Fraud perception and prohibition for reliable Transaction of cards using datamining

[1]Adit Chitnawis, [2]Asim Ubare, [3]Namrata Shahasane, [4]Prof. Siddhesh Khanvilkar

Pillai HOC College of engineering and technology, Rasayani
Navi Mumbai, India

***Abstract*: Financial fraud is an ever growing threat with overwhelming consequences in the financial industry. As a need of security and reliable transaction for the users who use this technology in day to day life. We propose a system where a specific pattern is granted on every transaction for users who do transaction through cards. This pattern contains location of the user and limit levied by bank on user transaction as specified by user. The system also allows to discover suspicious transaction and if found to be distrustful then that transaction is immediately adjourned and verification of transaction is done hence it could be blocked if authenticate acknowledgement is not obtained within the specific time span from user.**

***Keywords*: Fraud, Credit card, Transaction**

1. INTRODUCTION

With an upsurge in financial accounting fraud in the current economic scenario experienced, financial accounting fraud detection have received considerable attention from the investors, academic researchers, media, the financial community and regulators. Due to some high profile financial frauds discovered and reported at large companies like Enron, Lucent, WorldCom and Satyam over the last decade, the requirement of detecting, defining and reporting financial accounting fraud has increased. Fraud can be defined as criminal deception with intent of acquiring financial gain. High dependence on internet technology has enjoyed increased card transactions. As card transactions become the most prevailing mode of payment for both online and offline transaction, credit card fraud rate also accelerates. Credit card fraud can come in either inner card fraud or external card fraud. Inner card fraud occurs as a result of consent between cardholders and bank by using false identity to commit fraud while the external card fraud involves the use of stolen credit card to get cash through dubious means. A lot of researches have been devoted to detection of external card fraud which accounts for majority of credit card frauds. Detecting fraudulent transactions using traditional methods of manual detection is time consuming and inefficient, thus the advent of big data has made manual methods more impractical. However, financial institutions have focused attention to recent computational methodologies to handle credit card fraud problem.

2. LITERATURE REVIEW

In [1] To stop these fallacious transactions a system is designed which uses the combination of Hidden Markov Model, Behavior Based Technique, and Genetic Algorithm. Each and every transaction is tested with above mentioned technique and Fraud Detection system test the transaction and detects fraud. The goal is to detect least and accurate false fraud detection.

In [2] In this system KNN algorithm and outlier detection methods are implemented to optimize the best solution for the fraud detection problem. These approaches are proved to minimize the false alarm rates and increase the fraud detection rate. Any of these methods can be implemented on bank credit card fraud detection system, to detect and prevent the fraudulent transaction.

In [3] This system uses data mining technology to build credit card acquiring fraud analysis model based on mass credit card transaction data and merchant materials, and also developed merchant fraud risk management system. The application of this system effectively reduces the frequency of fraudulent credit card transactions, and helps to minimize losses from merchant's fraud.

3. PURPOSE SYSTEM

We propose a system where a specific pattern is granted on every transaction for users who do transaction through cards. This pattern contains location of the user and limit levied by bank on user transaction as specified by user at the time of opening bank account. The system also allows to discover suspicious transaction and if found to be distrustful then that transaction is immediately halted and verification of transaction is done hence it could be blocked if authenticate acknowledgement is not obtained within the specific time span from user.

Our system detects the fraud while ongoing transaction is carried out ,we are focused on prevention of the fraud before it happened. When a transaction is found suspicious, system re-verify the transaction by sending verification link on E-mail and notifying by sending SMS on mobile phone of user.

Workflow of system

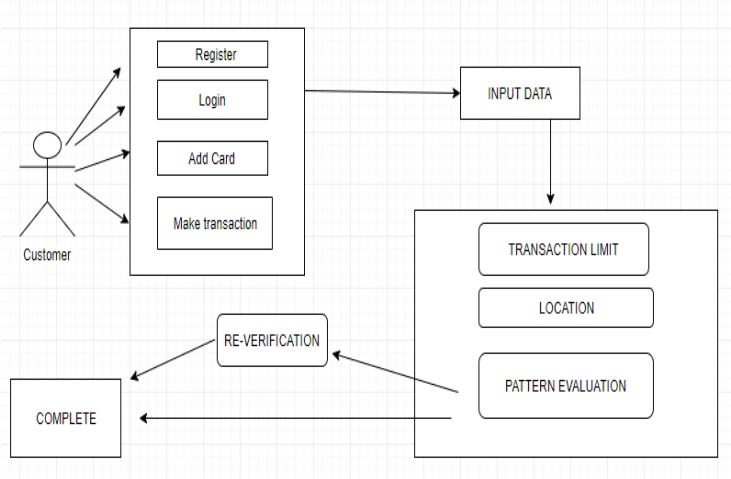


Figure 3.1 Workflow of system

4. METHODOLOGY

Datamining: Data mining is popularly used to effectively detect fraud because of its efficiency in finding unknown patterns in a collected data set. Data mining is a technology that allows the discovery of knowledge in a dataset. Data is collected from different sources into a dataset and then we can discover patterns in the way all data in the dataset relates with another and then make predictions based on the patterns discovered. Data mining takes a dataset as an input and produces models or patterns as output. Data mining refers to extracting the hidden, previously unknown and potentially useful information from database, and then offering the understandable knowledge, such as association rules, cluster patterns etc, so as to support users for decision-making.

