Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Various Types of Credit Card Fraud and Security Measures

Eswari.M*
Department Computer Science and Engineering & Anna university, India

Navaneetha Krishnan.M
Head Department of Computer Science and Engineering & Anna university, India

Abstract— Now a day's credit cards usage has become hysterically. As credit card becomes the most famous in the form of amount for both online and regular purchase, in this cases fraud also increased. Credit card is process of transfer or debits the cash in bank organization. Credit card fraud is act of using credit card of authorized user by unauthorized user. Their various types of fraud and detect the fraud for providing security to credit card holder in banking industry. This criminal activity has been more complex and there is no safe for valid credit card holders. The aims of this paper are firstly, discussing various types of credit card fraud and secondly, how to reduce the fraud by taking security measures and using alternative data mining algorithms.

Keywords—Credit Card, Credit Card Fraud, Security Measures, Data Mining.

I. INTRODUCTION

Credit card frauds are robbing the card physical or stealing the user information like account number and password for illegal transactions. Credit card based purchases can be classified in two types such as Physical Card and Virtual Card. Physical Card purchase is nothing but presents his card actually to a trader for making a payment. Virtual Card purchase is giving some main information about a card like card number, expiration data and secure code is needed to make the payment[6].Anyone can apply for credit card by using valid details of card holder or can even use money from the card which is not known until complaint has hired. This criminal activity has been more complex and there is no safe for valid credit card holders. In the latest years, the current data mining involves community with credit card fraud detection model established on data mining. Classical data mining algorithms can't be used directly so another way is using heuristic approaches for security card holders. Section 2 contains of various types of frauds and security measures with alternative algorithm. Section 3 existing related work and algorithms in credit card fraud detection.

II. TYPES OF CREDIT CARD FRAUDS AND THEIR DETECTION ALGORITMS

In many situation of using credit card there are various types fraud has been found. Fraudsters are artistic of criminal acts and innovating new way of steal cards. This section consists of types of credit card fraud discussed in detail figure 1.

A. Application Fraud

When users apply for credit card using personal details like phone number, communication address and e-mail address. Using this details has been application fraud has classified into two types which are duplicate details and fraud identity. When a user has already accessing card and reapplying for another card using same information is called duplicate details. When unauthorized user steals valid user information for applying credit card is called fraud identity. The measure taken to reduce application fraud is checking user information is valid or not by correct proofs before giving the credit card. There are many algorithms introduced but recently using communal and spike detection algorithm [7] to overcome application fraud which is done by ranking link-types between user applicants by volume. When user submits application detected using synthetic communal relationships and white list is constructed to find valid user. The redundant attributes are frequently filtered which reduce the suspicion score for detecting fraud in previous work and better account for changing legal behaviour.

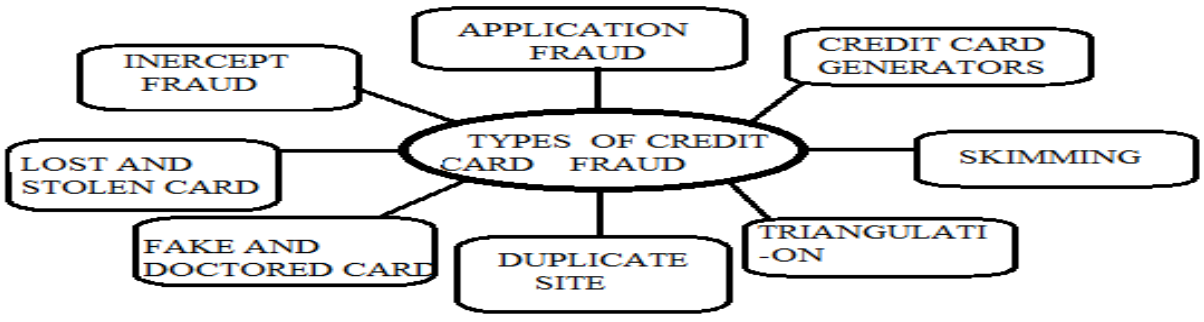

Fig. 1 Types Of Credit Card Fraud

B. Intercept Fraud

© 2014, IJARCSSE All Rights Reserved

Intercept fraud is done in postal service while the credit card has been issued to card holder. This card has robbed from postal service before it is received by cardholders. Postal service is easy way to steal credit card without knowing present of card holders. The measure taken to reduce intercept fraud is done by card issuers and post office. Card issuers should give credit card in local bank by verifying their passport and voter id whether the user details and photo are valid then hand over the credit card to the particular card holder.post office should introduces anti-theft among staffs and has their own fraud detection branch in order to find the fraud more easily and fast when complaint has hired. [8] The card is electromagnetically recorded which has aborted with a man-readable code or man-non readable code. Especially, the electromagnetically recorded code has an account, a visual comparison algorithm code, a visual comparison code, an electronic comparison code, a card identification number and a personal identification number .A reader can see the account code in order to produces electromagnetically coded account number. The reader achieves electronic comparison code with a preselected mathematical algorithm and compares the algorithm answer with a preselected portion of the account number. The reader processed card identification number with another preselected algorithm and compares the algorithm answer with the visual comparison code. By using visual comparison algorithm code to overcome intercept fraud.

