ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

Secure Mechanism for Credit Card Transaction Fraud Detection System

Alka Herenj[1], Susmita Mishra[2]

PG student, Dept. of CSE, Rajalakshmi Engineering College, Thandalam, Chennai, India[1]

Assistant Professor, Dept. of CSE, Rajalakshmi Engineering College, Thandalam, Chennai, India[2]

ABSTRACT: **Credit Card Fraud is the most common, prevalent and costly crime in existence these days. Business rules, scorecards and known fraud matching methods are used in the existing system to detect frauds. However, all these methods have certain limitations. A new multilayered detection system is been proposed which is entirely data-mining based and they deal with real social relationships and finds spikes in duplicates and finally assigns suspicious scores which helps in identifying the fraudster. The data mining layers prevent fraudsters to attack and enhance a secure transaction. This research is totally concerned with credit card application fraud detection by performing the process of asking security queries to the persons involved in the transactions and as well as by removing real time data errors.**

Keywords: Credit Card Fraud, Anomaly detection, Threshold Transaction, Security, Data mining layers

I. Introduction

In this generation where carrying heavy cash is very cumbersome and risky too, credit card comes as a boon and is extensively used due to its convenience and safety. Credit Card also called plastic money is the plastic card which gives authorization to the buyers to purchase goods by borrowing money from the financial institution within the given eligible limit. A credit card is a payment card issued to users as a system of payment. It permits the cardholder to pay for goods and services based on the holder's promise to get hold of them. The issuer of the card creates a revolving account and grants a line of credit to the consumer from which the user can borrow money for payment to a merchant or as a cash advance to the user.

The features of credit cards are:

Credit Limit: The maximum amount that the card holder will be allowed to borrow will be as per the permitted credit limit, which is based on the income earned, previous credit history etc. of the applicant.

- **Interest Rate:** An Interest Rate is charged on due balance. The interest rate can be anywhere from 0 to 79%. Also a late payment fee is levied if the minimum amount as mentioned on the bill is not paid.
- **Time Limit**: The borrower gets credit for 20 to 50 days depending on the date of the bill and not on the date of purchase of goods/service. The due amount has to be paid by the mentioned due date and if the amount is not paid within the given date, a grace time of few more days is granted after which interest is levied.
- **Incentives:** The credit card holders will be given incentives depending upon the type of credit card they are using.

The parties involved in Credit Card Transaction are:

- Card Holder or Applicant
- Bank issuing credit card
- Merchant
- Acquiring Bank

The Steps involved in Credit Card transaction are as follows:

- **Authorization:** that amount of the cardholder's credit limit. The cardholder presents the card as payment to the merchant and the merchant submits the transaction to the acquirer. The acquirer verifies the transaction type, the credit card number and the amount with the issuer (Card-issuing bank) and reserves for the merchant. An authorization will create an approval code, which the merchant keeps with the transaction.

- **Batching**: Authorized transactions are stored in "batches", which are sent to the acquirer. Batches are usually submitted once per day at the end of the business day. Suppose a transaction is not submitted in the batch, the authorization will be valid for a period determined by the issuer, after which the held amount will be return to the cardholder's available credit. Few transactions may be submitted in the batch without prior authorizations; these are either transactions falling under the merchant's floor limit or ones where the authorization was unsuccessful but the merchant still attempts to force the transaction through.

- **Clearing and Settlement**: The acquirer sends the batch transactions through the credit card association, which debit the issuers for payment and credits the acquirer. Effectively, the issuer pays the acquirer for the transaction.
- **Funding**: Once the acquirer has been paid, the acquirer has to pay the merchant. The merchant gets the amount totalling the funds in the batch minus either the "discount

rate," "mid-qualified rate", or "non-qualified rate" which are tiers of fees the merchant pays the acquirer for processing the transactions.

- **Chargebacks**: A chargeback is an event in which money in a merchant account is held due to a dispute relating to the transaction. Chargebacks are basically initiated by the cardholder. In the result of a chargeback, the issuer will return the transaction to the acquirer for resolution. The acquirer forwards the chargeback to the merchant, who must either agree to the chargeback or contest it.

