does not realize the card has been lost that can lead to a worth of economic loss to the credit card concern and another kind of spending, only some important data about a card is card number, expiration date, secure code is required to make the online expense. Such kinds of payments are usually done on the network or through the mobile phone. To require fraud in these types of spending, a fraudulent simply needs to know the details of user-holder. Most of the time, the genuine user-holder does not know aware of someone has robbed his card data. The only way to detect this kind of fraud is to analyze the spending patterns on every card and for inconsistency with respect to the usual spending outlines. Fraud detection is based on the analysis the user-holder of existing purchase data in a hopeful way to reduce the rate of successful credit card frauds transaction. Unconventionality from such outlines is an impending risk to the system on online spending [1].

In this paper, the Hidden Markov Model (HMM) algorithm is used for categorization of Credit card actions for transaction dispensation and the fraud is noticed by using the fraud noticed model during transaction dispensation. Economic fraud is an ever growing menace with far consequences in the economic industry. HMM, Fraud discovery model and image process had played an imperative role in the detection of credit card fraud in online transactions. In fraud detection, most interesting is a data problematic, due to two major motives – first, the profiles of user-holder is normal and fraudulent actions is changed constantly and secondly, credit card fraud data sets are greatly changes its place. The using fraud detection (FD) algorithm presentation of detection in credit card transactions is highly unnatural by the sampling approach on data set, chosen of HMM, Fraud detection.

A reliable growth of the target scarce population of frauds is significant considering issues such as labeling rate; algorithm HMM, fraud discovery; and regularly changing of outlines in the data running source. Fraud detection model is used to model the possibility and density of credit card user's past performance so that the possibility of current performance can be calculated to detect the past performance [3]. Finally, Bayesian nets are used to describe the statistics of a fraud and the statistics of dissimilar specific user. The main task is to explore dissimilar views of the same problem and see what can be learned from the submission of each dissimilar technique.

2. Related Works

In today situation when the fake transactions come through a discussion, fake on credit card makes to think too long. Nowadays

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

the high increase in fake transactions of the credit card has increasing in all places in a few years [4]. Fake detection of transactions are used to maintain the records of behavior of user data in order to find, detect, or avoid the unwanted behavior of the user's card holder [5]. Like credit card has become the most general mode to make payment for both online and offline payment of purchase for a transaction. Fake transaction detection in credit card was not a concern to capture the fake transaction problems, but it also captures some actions as soon as Possible. The use of card in credit transaction is widely used in today society within the world [6]. Fake on Credit provides millions of dollars on business and it gets increasing on each year. Fake transaction provides suitable cost to our economy on worldwide. New techniques are developed based on detection of fake, Processing of image, programming on Hidden Markov Model (HMM), Artificial Intelligence has been presented to detect fake on credit card transactions [7]. This gives the new fake transaction on credit card techniques can be mixed successfully to get a great fake coverage on transactions combined with a less or more false on alarm rate. This can be presented a literature work of present techniques are used in detecting fake on credit card transaction and also provide a fake on telecommunication. The motive of this approach is to present a complete review of many dissimilar techniques to detect fake transaction [8].

Fake on Credit card have become high usage of credit card in future years. In order to improve shopkeepers risk on management level in an effective, standard way by building an accurate and easy handling on credit card risk maintain system is one of the major important work for the shopkeeper bank [9]. Our motive of the paper is to find the user's model that gives the best fake transaction case. These models are compared with the parameters of their operation made on shopping. In order to develop the detection of fake system it provides by combination of the three fixed methods that could be benefit to fake on transaction. It can also possible to use Bayesian Networks by some of the input method and improved the HMM and Fake detection model in the day to day life detection system. In the upcoming year, these models can be used to elaborate the health insurance of fake detection [10], Here they are using OTP number generates before the transaction and using common detection to increase the accurate level of fake transaction. Two major methods have been used to detect the receiving transaction of fake [11]. During transaction time they are used to producing questions using checking of an engine. The process of producing questions is performed on each time for high security. If all of the questions are not acknowledged than the transaction fails and a message is sent to mobile at the same time [12]. The user has to click on specific part of an image for creation of diagrammatic validation in the click point of authentication in image system. An image contains some parts and regions and also the graphical diagrammatic validation sequence string generated when the user points out on some parts of the regions. This system is used to analyze the possible attacks made by fake transaction [13]. The system also detects the fake during the transaction steps using HMM [14]. The VC is used to produce OPT for making effective detection on credit card fake transaction to eliminate economic damage [15]. If the recorded HMM is not meets the threshold than it is found to be fake transaction. At the same time, valid transaction is not eliminated. Here producing dynamic password used to send to your mobile phones concurrently [16]. In this system the risk metrics of using the credit card, every user holder spends method by using HMM. By using this validated security checking of the information in a transaction is to find whether fake or valid [17]. The method is to not prevent the fake types in fake detection of credit card transaction over point of switching OS terminals. The fake detection can be done by SVM and decision tree to increase the performance.[18].

