Credit Card Fraud Detection Using BLAST-SSAHA Hybridization & Hidden Markov Model

Bhaviya Rajesh Gandani

Abstract **— In today's generation, the use of credit card has become mundane across the world. Credit card is nothing but a card that entitles the holder to borrow money from the issuer. Credit cards are used at the point of sale as a means of paying the seller for goods or services in lieu of payment by cash or check. Because of their ease of use, credit cards have become the most popular methods in the world. It is quite worthy to do online shopping, paying bills or other related tasks by using credit cards. Though a credit card is the best form of payment, there is a rapid increase in the fraud transaction using the credit card. Normally, the fraudulent transaction is detected after the transaction is been done and because of these, it becomes arduous to find a fraudster and more than that the issuing authorities has to bear the losses. To solve this major concern, BLAST-SHAHA hybridization and hidden markov model is used. BLAST-SHAHA hybridization is used to determine the analogy between the incoming transaction and the previous transactions of a particular cardholder and can detect fraud when there is any mismatch between the transactions. Hidden markov model is nothing but the ubiquitous tool used to model time series data. In this issue, hidden markov model is used to detect the fraud transactions and raise an alarm in the event of fraud transactions.**

Keywords**—Hidden markov model, BLAST-SSAHA hybridization, Credit card, Fraud detection**

I. INTRODUCTION

Generally, payment using credit card has become significant in day-to-day life. Credit cards are used as physical card for offline shopping and virtual card for online shopping.

Manuscript received August, 2015.

Bhaviya Rajesh Gandani*, Dept. Of Computer Science, Theem College of Engineering Mumbai, India, +91-7875337948*

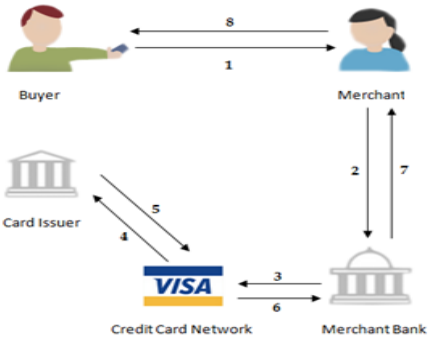

Fig.1: Credit Card Payment Procedure

The Fig.1 describes the credit card payment procedure which is done offline or online. There are 8 steps carried out for completing the purchase. Step 1 states that the cardholder presents his/her card to the merchant for payment. Step 2 states that merchant processes the card and transaction information and requests an authorization from the merchant bank. Step 3 describes the merchant bank submits the authorization request to credit card network. Step 4 describes that credit card network forwards the request to card issuer. Step 5 states that card issuer approve or decline the transaction and responds to credit card network. Step 6 states that credit card network forwards the response to merchant bank. Step 7 describes that merchant bank forwards the response to merchant. Step 8 describes that merchant receives the authorization response and completes the transaction accordingly.

To instigate the fraudulent transaction in an offline purchase, an attacker has to embezzle the credit card from the card holder and if the card holder is unaware about the loss of his/her card; the credit card company will bear substantial losses.

Different from the offline purchase, online purchase fraudulent transaction requires only the modicum amount of information about the credit card. Online purchase is been done either through telephone where the card holder provides the details of the credit card or through the secure payment gateway site. In both the scenarios, chances of fraud transaction are possible. In telephone online purchase fraud transaction, card holder might provide the card details to the fraud. In secure payment gateway site fraud transaction, chances are that card holder is been redirected to the fake site created by the fraudster but it's quite similar to the actual secure payment gateway so that card holder is unaware of fraud transaction. For online purchase fraud transaction, the fraudster just fetches the credit card number, expiration date of credit card and card code number (CVV).

ISSN: 2278 – 7798

In order to detect such kind of embezzlement, it's important to scrutinize the spending patterns on every card purchase and to figure out any erratic with respect to usual spending patterns. Therefore, fraud detection mechanism, which is based on the analysis of previous purchase data of card holder, works well to impede this kind of frauds. Analysis for creating the patterns is been done by knowing the information about the typical purchase category of a card holder, time since the last purchase made by the card holder, the amount of money spent etc. Awry from such patterns may lead to major concern in the system.

II. Fraud Detection Mechanisms

There have been various credit card fraud detection mechanisms been implemented. Below is the list for the same:-

A. Genetic Algorithm

Genetic Algorithms are algorithms where the optimal solution is been found by doing the random probability distribution or pattern that may be analyzed statistically but may not be predicted precisely. In order to detect the fraud, genetic algorithm takes various factors into consideration. These factors include credit card usage frequency count, credit card usage location, average daily spending, current bank balance, credit card overdraft etc.