Credit cards are one of the most famous targets of fraud but not the only one; fraud can occur with any type of credit products, like home loans, personal loans, and retail. The explosion of credit card fraud is not only due to the constant increase of card usage but also to the ease of perpetuating credit card fraud.

In the Credit Card business, fraud occurs when a lender is fooled by a borrower offering him/her purchases, believing that the borrower credit card account will provide payment for this purchase. Ideally no payment will be made. If the payment is made, the credit card issuer will reclaim the amount paid. It is on the internet that half of all credit card fraud is conducted. Fraudsters have usually connections with the affected business. It can be an internal party but most likely an external party. As an external party, fraud is committed being a prospective/existing customer or a prospective/existing supplier. Three different profiles can be identified for external fraudsters: the average offender, criminal offender, and organized crime offender.

Fraud is an intentional deception made for personal gain or to damage another individual. Fraud could be a crime, and additionally a civil law violation. Defrauding individuals or entities of money or valuables is a common purpose of fraud. Fraud is usually understood as dishonesty calculated for advantage. An individual who is dishonest may be called a fraud. Fraud would simply describe the method used to break the law or regulation requiring the license. Fraud requires an additional element of False Pretenses created to induce a victim to turn over property, services, or money. Fraud resembles theft in that both involve some form of illegal taking, but the two mustn't be confused.

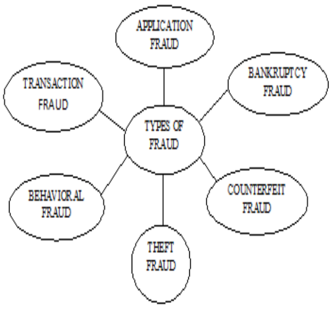

Fig. 1 Types of Fraud

Bankruptcy Fraud is one of the most difficult types of fraud to predict. Bankruptcy fraud means using a credit card while being insolvent. In other words, purchasers use credit cards knowing that they are not able to pay for their purchases. The bank will send them an order to pay. However, the customers will be recognized as being in a state of personal bankruptcy and not able to recover their debts. The bank will have to cover the losses itself. Usually, this type of fraud loss is not included in the calculation of the fraud loss provision as it is considered a charge-off loss. The only way to prevent this Bankruptcy Fraud is by doing a pre-check with credit bureau in order to be informed about the banking history of the customers.

Theft Fraud means using a card that is not yours. The perpetrator will steal the card of somebody else and use it as many times as possible before the card is blocked. The sooner the owner will react and contact the bank, the faster the bank will take measures to stop the thief.

Counterfeit Fraud occurs when the credit card is used remotely; only the credit card details are needed. At one point, one will copy your card number and codes and use it via certain web-sites, where no signature or physical cards are required.

Application fraud is when someone applies for a credit card with false information. To detect application fraud, the solution is to implement a fraud system that allows identifying suspicious applications. To detect application fraud, two different situations have to be distinguished: when applications come from a same individual with the same details, the so-called duplicates, and when applications come from different individuals with same details, the so called identity fraudsters.

Behavioral fraud occurs when details of legitimate cards have been obtained fraudulently and sales are made on a 'cardholder present' basis. These sales contain telephone sales and e-commerce transactions, where only the credit card details are required. Behavioral fraud can be detected by implementing a fraud scorecard predicting which customers are likely to default. Traditional credit scorecards are used to detect customers who are likely to default, and the cause for this may include fraud. Regarding the process, using scoring for fraud prevention is similar to any other use, including profit, default, and collection. The score reflects experience of past cases, and the result is a binary outcome: a genuine customer or fraudster.

II. BACKGROUND

Many individual data mining and non-data mining techniques have been designed implemented and evaluated in fraud detection.