3. Proposed System

Fraud is growing with the wide use of internet for transaction and in growth of online transactions. Hidden Markov Model (HMM) and credit card recognition (CDD) algorithm innovation resolutions are chosen to protect economic service businesses and credit user-holder from regularly evolving online fraud outbreaks. The motive of this article is to construct an efficient and efficient fraud detection system which is adaptive to the performance changes of user-holder by combining categorization and clustering techniques. The system is two step of fraud detection system which links the entering transaction against the transaction olden time's history to identify the irregularity by using the Hidden Markov Model (HMM) and fraud detection (FD) algorithm in the first step.
In the second step, to reduce the false alarm rate supposed anomalies are checked with the fraud olden time's history database and make sure that the identified anomalies are due to fraudulent transaction. In this work, the fraud identification supports incremental update of transactional data and it handles maximum fraud reporting with high speed and low cost. Planned model is evaluated on both falsely generated and real life data and appearance is very good with accuracy and efficient in identifying fraud transaction in credit card.

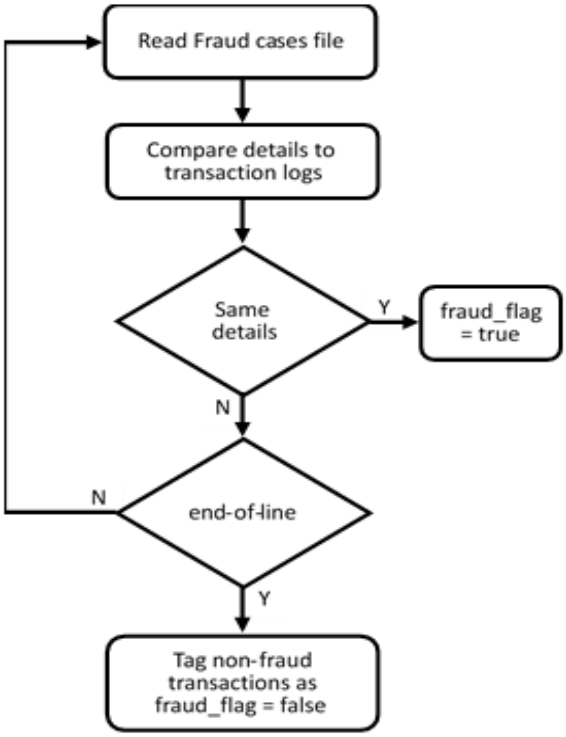


Fig. 1 Flow Diagram of Proposed System

The network becomes most common method of payment for online transaction. Banking system provides e-cash, e-commerce and e-services by using transaction through online. Credit card is one of the greatest ways for online transaction in internet. The risk of fraud transaction using credit card has also been growing very fast today's world. Credit card fraud recognition is one of the moral issues in the credit card industry, advance dealing, fraud detection (FD) algorithm banks and economical institutes. Many concert for credit card fraudulent detection, but hidden Markov Model (HMM) is the great engineering performs implementation for credit card fake detection system. Hidden Markov Model (HMM) generate, observation signs for online transaction, we have shown the Hidden Markov Model (HMM) for fraud identification in Credit card documentation. Hidden Markov Model (HMM) generates, observation signs for online transaction. Statement in an HMM based system is initially user-holder of credit card spending profile and checking an entering transaction, against spending performance of the user-holder.

3.1. Correlation of Page Fraud detection model Categorization

Repeated item and sets of items that happen concurrently in many transactions as the user distinct minimum support. The Fraud identification model support () is defined as the element of the records of database that contains the item set as a subset: For sample, if the database contains 1000 accounts and the item set appears in 800 accounts, then the support () = 800/1000 = 0.8 = 80%; that is, 80% of transaction support of the itemset. In credit card transaction data, the authorized outlines of a purchaser are the set of quality values specific to a purchaser when he does authorized transaction which shows the purchaser performance of user-holder. It is found that the fraudulent are also behaving almost in the same manner as that of a user-holder.

