INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Hybrid methodology for credit card anomaly detection

Rushabh Jadvani
rushabh.j9999@gmail.com
Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra

Vivek Parmar
parmarvivek999@gmail.com
Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra

Dhruvin Sangani
dhruvinsangani@gmail.com
Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra

Payal Sanghavi
payalsanghavi5@gmail.com
Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra

ABSTRACT

Nowadays, people prefer cashless transactions out of which card payment is most prominent. But with its popularity and ease of use, comes threat. Threat of fraud and misuse as we have seen in many debit card fraud cases wherein victims come to know about the fraud transactions done on their account only after transaction was done and they couldn't do anything. Hence detecting such frauds while they are actually happening is difficult. It is only after the transaction is done, we get to know that this particular transaction was fraudulent. Hence in this paper, We have tried to throw some light on a combination approach that includes Hidden Markov Model and Fuzzy logic which we believe can help in accurate detection and prevention of frauds related to card payments.

Keywords: *Credit Card, fraud detection, Hidden Markov Model, Spike Detection, Fuzzy C means, Communal detection.*

1. INTRODUCTION

In day to day life credit cards are used for purchasing goods and services with the help of virtual card for online transaction or physical card for offline transaction. In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company. In online payment mode, attackers need only little information for doing fraudulent transaction (secure code, card number, expiration date etc.). In this purchase method, mainly transactions will be done through Internet or telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the "usual" spending patterns. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds. Since humans tend to exhibit specific behaviorist profiles, every cardholder can be represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system. To avoid credit card fraud detection we have used different algorithms which make detection easy for us, the algorithms we have used are Hidden Markov Model [4], RUS & MRN [3] Fuzzy C Means[2], KNN & Outlier Detection[6]. This will help us to achieve our goal which is fraud detection and it will divide the transactions in to part and will verify at every stage of transactions and its double secured layered website. Thus it will help us too secure the transaction and will detect fraud easily.

2. LITERATURE REVIEW

Hidden Markov Model: A Hidden Markov Model [4] is a finite set of states; each state is linked with a probability distribution. Transitions among these states are governed by a set of probabilities called transition probabilities. In a particular state a possible outcome or observation can be generated which is associated symbol of observation of probability distribution. It is only the outcome, not the state that is visible to an external observer and therefore states are ``hidden" to the outside observer; hence the name Hidden Markov Model. Hence, Hidden Markov Model [4] is a perfect solution for addressing detection of fraud transaction

through credit card. One more important benefit of the HMM-based approach is an extreme decrease in the number of False Positives transactions recognized as malicious by a fraud detection system even though they are really genuine. In this prediction process, HMM consider mainly three price value ranges such as. a. Low (l), b. Medium (m) and, c. High (h).

Communal detection (CD): Whitelist oriented approach to a fixed set of attributes is done by CD. The CD [8] is working in real time with the whitelist database (WL Database). It can be used to compare the current application with WL database based on the similarity in the attributes. The communal relationship reflects the family bonds and legitimate behavior of the same applicant. WL Database is constructed by link-types and its volume.

CD algorithm performs with communal data of the applicant. It uses to identify for legal behavior and data errors of the applicant. The CD algorithm works in real time by exact or similar matches between categorical data, giving scores. Combinations of mini-discrete and micro-discrete streams of data from current and previous applicants are implemented in this algorithm. The WL Database is updated and reconstructed for a period of time and reset the parameter values by this algorithm.

Spike Detection (SD): Contrast ion of the CD is SD algorithm. Blacklist or attribute-oriented approach on the variable - size set of attributes is done by SD [8]. After CD evaluation, SD takes care of the further process. It compares and evaluates the attribute with black list database (BL Database). BL database collects the data from Cibil History database (CH Database). CH Database consists of the past history of applicant's behavior in the Banking process. Strengthen of the CD is done by SD by providing attributes weights, reflecting the degree of importance of the attribute. This method trades of effectiveness for efficiency.

Fuzzy C-means: Fuzzy c-means [2] (FCM) is a clustering algorithm that allows individual data to belong to two or more clusters. This method has a great advantage to overcome the limitations of the hard clustering, and hence widely applied in many real life applications. Let Cl = {c1,…..,cn} be the clusters belonging to the datasets for a particular card Ck and A = {a1,a2,…..,an} be the possible attributes in a transaction. In this work, the attributes used for clustering are transaction amount and items purchased. Suppose, transaction made on a card Ck is denoted as TCk. The cluster is formed based on the spending patterns followed by cardholder Ck. The Euclidian distance dik from the cluster head pi to the object point xk of the transaction TCk is calculated by using the following expression: SC = dik = ||xk – pi|| (1) The SC is then compared with the already pre-set threshold values i.e. upper threshold Uth) and the lower threshold (Lth) which are determined experimentally. Depending on the result of comparison, three rules are defined as follows: a) If (SC < Lth), then the credit card transaction is allowed. (Genuine) b) Else if (Lth SC Uth), then move the transaction to the suspicious table for applying the learning mechanism for strengthening the initial observation. (Suspicious) c) Else, reject the transaction i.e. when SC > Uth. (Fraudulent) The transactions those are found to be suspicious are passed to the learning phase before taking the final decision.

