Fraud Detection in Online Credit Card Payment

Aishwarya Kaneri[1], Anugrah S[2], Isha Bharti[3], Samruddhi Jadhav[4], Mitali Kadu[5]

[1,3,4,5] Cummins College of Engineering, Pune University
[2]Army Institute of Technology, Pune University

***

Abstract - *Online shopping has become an integral part of our life. As card payment becomes the most prevailing mode of payment for both online as well as regular purchase, frauds related with it are also accelerating. Fraud detection in card payment is a crucial part of e-shopping. It includes monitoring of the spending behavior of customers in order to detect and avoid fraud. This paper uses outlier analysis for detecting fraud in which behavioral pattern of the customers along with their social and financial status is considered. Various rules for fraud detection are considered which if not followed can lead to a suspicious transaction. History of past transactions of user is maintained at payment engine's database. Analysis of real data at payment engine's database and data obtained from user is done by algorithm described in this paper for fraud detection and a possible fraudulent transaction is detected at real time.*

Key Words: Behavioral pattern, Credit card, Data mining, Fraud detection, Fraudulent transaction, Outlier analysis, Payment gateway.

1. INTRODUCTION

In era of plastic cards with rapid advancement of electronic commerce, the credit card has become convenient and de facto standard for online shopping. The increased number of credit card transaction open the door for thieves to steal credit card details and commit fraud. it impacts a fraction of percent of all purchases made with plastic, according to data from Federal Reserve ,it represents one of the biggest concerns among customers. Due to this card issuers bore a 63% share of fraudulent losses in 2012 and merchants assumed the other 37% of liability, according to the Nilson Report, August 2013. So it becomes essential to improve the fraud detection system to minimize the losses. The credit card fraud detection system presents a number of challenging issues for data mining.

This paper is to purpose a credit card fraud detection system using outlier analysis. Outlier is a data point which is significantly different from the remaining data and deviates so much from other observation as to arouse suspicions that it was generated by a different mechanism[10]. Outlier analysis of transactional data depending on its past behavioural patterns is done to label transaction as either fraudulent or not. For analysis, Rule Engine is implemented.