B. Neural Network

Neural Network, as the name suggests, is used to detect frauds with the help of a computer or a system that work and think like a human brain. Similar to the human brain, this neural network system learns from the past experience and knowledge and based on that; it fetches out a pattern and make predictions. The neural network systems are been trained on parameters with respect to card holder details such as income of a card holder, occupation of a cardholder, number of large purchases on credit card, large purchase frequency, large purchase locations etc. Every time, it checks for the pattern used by the one who did the purchase with the pattern of the original card holder. If the pattern is matched, transaction is genuine else it is fraud.

C. Decision Tree & Support Vector Machines

Fraud detection using decision tree and support vector machines scans each account separately using suitable descriptors and the transactions are been identified. Based on that, it finds whether the transaction is normal or fraud. The identification is based on the intuition score which is been produced by developed classifier model. Classifier predicts whether the transaction is normal or fraud when a new transaction is on progress.

III. Proposed Models

A. BLAST-SSAHA Hybridization

BLAST-SSAHA Hybridization is one of the most effective and cheapest ways to detect a credit card fraud transaction. BLAST stands for Basic Local Alignment Search Tool whereas SSAHA stands for Sequence Search and Alignment by Hashing Algorithm.

The Fig.2 shows the working of BLAST-SHAHA Hybridization in Credit Card Fraud Detection System. Whenever a new transaction is initiated, BLAST-SHAHA Hybridization decides whether the transaction is authentic or fake.Thus; it avoids the loss of money and impedes the fraudster from making the fraud transaction successful. A Time Amount (TA) sequence is been created by merging the incoming sequence with the sequence that are in the Customer

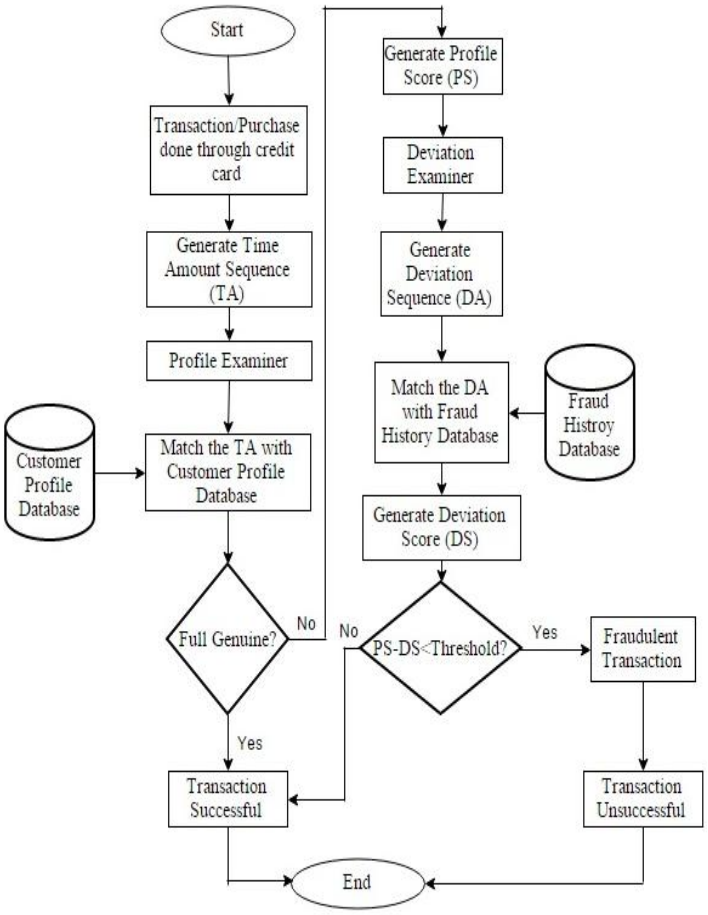

Fig.2: BLAST-SSAHA Hybridization in Credit Card Fraud Detection

Profile Database with respect to the particular card holder. It's the role of Profile Examiner to examine the incoming sequence of transaction with the genuine cardholder's previous spending sequence with the help of TA.

If the Profile Examiner finds much similarity between the incoming sequence of transaction and the spending sequence then it is proved that TA contains genuine transaction and thus the transaction is done successfully. But if there is some anomaly found by profile examiner then they are given to Deviation Examiner for further probe after generating the Profile Score (PS). PS is generated by Profile Examiner based on the similarity between TA and Customer Profile Database.