3. COMPARISON OF ALGORITHMS

Table 1: Comparison of Algorithms

Parameter	Fuzzy c mean	HMM	Communal Detection	Spike Detection	KNN	Outlier Detection
Efficiency	Much more	More	More	More	More	Less than fuzzy
Optimization	More	More	Less than fuzzy and HMM	More	More	less
Time Stamp	Yes	Yes	No	Yes	Yes	Yes
Time slot	Yes	Overall timeslot can be interrupted	No	Yes	Yes	No
Based on priority	Higher priority	Higher	Higher	Higher	Higher	Less
Implementation	Easy	Easy and can be merge with fuzzy c mean	Easy	Easy	Moderate	Difficult
Popularity	Most popular	Most popular	Less	More popular	More popular	Moderately popular
Base algorithm	Mean	Markov model	Based on itself	Based on itself	Bayesian version	Based on itself
Performance	Very good	Very good	Good	Very good	Good	Good

4. PROPOSED SYSTEM

In the existing credit card fraud detection business processing system, fraudulent transaction will be detected after transaction is done. It is difficult to find out fraudulent and regarding loses will be barred by issuing authorities. Hidden Markov Model is the

statistical tools for engineer and scientists to solve various problems. In this paper, it is shown that credit card fraud can be detected using Hidden Markov Model during transactions. Hidden Markov Model helps to obtain a high fraud coverage combined with a low false alarm rate. The fraud detection module will work in the following steps:

- The payment gateway will have details of credit card like card number, its expiry date etc.
- The merchant will provide details like shipping address, amount of purchase, transaction date and time etc.
- The payment gateway will send necessary parameters to the Fraud Detection System.
- Our proposed system will use suitable data mining techniques in a neural network to train itself and generate outcome.
- On the basis of learning, the final result of a transaction (fraudulent or not) will be sent to the payment gateway.
- The final result containing the decision and other relevant information will be displayed in the final UI page to the merchant by payment gateway administrator.

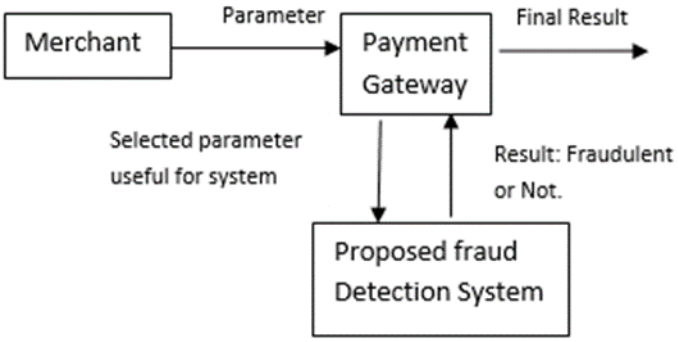

Fig 1. System Architecture

5. CONCLUSION

In this paper we have discovered application of Hidden Markov Model [4] in MasterCard fraud detection. The various steps in MasterCard group action process square measures represented because the underlying model of Hidden Markov Model. The objective of this paper is to detect frauds caused by credit card by merging various types of algorithms discussed in this paper. Therefore, by combining all the algorithms that are described in this paper, the frauds were detected successfully.

6. REFERENCES

[1] Aman Srivastava. Sandipani Basu, Credit Card Fraud Detection at Merchant Side using Neural Networks 2016 InternationalConference on Computing for SustainableGlobal Development (INDIACom).
[2] Tanmay Kumar Behera, Suvasini Panigrahi, Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering, Second International Conference on Advances in Computing and Communication Engineering-2015.
[3] Anusorn Charleonnan, Credit Card Fraud Detection Using RUS and MRN Algorithms, the Management and Innovation Technology International Conference-2016
[4] Shailesh S. Dhok, Dr. G. R. Bamnote, Credit Card Fraud Detection Using Hidden Markov Model, International Journal of Advanced Research in Computer Science.
[5] S.Patil, V.Bhusari, Study of Hidden Markov Model in Credit Card Fraudulent Detection, International Journal of Computer Applications (0975 – 8887).
[6] N.Malini, Dr.M.Pushpa, Analysis on Credit Card Fraud Identification Techniques based on KNN and Outlier Detection, 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics.
[7] Anusorn Charleonnan, Credit Card Fraud Detection Using RUS and MRN Algorithms, The 2016 Management and Innovation Technology International Conference.
[8] Ramkumar E. & Mrs. Kavitha P., Online Credit Card Application & Identity Crime Detection, International Journal of Engineering Research & Technology(IJERT).