This means that fraudulent are interfering into purchaser accounts after wisdom their genuine transaction performance only by user cardholder. Therefore, instead of finding a common outline for fraudulent performance it is more valid to identify fraud outlines for each purchaser. Thus, in this study, we have constructed two outlines for each purchaser one is Fraud identification model or FRAUD outlines and another one is fraud pattern. When repeated outlines mining is applied to credit card transaction data of a specific purchaser, it returns set of characteristics showing same values in a group of transactions specified by the support. Usually the Fraud detection (FD) model outlines mining algorithms like that of return many such collections and the longest collection containing maximum number of characteristic is selected as that specific purchaser authorized outlines. The training (outlines recognition) algorithm is given below.

Step1: Isolate each user data set from database from every transaction to user's transaction.

Step2: Each user transactions isolate the valid transaction and fake transactions.

Step3: Apply Fake detection (FD) model algorithm to the data set of valid transactions of each user. The Fake detection model algorithm gives a data set of recent data sets. Take the greatest recent data set like the valid design appropriate to each user. Save these valid outlines in legal database design.

Step4: Apply Fake detection (FD) model algorithm to the group of fake transactions of each user. A priority algorithm gives back a group of recent item sets. Take the highest recent data set as the fake outline appropriate to that user. Store these fake outlines in fake outline database.

Input: User Transactions Database, support

Output: Fake detection model design Database CCD, Fake Outline Database FOD

Begin
Group the transactions of each user together.
Let there are “”groups corresponds to “”users
for to do
Separate each group GI into two different groups FOM
and FOM of Fake detection model and fake transactions. Let there are “” legal and “” fake transactions
FIS = fake(FOM, ,); //Set of frequent itemset
LP = ; //Large Frequent Itemset
CCD() = LP;
FIS = fake(FOM, ,); //Set of frequent itemset
FP = ; //Large Frequent Itemset
FPD() = FP;
end for
return CCD & FPD;
end

3.2. Definition Measures of Hidden Markov Model Outline and Fake Detection Algorithm

After finding the HMM and fake outlines for each user, the fake detection system traverses these fake and HMM and outline databases in order to detect fakes. These outline databases are much smaller in size than original user transaction databases as they contain only one record appropriate to a user. This investigate propose a matching algorithm which traverses the outline databases for an using fake Detection algorithm match the incoming transaction to detect fake. If a match is found with authorized outline of the appropriate user, then the matching algorithm returns “0” by providing a green signal to the bank for allowing the transaction. If a closer match is found with fake outline of the appropriate user, then the matching algorithm returns “1” giving an alarm to the bank for stopping the transaction. The size of outline databases is where the number of users is and is the number of attributes. The matching (fake Detection) algorithm is explained below.

Step1. Count the number of attributes in the incoming transaction matching that of the authorized outline of the suitable user. Let it be.
Step2. Count the number of attributes in the incoming transaction matching that of the fake outline of the suitable user. Let it be.
Step 3: If the data are high than the user given similar percentage, so the being paid transaction is allowed.
Step 4: If the data are high than the user given similar percentage, so the being paid transaction is allowed to perform.
Step 5: If both the data are higher than 0, so the being paid transaction is malicious or it may allow to perform.

Input: Correct design database (CCD), Fake design database (FDD), receiving transaction, no of people, no of parameters, no of similar percentage
Output: if it is correct data it produces zero, if not it will produce one to indicate as fraud.

Presumption:
1. The first parameter of each log in design database and gave a customer identification id for a receiving transaction.
2. If the parameter is lost in the recent data set that is each parameter has diverse values in every transaction and then it is not given to the design. So it is not a valid user.

Start
LC=0; // Parameter to count same Fake transaction
FC=0; // Used to count same fake parameter
for 1 to do
if(CCD (1)=(1) then // first parameter
for 2 to do
if(CCD () is correct and CCD()=()) then
FC=FC+1;
end if
end for
end if
end for
if (FC=0) then // no fake
if(LC or number of correct parameters in valid design) >= MP) then
return (0); // valid transaction
else return (1); // fake transaction
end if
else if (LC=0) then // no valid design
if((FC or number of correct parameters in fake design)>=MP) then
return (1); // fake transaction
else return(0); // legal transaction
end if
else if(LC>0 && FC>0) then // both valid and fake design are here
if (FC>=LC) return then (1); // fake transaction

else return (0); // valid transaction
end if
end if
end

3.3. Creation of Recording and Test Data Set

The steps are used to create record and tesed data sets in the database to calculate the model.
(1) Initially, we eliminate the appropriate transactions to customer having only 1 transaction in a database, but it shows in recorded or test data. Now the data are minimized to 40918 transaction.