ISSN: 2278 – 7798

Deviation Analyzer creates the deviation sequence (DA) by examining the matching patterns between the incoming sequence of transaction and the Fraud History Database. Deviation Examiner then generates the Deviation Score (DS) based on DA.

Finally, the difference between PS and DS is calculated and if the difference is above the Threshold then the transaction is carried out successfully. Else, it will raise an alarm stating that transaction is fraudulent and thus blocks the transaction to be done.

B. Hidden Markov Model

Hidden Markov Model (HMM) is an implementation based on the probability distribution in which there are sequences of observations but the sequence of states, that went through to generate these observations, is unknown. HMM is very effective tool to detect the credit card frauds because its speed of detection is fast. HMM is a stochastic model in which analysis is been done statistically but prediction may not be precise. HMM is a model in which the system is assumed to have the Markov process with hidden states.

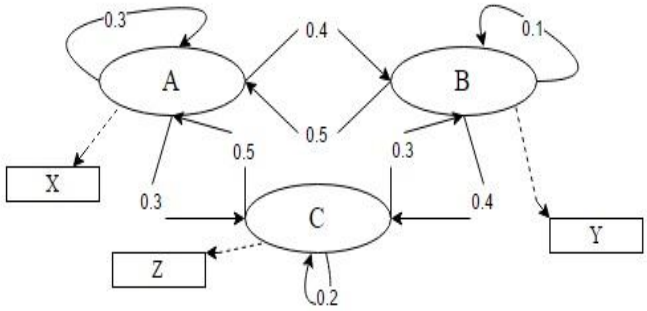

Fig.3: Markov Process

The Fig.3 shows the Markov Process. There are three states A, B, C and three observations X, Y, Z. The probability distribution is done with states accordingly. Suppose, for example, there is the sequence of observations given as Y-X-X, we can easily verify the sequence of states with these observations B-A-A and the probability of sequence is the product of transitions i.e. 0.5 * 0.3 = 0.15.

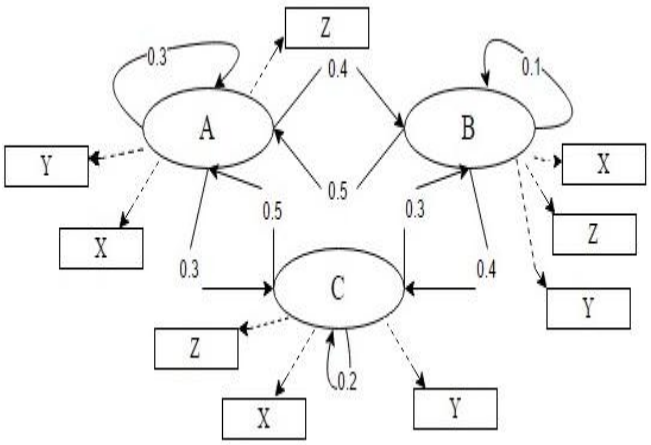

Fig.4: HMM Model

The Fig.4 shows the extension of Markov Process which is called as Hidden Markov Model. In this model, all the observations are provided in each state. Suppose, for example, there is the sequence of observations given as Y-X-X, we can't verify the sequence of states that produced these observations and hence the state sequence is hidden. Hence, the name given is Hidden Markov Model.

In order to detect credit card fraud, HMM categorize the card holder's profile as low, medium, high based on the spending patterns of the card holder with respect to the amount. Each card holder is been assigned a set of probabilities based on their spending patterns. Whenever the transaction is in progress, the amount of that transaction is matched with the card holder's category. The transaction is successful only if it justifies the predefined threshold value else the transaction is declared as fraudulent.

Based on the category, the card holder will need to answer the security questions for the transaction to be done successfully. Low category will have questions like city of birth, childhood hero etc. Medium category will have questions like school name, mother's maiden name, favorite color etc. High category will have questions like dream job, favorite car, favorite sport etc.

For instance, there is an incoming transaction of $750 and card holder's categories are Low = ($0, $500), Medium = ($500, $800) and High = ($800 to credit card limit); then transaction which the card holder does will follow the medium category. So, the card holder will need to answer the questions which belong to the medium profile of that card holder. Depending upon the answers, transaction is declared as legitimate or fraudulent.

HMM Example -

Table 1: Credit Card Transactions

Transaction	Amount	Transaction	Amount
1	550	11	525
2	650	12	850
3	185	13	900
4	200	14	690
5	350	15	100
6	700	16	725
7	50	17	275
8	775	18	595
9	10	19	580
10	660	20	135

Low = ($0, $500),
Medium = ($500, $800) and
High = ($800 to credit card limit)

Table 1 shows the transactions done using a credit card till date. Transaction are arranged in an ascending order of most recent transaction i.e. transaction done for the first time are placed in 20th position and last transaction is placed in 1st position.