There are non-data mining layers of defence to protect against credit application fraud which also has certain limitations. The first existing defence is created up of scorecards and business rules. In Australia, one business rule is the hundred-point physical identity check test which requires the applicant to provide sufficient point-weighted identity documents face-to-face. They must add up to at least 100 points, where a passport is worth 70 points. Another business rule is to contact (or investigate) the applicant over the Internet or telephone. The above two business rules are highly effective, however human resource intensive. To rely less on human resources, a business rule is to match an application's identity number, phone number, or address against external databases. This is convenient; however the public telephone and address directories, credit history data and semipublic voters' register, can have data quality issues of completeness, accuracy and timeliness. In addition, scorecards for credit grading can catch a small percentage of fraud which does not look creditworthy; but it also removes outlier applications which have a higher probability of being fraudulent.

The second existing defence is called fraud matching. Here, better known frauds are complete applications which were confirmed to have the intent to defraud and usually periodically recorded into a blacklist. Moreover, the current applications are matched against the blacklist. This has the profit and clarity of hindsight because patterns often repeat themselves. Additionally, there are two main problems in using known frauds. Firstly, they are untimely due to long time delays, in days or months, for fraud to expose it, and be reported and recorded. This provides a window of opportunity for fraudsters. Secondly, recording of frauds is highly manual. This implies known frauds can be incorrect, expensive, difficult to obtain and have the potential of breaching privacy. In many data mining techniques much of work in credit application fraud detection remains proprietary and exact performance figures unpublished so it is not necessary to compare the new techniques with leading ones. For example,[3] has Detect which provides four categories of policy rules to signal fraud, one of which is checking a new credit application against historical application data for consistency. In another example,[4] has ID Score-Risk which gives a combine view of each credit application's characteristics and their similarity to other industry-provided or Web identity's characteristics.

Statistical tools are based on comparing the observed data with expected values, but expected values can be derived depending upon the content. [5], has Statistical fraud detection methods which may be 'supervised' or 'unsupervised'. In supervised, samples of both fraudulent and non fraudulent records are used to construct models which allow one to assign new observations into one of the two classes. Unsupervised methods simply seek those accounts or customers which are most dissimilar from the norm. Case-based reasoning is used in screening of Credit Applications. [6] uses threshold nearest neighbour matching. Diagnosis utilizes multiple selection criteria and resolution strategies to analyse the retrieved cases. Peer group Analysis [7] compares the cumulative mean weekly amount between a target account and other similar accounts at subsequent time points. On credit card accounts, the time window to calculate a peer group is 13 weeks and the future time window is 4 weeks. Bayesian networks [8] uncover simulated anthrax attacks from real emergency department data. Break Point Analysis [7] monitors intraaccount behaviour over time. It detects rapid spending or sharp increases in weekly spending within a single account.

III. MAIN CONTRIBUTION

The main contribution of this paper is to enhance secure transaction in credit card applications by using two new data-mining layers. These new layers improve detection of fraudulent applications because the detection system can detect various kinds of attacks, better account for changing legal behavior, and eliminate the redundant attributes.

CD or Communal Detection layer is based on whitelist-oriented approach. It utilizes fixed set of attributes. White-listing makes use of real social-relationships. This reduces false positives by lowering the suspicion scores.SD or Spike Detection layer is used to complement and strengthen CD. This layer is an attribute oriented approach concentrating on variable-size set of attributes. It detects spikes in duplicates or similar applications. This increases true positives by adjusting suspicion scores appropriately. Hence, by using both the data mining layers suspicious scores are generated. A threshold transaction amount is calculated based on the previous transactions made by the user. If the credit transaction amount is higher than the threshold, the user performing the transaction has to answer a security question. If the answer results to success, the transaction is authenticated or else it will be declined. In this manner a secure transaction will be processed.

IV. PROPOSED METHODOLOGY

This section is divided into five sections which systematically explains the modules and its purposes.