(2) Then we split that transaction into data set. The recorded set contains 21000 transactions and test set contains 19918 transactions.

Positives (P): No of fake transactions;
Negatives (N): No of valid transactions;
True positives (TP): No of fake transaction found as fake;

True Negatives (TN): No of hidden Markov Model transaction found as valid;
False Positives (FP): No of fake transaction found as fake;
False Negatives (FN): No of fake transaction found as fake;

Table 1: Imbalanced data

Number of customers	Number of transactions in training set			Number of transactions in testing set		
	FRAUD DETECTION or HMM	Fraud	Total	FRAUD DETECTION or HMM	Fraud	Total
200	652	25	677	489	17	506
400	1226	48	1274	864	30	894
600	1716	64	1780	1244	48	1292
800	2169	71	2240	1612	57	1669
1000	2604	131	2735	2002	102	2104
1200	3056	157	3113	2604	144	2748
1400	3440	158	3598	3083	147	3230

3. Result and Discussion

The safety data store in the data set of the registration module. If someone lost the user card so that user's security information will be asked. To verify, the security information contains the group of image is provided to the user to choose the right retort. So that the user able to traverse the next section. Henceforth Hidden Markov Model and fuzzy Darwinian detection algorithm are used to avoid the problem. This algorithm is an extreme reduce the cruel on transaction which gives many number of False Positives found by this system. It used many kinds of transaction like remarks. From that it represent them state in the hidden Markov model. Scam Sapper gives few amounts of false in alarm rate repeating the used data are separated from the transaction belongs to some customer having only one transaction, which is very rigid to analyze the outline of a single transaction. From this method the used data have become less to 19165 transactions. Nowadays there are many dissimilar set of people have selected randomly from the data set.

They used and tested data in the database of a transaction to create dissimilar prepare and test those data to calculate the better operation of Scan Sapper with an increase number in the transactions.
The credit cardholder starts the transaction by communicating to PIN number of a credit card and stores by differentiating the each part of user data that describes an appropriate transaction to be performed by valid user of the cardholder at future.

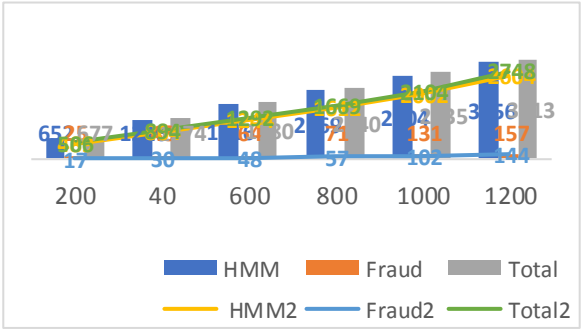


Fig. 2 Training dataset

The group of data is combined as network in the database are agree when the personal checking code is given correctly to communicate with the user. In our day to day life credit card usage is increasing in high. Like credit card has become the trendy mode to make payment in both ordinary and online purchasing. And also malicious transaction is also getting increasing.

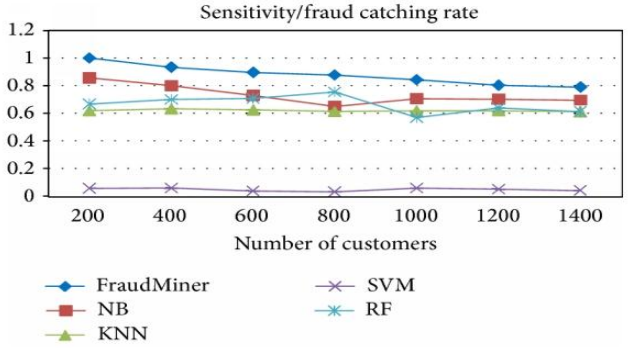


Fig. 3 Sensitivity/fake catching rate

In our survey Fig. 3 work most of the customer works on payments analysis and also few of the customers uses few derivative attributes. Therefore we not found some research happen on unknown data of the transaction in the credit card data set. The data set has some derivative attribute lesson fails to achieve it. So the subjective of the research paper is to improve the efficiency of the fraud to detect from unknown and malicious data in the database.