C. Lost and Stolen Cards

When a user loses his/her card in unknown location in absent of mind than anyone may take card using money by transferring. If anyone robbing the card from card holder by knowing their personal details for illegal transaction. The measure taken when lost or stolen card from card holder by implementing new technology like if card is loosed then card holder must hire complaint to particular bank that card can't used anywhere by anyone like blocking the card. If card is stolen then identifying fraud by the help of bank. [9] Using Data stream outlier detection algorithm which is based on reverse k-nearest neighbours (SODRNN) which lost and stolen card makes to stop fraudulent transactions and reduces the number of scans of database to only one. Analysis of this algorithm in both synthetic and real data sets is efficient and effective. When new coming object is inserted then all objects in current window whose k-nearest neighbours are influenced and gives m object whose RNNK (p) is small as outliers in the given query.

D. Fake and Doctored Cards

The formations of fake and doctored cards are major traditional forms in credit card fraud. Fake card is has become outmoded in credit card techniques because it has consists lot of security features and good quality of card. Fake card is nothing but creating duplicate card by scratch or altering the present card in order to show different details. Doctored card is form changing the present card that user has acquired to delete metallic strip using a powerful electro-magnet then changing the details so that it is matching with valid user. Thus this form of card has been outmoded and yet many new techniques are still finding by fraud to form this kind of cards. [13] The Card Verification Method is provides 3 0r 4 digit numeric code which is printed on the card but it is not visible in the magnetic stripe. When card is not available card holder can this numeric code during and submit it with authorization. This code cannot copy from receipts or skimmed from magnetic stripe which protect merchant. But it doesn't provide security during transaction by physically stolen cards. In future card security is increased rapidly by using hologram.

E. Duplicate Site

Criminal has been more in duplicate site which is formed in order to get confidential data from card holder. Example is creation of fault site such as purchasing items by online payment. Card holder can buy the items by giving all details of card in that site but hackers get all details for access credit card. This way of encrypting valid user details in duplicate site through internet. The measure should be to reduce duplicate site is done by allow authorized site should consists of standard bar code verification it. Valid user should be known about this duplicates site in the network. [10]Using Hidden Markov Model (HMM) is used to check transaction processing during online shopping or e-commerce. An HMM is a double embedded stochastic process with two hierarchy levels. It is used to model convoluted stochastic processes compared with traditional Markov model. It contains finite set of states conducted by a set of transition probabilities. In that state, an outcome or observation can be developed with probability distribution. It is only the outcome which is not visible an external observer.

F. Skimming

Skimming is outmoded device which is used for information provided in the magnetic stripe on the backside of the card is transcribed to another stripe of credit card. When skimming was introduced it has become fast moving among all fraudsters they are taken place in hotel and shops. This device is portable which is carried in pocket in order read details of card holder by swiping card in electronic magnetic stripe reader. There is new advanced technology in skimming device is called as scanner which is used read card holder details illegal and can also re-write same details it is way of crashing encryption process. This devices are movable, can cache more than hundreds of smart chip details and able to re-write the chips. It is process of skimming cards which consists of software has able of collecting the access able data stored on credit cards illegally. Customer can't able trace back when skimming has taken placed. [12] To judge original user not only by card's pin number during transaction by also asking secret questions and SMS feedback system for credit card. Using genetic algorithm, neural network, ADA COST algorithm filters the database two ways such as first is filter database for user and card information and second is Rule based filter need to update the database for both user and credit card then analysing transactional behaviour. This authentication mechanism is useful while transaction to secure cash card from being cloned via skimmed device and providing more security.

G. Triangulation

© 2014, IJARCSSE All Rights Reserved

Triangular is another type of credit card fraud which is similar like duplicate site. Triangulation operates are in web site which consists high offers in goods like receiving the goods before payment or high sale offers. To purchasing the goods, customer should giving full details like address, phone number and valid information in the particular site. When customer provides all confidential information in that site then fraud will buy the goods in another name by using valid information. Fraudsters can purchase goods using details of card holder from different countries. Customer will not able to trace back and leads to great confusion because during enquire police are unable find fraud due to different social, political and nations. [11]Using Genetic algorithm is better solutions for triangulation problem as time processes to detect whether any fraud has been occurred in the transaction or not and also show the user about the result. It checks instance of input then finally holds optimal solution. It is an evolutionary search and optimisation technique which is Mimics natural evolution .In future there may able to generalized for global fraud detection problem and classify problem in variable misclassification costs.