ISSN: 2278 – 7798

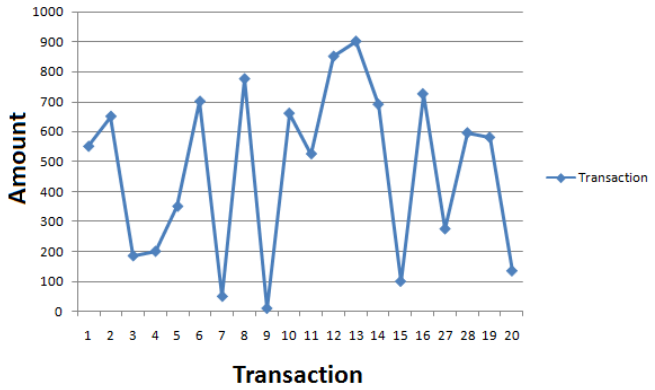

Fig.5: Transaction Chart Based on Table

The Fig.5 shows the transaction chart based on Table 1. It shows the transaction in x-axis and amount in y-axis.

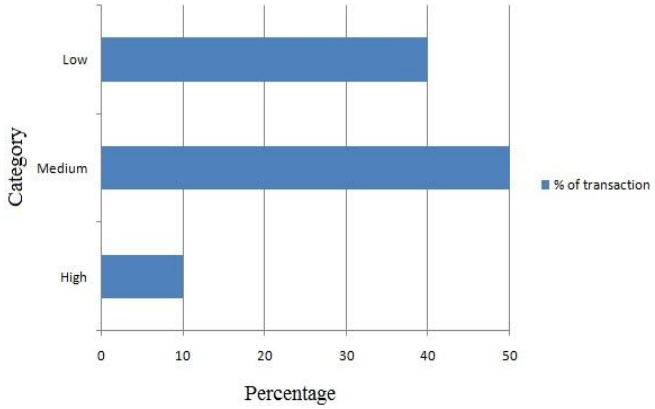

Fig.6: Percentage of transactions category wise

The Fig.6 shows the percentage of transactions category wise. It is observed from the example that spending profile that lies in medium category has higher percentage than the spending profiles that falls in other two categories. Hence, the card holder has been asked the questions most of the times that lie in medium category.

IV. Conclusion

The optimal solution for credit card fraud is implementing BLAST-SSAHA Hybridization or HMM model. We also discussed with other alternative algorithms that can detect frauds. BLAST-SSAHA Hybridization matches the incoming transaction with the previous spending patterns to detect fraud whereas HMM makes use of probability distribution to detect fraud. Further research can be made on these models by implementing it to a more secure level.

V. References

[1] Vasili s Aggelis "Offiine Internet Banking Fraud Detection". 0-7695-2567-9/06, 2006, IEEE Proceedings of the /first International Conference on Availability, Reliability and Security.

[2] Abhinav Srivastava, Amlan Kundu, Shamik Sural. "Credit Card Fraud Detection Using Hidden Markov Model" IEEE Transaction, January-March 2008. Pp. 3747.

[3] Qinghua Zhang "Study on Fraud Risk Prevention of Online Banks". International Conference on Networks Security, Wireless Communications and Trusted Computing.978-0-7695-3610-1/09, 2009 IEEE, pp 181184.

[4] Osama Dandash,Phu Dung Le and Bala Srinivasan " Security Analysis for Internet Banking Models". Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, IEEE transaction, 2007, pp. 1141-1146.

[5] X.D. Hoang, J. Hu, and P. Bertok, "A Multi-Layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls," Proc. 11th IEEE International Conf. Networks, 2003, Pp.531-536.

[6] Khyati Chaudhary and Bhawna Mallick "Exploration of Data Mining Techniques in Fraud Detection System", International Journal of Electronics and Computer Science Engineering 1765, ISSN- 2277-1956.

[7] Mubeena Syeda, Yan-Qing Zbang and Yi Pan" Parallel Granular Neural Networks for Fast Credit Card Fraud Detection", IEEE Transaction .2002, pp.572-577

[8] Aleskerov, Emin, Bernd Freisleben, and Bharat Rao "CARDWATCH: A neural network based database mining system for credit card fraud detection.", Computational Intelligence for Financial Engineering. Piscataway, NJ: IEEE, 1997, pp.220-226.

VI. Author's Profile

Bhaviya Rajesh Gandani
B.E. In Computer Engineering (2013), Mumbai

ISSN: 2278 – 7798