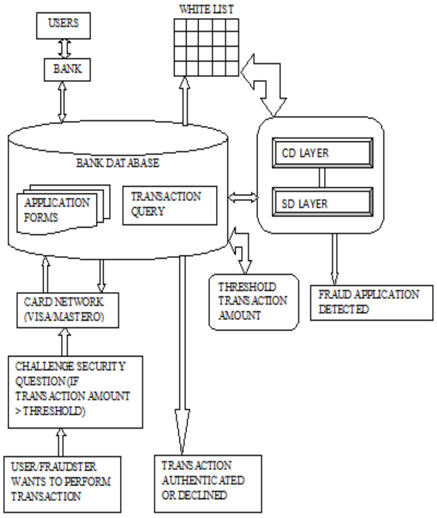
USERS
WHITE LIST
BANK
BANK DATABASE
APPLICATION FORMS
TRANSACTION QUERY
CD LAYER
SD LAYER
CARD NETWORK (VISA/MASTERO)
THRESHOLD TRANSACTION AMOUNT
FRAUD APPLICATION DETECTED
CHALLENGE SECURITY QUESTION(IF TRANSACTION AMOUNT > THRESHOLD)
USER/FRAUDSTER WANTS TO PERFORM TRANSACTION
TRANSACTION AUTHENTICATED OR DECLINED

Fig. 2 Architecture Diagram

A. *Credit Card Application Form & Initial White List Creation*

Bank Database is created. Credit card Application for with ten attributes is created. The attributes include Applicant name Address, Date of Birth, mobile Number, email id, occupation, Driving License ID, Passport ID, Social Security Number (SSN) etc. The SSN, Passport ID, Driving License ID are known as Unique IDs of a person.

Customers request the bank to obtain Credit Card. Now the Bank provides application forms to the customers. The customers fill the application form and submit it to the Bank. The applications are compared to each other and will be assigned a link type. The link type is nothing but a binary string (eg.01011111) in which '1' represents matched fields and '0' represents unmatched fields. Finally, initial white list is created. The White list has list of verified applications, link type, number of applications corresponding to a particular link type and weight.

B. *CD Suspicious Score*

Here a new application form submitted by a user and applications in the whitelist are taken as input to the Communal Detection (CD) layer. New Application is compared with windows of applications in the whitelist. CD layer is used to find communal relationships between the applications. If four or more fields are matched in the new application against application in the whitelist, then CD assigns less suspicious score. Otherwise the new application form is added into the whitelist and the list is updated. Since CD accounts for legal relationship it assigns less suspicious scores to new application form and gives as input to the SD layer.

C. *SD Suspicious Score*

Here the application form i.e. the output of the CD layer is taken into account. Spike Detection (SD) layer verifies the matched fields for their priority. The unique ID fields are given higher priority. If unique IDs are matched then the suspicious score gets increased and the application form is declared as fraud and hence finally rejected. If none of the unique IDs are matched then the application form is added into the whitelist and the list is updated. Since the SD accounts for fraud behaviour detection, the fraud application is rejected.

D. *Threshold Transaction Amount Calculation*

The Bank monitors the transaction history of legal user or the credit card holder. Based on the previous transactions made by the user the bank calculates a threshold value of the transaction amount. The threshold value is nothing but average of all the previous transactions.

E. *Secure Transaction*

The case assumed here is that the card holder unfortunately missed his card there by a fraud gets the card. Now the fraudster or the legal user performs credit transaction. If the credit transaction amount is higher than the threshold, the fraudster or legal user is asked to challenge the security question. If the challenge is success i.e. in case of legal user the transaction is authenticated otherwise it is declined in case of fraudster. Hence the secure transaction is performed.

V. RESULTS & DISCUSSIONS

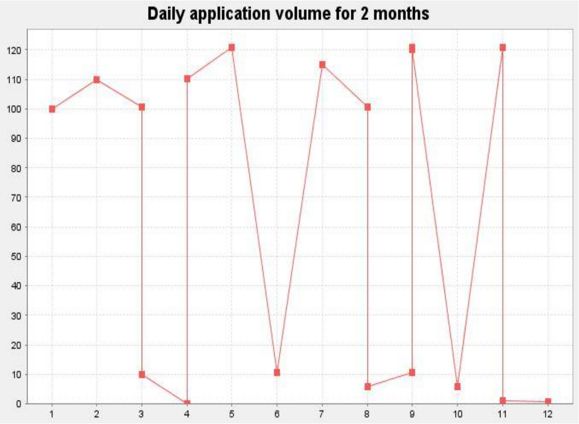

Fig. 3 Fraud in Credit Applications

Fig 3 shows the detailed ups and downs in the credit applications for two months.