Algorithm we are using for detecting credit card Fraud

Logistic Regression: Logistic Regression is one of the classification algorithm, used to predict a binary values in a given set of independent variables (1 / 0, Yes / No, True / False). To represent binary / categorical values, dummy variables are used. For the purpose of special case in the logistic regression is a linear regression, when the resulting variable is categorical then the log of odds are used for dependent variable and also it predicts the probability of occurrence of an event by fitting data to a logistic function. Such as O = e^(I0 + I1*x) / (1 + e^(I0 + I1*x)) Where, O is the predicted output

I0 is the bias or intercept term

I1 is the coefficient for the single input value (x). Each column in the input data has an associated I coefficient (a constant real value) that must be learned from the training data.

y = e^(b0 + b1*x) / (1 + e^(b0 + b1*x))

Logistic regression is started with the simple linear regression equation in which dependent variable can be enclosed in a link function.

A(O) = β0 + β(x) Where

A() : link function

O : outcome variable

x : dependent variable

A function is established using two things:

1) Probability of Success (pr) and

2) Probability of Failure (1-pr).

pr should meet following criteria:

a) Probability must always be positive (since p>=0)

b) Probability must always be less than equals to 1 (since pr <= 1). By applying exponential in the first criteria and the value is always greater than equals to 1.

pr = exp(βo + β(x)) = e^(βo + β(x))

For the second criteria, same exponential is divided by adding 1 to it so that the value will be less than equals to 1

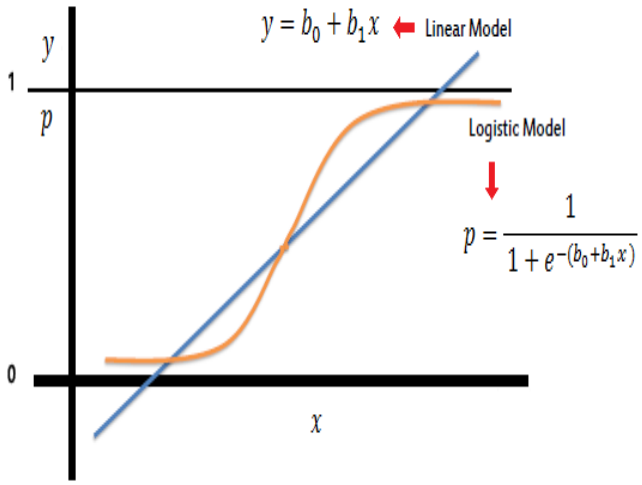
pr = e^(βo + β(x)) / e^(βo + β(x)) + 1 Logistic function is used in the logistic regression in which cost function quantifies the error, as it models response is compared with the true value.

X(θ)=−1/m*(Σyilog(hθ(xi))+(1−yi)log(1-hθ(xi)))

Where

hθ(xi) : logistic function

yi : outcome variable Gradient descent is a learning algorithm



Conclusion

Our system detects the fraud while ongoing transaction is carried out, we are focused on prevention of the fraud before it happened. Our system reduces the impact of fraud because of the daily transactions limit criteria specified by the user at the time of opening the bank account. In this system we will be using Logistics Regression to check the validity of the transaction made by the user. The system sends a SMS and mail to the user to enhance the security of the application. The user will click on the link provided in the mail to make the transaction valid. So as to prevent attacker from making fraudulent transaction.

Acknowledgment

We remain immensely obliged **to Prof. Siddhesh Khanvilkar** for providing us with the moral and technical support and guiding us. We would also like to thank our guide for providing us with his expert opinion and valuable suggestions at every stage of the project. We would like to take this opportunity to thank **Prof. Monisha Mohan**, Head of Information Technology for her motivation and valuable support. This acknowledgment is incomplete without thanking teaching and non-teaching staff of the department of their kind support. We would also like to thank **Dr. Madhumita Chatterjee**, Principal of Pillai HOC College of Engineering and Technology, Rasayani for providing the infrastructure and resources required for the project.

References

[1] Ayushi Agrawal Shiv Kumar Amit Kumar Mishra: A Novel Approach for Credit Card Fraud Detection Published in**:** IEEE Internet of Things Journal (Volume: 5 , Issue: 5 , Oct. 2018)

[2] N. Malini M. Pushpa: Analysis on credit card fraud identification techniques based on KNN and outlier detection Published in**:** 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)

[3] Yuh-Jen Chen Chun-Han Wu: Big Data-Based Fraud Detection Method for Financial Statements of Business Groups IEEE Published in: 2017