H. Credit Card Generators

Credit card generator is nothing but issuing the card to valid card holder by generating card credit number and expiry date correctly. Generating credit card is clarion and compact. An ancient generator consists up to 999 card number formed from single account number. This generator has no guard of guesstimate on valid expiry date because card holder or generator will not know at time of expiry date. So the measure taken to generator card is the latest generator has introduced account number ending with expiry date. Even generator can give information before expiry date so that card holder can renew credit card before expiry date get over. Thus using security measure credit card generator should provide valid card to valid user.

III. RELATED WORK

In the paper [7], proposes a new multilayered detection system complemented with two additional layers: communal detection finds real social relationships to reduce the suspicion score, and is tamper resistant to synthetic social relationships. Spike detection finds spikes in duplicates to increase the suspicion score, and is probe-resistant for attributes. Results on the data support the hypothesis that successful credit application fraud patterns are sudden and exhibit sharp spikes in duplicates. Although this research is specific to credit application fraud detection, the concept of resilience, together with adaptively and quality data are general to the design, implementation, and evaluation of all detection systems. In the paper [14], proposes to detect fraudulent transaction through the neural network along with the genetic algorithm. Genetic algorithm are used for making the decision about the network topology, number of hidden layers, number of nodes that will be used in the design of neural network for our problem of credit card fraud detection. For the learning purpose of artificial neural network we will use supervised learning feed forward back propagation algorithm. In the paper [15], to the classification of credit applications that has the potential to adapt to population drift as it occurs by Adaptive online algorithm. It a novel methodology for the classification of credit applications that has the potential to adapt to population drift as it occurs. This provides the opportunity to update the credit risk classifier as new labelled data arrives. Assorted experimental results suggest that the proposed method has the potential to yield significant performance improvement over standard approaches, without sacrificing the classifier's descriptive capabilities.

IV. CONCLUSIONS AND FUTURE WORK

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained. Causal Productions has used its best efforts to ensure that the templates have the same appearance.

ACKNOWLEDGMENT

The authors would like to the anonymous reviewers for their constructive and useful comments.

REFERENCES

[1] http://people.exeter.ac.uk/watupman/undergrad/owsylves/index.html
[2] http://www.fraudlabs.com/fraudlabswhitepaperpg1.html
[3] "Survey on credit card fraud detection methods"- Krishna Kumar Tripathi, Mahesh A. Pavaskar.
[4] Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK)- "Credit card fraud and detection techniques: a review".
[5] http://en.wikipedia.org/wiki/Credit_card_fraud.
[6] http://www.authorstream.com/Presentation/aSGuest126126-1328422-ppt-s/
[7] "Resilient Identity Crime Detection"- Clifton Phua, Member,Kate Smith-Miles, Senior Member,Vincent Lee, and Ross Gayler,2011.
[8] http://www.google.co.in/patents/US4626669?dq=Mobile
[9] "Credit card fraud detection using anti-k nearest neighbor algorithm"- Venkata Ratnam Ganji, Siva Naga Prasad Mannem, International Journal on Computer Science and Engineering (IJCSE).
[10] "Credit Card Fraud Detection Using Hidden Markov Model abd Its Performance"- Avinash Ingole,Dr. R. C. Thool, International Journal of Advanced Research in Computer Science and Software Engineering 2013.

© 2014, IJARCSSE All Rights Reserved

[11] "Genetic algorithms for credit card fraud Detection"- Satvik Vats, Surya Kant Dubey, Naveen Kumar Pandey, Proceedings of the 2013 International Conference on Education and Educational Technologies.
[12] "Credit And ATM Card Fraud Detection Using Genetic Approach**"-**Pratiksha L. Meshram,Parul Bhanarkar, International Journal of Engineering Research & Technology, December- 2012.
[13] "Overview of Fraud Prevention & Management"- Rashmi G.Dukhi and Sandhya Dahake,National Conference on Innovative Paradigms in Engineering & Technology 2012.
[14] NG Pavlidis, DK Tasoulis, NM Adams and DJ Hand," Adaptive consumer credit classification "Journal of the Operational Research Society (2012).
[15] Linda Delamaire , Hussein Abdou , John Pointon ," Credit card fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2, 2009.

© 2014, IJARCSSE All Rights Reserved