2. Algorithm Flow Diagram

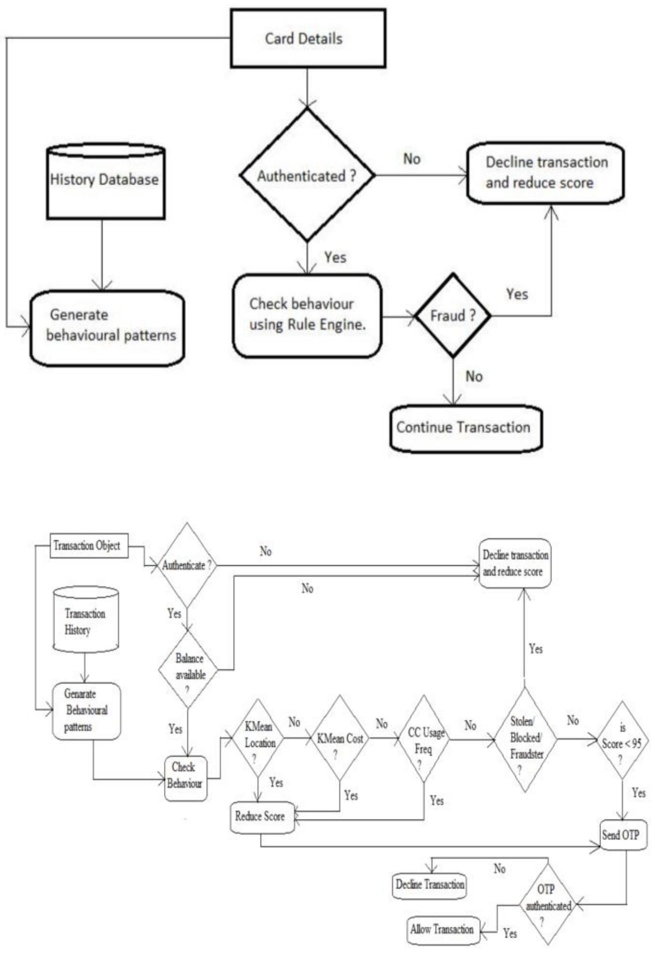

Fig -1: Overall flow of the algorithm

3. Experiment Process

The past transactions' data of the user is collected from the bank's database. The current transaction's data is compared against the patterns generated from the previously collected data. To generate the patterns based upon the user's behavior, various fraud detection rules are considered. Every user is provided with a score attribute which is stored in bank's database. This score is incremented if the current transaction's data of the user passes the rule and is decremented otherwise. If the current transaction's data of the user fails any rule or his current score goes below the threshold, then the transaction is suspicious.

3.1 Algorithm

kMeans Clustering algorithm is used to divide the past transactions' data collected into groups such that data objects in a group have maximum similarity and minimum difference (distance) as compared to other groups and outliers. Once the clusters are formed, it is seen whether the current transaction's data makes a fit into any one of the cluster's radius range. If not, then the current transaction is an outlier, hence it is a suspicious fraud.

Step 1 : Collect the past transactions' data of the user from the bank's database .

Step 2 : Behavioral patterns of the user are generated by clustering algorithms.

Step 3 : The current transaction's data is tested across all the rules and score is updated accordingly.

Step 4 : The score is checked against the threshold and transaction is labeled as suspicious or normal transaction.

3.2 Rules Considered for Fraud Detection

1. User Authentication : The user credentials are verified and validated.

2. Location : The current transaction's location is tested against the user's regular transaction locations' pattern.
   For example, if the user usually makes a transaction from Pune, Mumbai or Nashik, and suddenly the current transaction is being done from a distant place like California, then the transaction becomes a suspicious one.

3. Cost : The current transaction's amount is tested against the user's regular transaction amounts' pattern.

   For example, if the user usually makes a transaction of amount in the range of 5000 to 7000 and 25000 to 30000, and suddenly the current transaction is being done for amount of 100000, then the transaction becomes a suspicious one.

4. Credit : The current transaction's amount is checked against the credit of the user's credit card.

5. Credit Card Usage Frequency : Credit Card Usage Frequency = Total number of times the card is used / Credit card's age (in months) If Credit Card Usage Frequency is greater than 0.2, fraud condition is checked. Fraud condition = number of times Card used Today >(5 * Credit Card Usage Frequency). If Fraud condition is true, then then the transaction becomes a suspicious one[7].

6. Already a fraudster : If the credit card used for current transaction was used for a fraudulent transaction in past, then the current transaction is denied.

7. Stolen/Blocked : If the credit card used for current transaction is already reported as stolen or blocked, then the current transaction is denied.

8. Date (Timespan) : The current transaction's date is tested against the user's regular transaction dates' pattern. For example, if the transaction from a particular card occurs after a long span of time unlike his regular credit card usage pattern then the transaction becomes a suspicious one.

Table -1: Rules in Rules Engine

Rule Name	Pass Condition	Fail Condition
User Authentication	Valid credentials	Invalid credentials
Location	One of the regular purchasing locations Eg. Pune, Mumbai, Nashik	Sudden change in the location (larger distance) as compared to regular ones Eg. Pune , Mumbai, California
Cost	In the range of regular purchase amount Eg. Regular range : 5000-7000 Current Transaction : 6000	The total amount of purchase is way beyond the range of the regular purchase amount Eg. Regular range : 5000-7000 Current transaction : 70,000
Rule Name	**Pass Condition**	**Fail Condition**
Credit	The Credit in the card is greater than or equal to the purchase amount Eg.Credit balance – 2000 Purchase amount - 1500	The Credit in the card is less than the purchase amount Eg. Credit balance – 1000 Purchase amount - 1500
Credit Card Usage Frequency	Usage frequency is as usual	Credit card is used far more number of times as compared to its previous usage Eg. Previous usage :: 2-3 times a month Current usage :: 5th time in a day
Already a fraudster	No record of fraudulent transaction is present for the current card.	The credit card number is already used during a fraudulent transaction.
Stolen/Blocked	No record of being	The credit card is