4. Conclusion

CCFDM (Credit Card fraud detection method) find fraud from its uneven and unknown data set while performing a credit transaction on a card. This cause can be controlled by determining fraud and also outlines for every customer by providing Hidden Markov Model and FDM. The similar algorithm was proposed to determine to which outlines the received transaction of a specified customer is nearer and a better choice is choose. With the aim of handling the opposite side of data there was no selection is makes at each element which is the same as the outline. The concert calculation of the proposed model determine that proposed model has much more rate in detecting the fraud and stable classification and also in processing the image coefficient's correlation. It has fewer false in alarm rate, then the FDM must be fixed to some of the interactive changes. This can be put into the upcoming model by changing the data set of fraud and some outlines. The upcoming outline algorithm performed by setting points on time at stable outline algorithm once in three or six months on each one lakh transaction. This system takes few times and also this provides vital factor in day to day life applications because It is performed by navigating the small outline data set instead of large data sets.

References

[1] H.V. Poor, "Information and inference in the wireless physical layer, "IEEE Wireless Communications, 19, pp. 40-47, 2012.

[2] L. Sankar, S.R. Rajagopalan, and V.H. Poor, "Utility-Privacy Tradeoff in Databases: An Information-theoretic Approach," to IEEE Trans. Inf.Forens. Sec., 8 (6), pp. 838-852, 2013.

[3] S. Pawar, S. El Rouayheb, and K. Ramchandran, "Securing Dynamic Distributed Storage Systems Against Eavesdropping and Adversarial Attacks," IEEE Transactions on Information Theory, 57 (10), pp. 6734- 6753, 2011.

[4] L. Lifeng, S.-W. Ho, and H.V. Poor, "Privacy-Security Trade-Offs in Biometric Security Systems - Part I: Single Use Case," IEEE Trans. Inf. Forensics Security, 6, pp. 122-139, 2011.

[5] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Datamining for credit card fake: A comparative study," Decision SupportSystems, 50, pp. 602-613, 2011.

[6] V. Hodge, J. Austin, "A survey of outlier detection methodologies," J. ofArt. Intel, 22 (2), pp. 85-126, 2004.

[7] D. Tax and R. Duin, "Uniform object generation for optimizing one class classifiers," Journal of Machine Learning Research, 2, pp. 155-173, 2001.

[8] P. Danenas, "Intelligent financial fake detection and analysis: a surveyof recent patents," Recent Patents on Computer Science, 8 (1), pp. 13-23, 2015.

[9] A. Salazar, G. Safont, A. Soriano, L. Vergara, "Automatic credit cardfake detection based on non-linear signal processing," 46th Annual IEEE International Carnahan Conference (ICCST), Boston, USA, pp.207-212, 2012.

[10] R.H. Girgenti, T.P. Hedley, Managing the risk of fake and misconduct: meeting the challenges of a global, regulated and digital environment, McGraw-Hill, 2011.

[11] Nabha Kshirsagar et al, "Credit Card Fake Detection System using Hidden Markov Model and Adaptive Communal Detection" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015.

[12] Akash Pawar, Vishwajit Patil, "Credit Card Fake Detection Using Hidden Markov Model" International journal on information Technology, Mumbai, India.

[13] Vishwesh Satyanarayan Rathi, "Credit Card Fake Detection System using HMM and Image Click Point Authentication" Journal on Computer Engineering, SSBT COET, Bambhori, Jalgaon, India.

[14] Twinkle Patel, Ms. Ompriya Kale, "A Secured Approach to Credit Card Fake Detection Using Hidden Markov Model" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 5, May 2014 .

[15] Prajakta Akole, Nikita Mane, "Secure Transactio :An Credit Card Fake Detection System Using Visual Cryptography" International Journal on Computer Engineering, JSPM's BSIOTR College, Wagholi, Pune.

[16] Vivek Kumar Prasad, "Method and System for Detecting Fake in Credit Card Transaction" International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 5, July 2013.

[17] S Santhosh Baboo, N Preetha,"Analysis of Spending Outline on Credit Card Fake Detection" IOSR Journal of Computer Engineering (IOSR-JCE), Volume 17, Issue 2, Ver. 1 (Mar – Apr. 2015).

[18] Y. Sahin and E. Duman "Detecting Credit Card Fake by Decision Trees and Support Vector Machines" Proceedings of the international Multi-Conference of Engineers and Computer Scientists 2011 Vol I, IMECS 2011, March 16 – 18, Hong Kong.