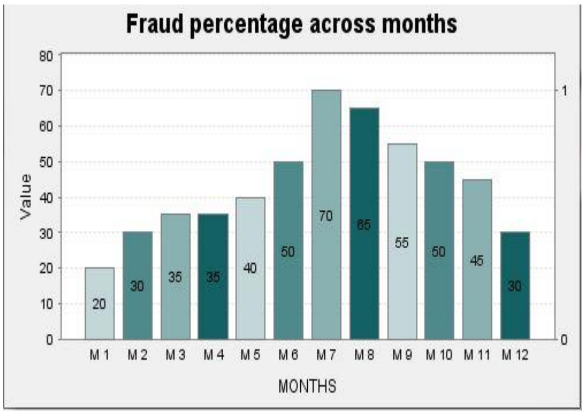

Fig. 4 Occurrence of Fraud in Credit Applications in a year

Fig 4 shows how occurrence of fraud is detected in a year. It's not that, fraud has completely vanished but we can say that its uncertain and unpredictable. However measures can be applied to stop them from occurring.

Our empirical results demonstrate how legal behaviour is distinguished from fraud behaviour. It is accomplished by the process of asking security queries to the persons performing transactions if they exceed the threshold transaction amount. This work convincingly express that CD and SD layers produce effective and secure transaction as well as make it obvious that real time data errors are removed.

VI. CONCLUSION

The main focus of this paper is the detection of fraudsters in credit applications and by implementing the new data mining layers which helps in performing a secure transaction. It has documented the development and evaluation in credit card application fraud detection system. The implementation of CD and SD layers is done to detect fraudulent activities in duplicates as well as the real social relationships. Communal Detection and Spike Detection layers are continuously updated so that the fraudster should never get a chance of attacking again. Similarly the threshold transaction amount will also be updated according to the transactions done by the user.

REFERENCES

[1] Linda Delamaire, Hussein Abdou and John Pointon, “Credit Card Fraud and Detection Techniques”, bank and bank systems, vol.4,no.2,pp.57-68, 2009.
[2] Clifton Phua, Kate Smith-Miles, Vincent Cheng-Siong Lee and Ross Gayler, “Resilient Identity Crime Detection”, IEEE Transactions on Knowledge and Data Engineering, vol.2, no. 3,pp.533-546, 2012.
[3] Experian Detect: Application Fraud Prevention System, Whitepaper,
http://www.experian.com/products/pdf/experian_detect.pdf, 2008.
[4] ID Analytics, “ID Score-Risk: Gain Greater Visibility into Individual Identity Risk, “Unpublished, 2008.
[5] Richard J.Boltan and David J.Hand, “Statistical Fraud Detection”, pp.1-54, 2002.
[6] I. Witten and E. Frank, “Data Mining: Practical Machine Learning Tools and Techniques with Java” , Morgan Kauffman, 2000.
[7] R.Boltan and D. Hand, “Unsupervised Profiling Methods for Fraud Detection”, Statistical Science, vol. 17, no. 3,pp.235-255, 2001.
[8] W. Wong, A. Moore, G. Cooper and M. Wagner, “Bayesian Network Anomaly Pattern Detection for Detecting Disease Outbreaks”, Proc.20th Int’l Conf. Machine Learning, pp.808-815, 2003.
[9] P. Brockett, R. Derrig, L. Golden, A. Levine and M. Alpert, “Fraud Classification Using Principal Component Analysis of RIDITs”, The J.Risk and Insurance, vol.69, no. 3, pp.341-371, 2002.
[10] Chris Jay Hoofnagle, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law and Technology, Vol. 21 no.1, pp.98-122, 2007.