	stolen/blocked is present for the current card	reported as stolen or it is blocked Eg. Card no 340000000000009 is reported as stolen according to our database.
Date(Timespan)	The transaction occurs during regular interval pattern	The transaction from a particular card occurs after a long span of time unlike his regular purchase pattern.

4. Results

1. Card number 5500000000000004 has made previous transactions at locations with latitude and longitude values as [(17.532, 21.576), (18.345, 22.534), (17.655, 22.654), (16.651, 20.127), (20.764, 72.765), (21.64, 71.75), (20.94, 73.765)]. The current transaction is made from location (100.654, 181.409). The clusters formed are [17.532, 21.576), (18.345, 22.534), (17.655, 22.654), (16.651, 20.127)] and [(20.764, 72.765), (21.64, 71.75), (20.94, 73.765)]. The current transaction's data doesn't fit into any one of the cluster's radius range. Hence the score is decremented as the transaction is suspicious.

2. Card number 4111111111111111 has made previous transactions of amounts [1000, 1500, 1200, 500, 2000, 15000, 17000, 20000]. The current transaction is made of amount 1,000,000. The clusters formed are [1000, 1500, 1200, 500, 2000] and [15000, 17000, 20000]. The current transaction's data doesn't fit into any one of the cluster's radius range. Hence the score is decremented as the transaction is suspicious.

5. CONCLUSION

This paper presents mechanism of credit card fraud detection and examines the result based on the principles of clustering algorithm. Using outlier analysis this paper, tries to minimize false alerts and improving existing models for detection of fraud. In this study fraud detected and fraud transactions are generated by maintaining the fraudulent history table. If this is applied into bank credit card fraud detection system, the probability of fraud transactions can be predicted soon after credit card transactions by the banks. Though fraud in online card payment cannot be eradicated still this study is trying to minimize fraud.

ACKNOWLEDGEMENT

We render our sincere thanks to Barclays team (BTCI, Barclays Technology Centre India) for their support and encouragement.

REFERENCES

[1] S .Benson Edwin Raj ,A. Annie Portia- Analysis On Credit Card Fraud Detection methods ,IEEE International conference on computer, communication and Electrical Technology, IEEE March 2011.

[2] Daniel Garner -Genetic algorithms for credit card fraud detection , IEEE Transactions May 2011.

[3] M.HamdiOzcelik, Mine Isik, —Improving a credit card fraud detection system using Genetic algorithm , IEEE International Conference on Networking and Information Technology, IEEE 2010.

[4] Wen-Fang YU, Na Wang-Research on Credit Card Fraud Detection Model Based on Distance Sum, IEEE International Joint Conference on Artificial Intelligence 2009.

[5] Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, —BLAST-SSAHA Hybridization for Credit Card Fraud Detection,‖ IEEE Transactions On Dependable And Se-cure Computing, vol. 6, Issue no. 4, pp.309-315, October-December 2009.

[6] Ashish Gupta 1, Jagdish Raikwal- Fraud Detection credit card Transaction using Hybrid model-International Journal of engineering and computer science ISSN:2319-7242 Volume 3 Issue 1 Jan, 2014.

[7] K.RamaKalyani, D.UmaDevi - Fraud Detection of Credit Card Payment System by Genetic Algorithm, International Journal of Scientific & Engineering Research Volume 3, Issue 7, July-2012.

[8] Wang Xi- Some Ideas about Credit Card Fraud Prediction China Trial. Apr. 2008.

[9] White paper- How a hybrid Anti-Fraud approach could have saved government benefit programs more than $100 millions.