Credit And ATM Card Fraud Detection Using Genetic Approach

Name:- Ms. Pratiksha L. Meshram
Institute:-Abha Gaikwad-patil college of Engg, Nagpur

Name:- Prof. Parul Bhanarkar
Institute:- Abha Gaikwad- patil C.O.E.. Nagpur

Abstract: - Along with great increase in credit & ATM Card transactions, credit & ATM card fraud has become increasingly rampant in recent years. The proposed paper work investigates that the efficacy of applying classification models to credit card fraud detection problems. The different techniques & classification methods, i.e. genetic algorithm, decision trees, neural network & logistic regression are tested for their applicability in counterfeit or fake detection. The proposed system provides a useful framework to detect & prevent a fraud & to choose the best model to recognize the credit & ATM card fraud risk. The newer proposals made in this paper are likely to have beneficial attributes in terms of cost savings & time efficiency by analyzing the human behavioral pattern & recognition of fraudulent patterns. This methodology uses the watermarking procedural technique to embed the thumb impression in magnetic strip of cash card which plays a prominent role to authenticate the user. This authentication mechanism is useful while transaction to secure cash card by asking secret question to user for verification in case of credit card & SMS feedback system for ATM transactions. This authentication mechanism is useful while transaction to secure cash card from being cloned via skimmed device& providing more security i.e. only by judging person only by its pin no.

Keywords: - Genetic Algorithm, Data mining, decision trees, Artificial Intelligence(AI), Neural Network, ADA Cost Algorithm.

Introduction

In present, scenario when the term fraud comes into a discussion, credit card follows in the banks and the financial frauds done by the cash card cloning & various frauds clicks to mind so far. With the great increase in credit cards, ATM CARDS & E- transactions, fraud has increasing excessively in recent years. Fraud detection includes analyzing of the spending behavior of users/customer order purpose, uncovering, or escaping of undesirable behavior. As credit card becomes the most general mode of payment or both online as well as regular purchase, fraud relate with it are also accelerate. Fraud detection is concerned with not only capturing the deceptive events, but also capturing of such activities as rapidly as possible. The use of credit cards is common in modern day society. Fraud is a millions dough business and it is rising every year. Fraud presents significant cost to our financial prudence measure world wide .Modern techniques based on Data mining, Machine learning, Sequence Alignment technique, Fuzzy Logic, Genetic Programming, Artificial Intelligence (AI) etc. ,has been introduced for detecting & preventing credit/ATM card, CHEQUE book type of fraudulent transactions. This project shows AI, IMAGE Processing & data mining techniques are used for fraud prevention there by implementing as/which ask secret questions i.e. ATM feedback SMS system with reply & by thumb impressions instead of detecting a fraud, a fraud can also be prevented. As per as the literature survey & analysis of paper in the field of artificial Intelligence(AI),Genetic algorithm, Neural network it has been analyzed & observed that the technologies are meant for fraud detection but not for prevention.

Fraud means obtaining services/goods and/or money by wrong means, and is a growing problem all over the world nowadays. Fraud deals with cases involving criminal purpose that, mostly, are difficult to identify. Credit & ATM cards are one of the most famous targets of fraud but not the only one; fraud can occur with any type of credit products, such as personal loans, home loans, and retail E-transactions. After some time there are different types of frauds seen as the Internet is playing very essential role in the online commerce. The transaction of data is the wheel of internet services. Today E-commerce application is widely used in E-business and various kinds of service industry where all kind of transaction of data is made possible through internet. It is one of the best, cheapest and convenient processes for online trade. Privacy and security is the basic concern in this kind of transaction. Privacy is handled by Cryptography but for security we have to apply techniques which are necessary to secure our transaction and the digitized data present in these transaction. Our approach is to enhance information security in the field of E-commerce, E-banking & ATM.

2. TYPES OF FRAUD

A range of types of scam in this paper include credit card frauds, telecommunication frauds, and computer intrusions, Bankruptcy fraud, Theft fraud/counterfeit fraud, Application fraud, Behavioral fraud.

2.1. Credit Card Fraud: Credit card fraud has been divided into two types: Offline fraud and On-line fraud.

2.1.1. Offline fraud is committed by using a stolen physical card at call center or any other place.

2.1.2. On-line fraud is committed via internet, phone, shopping, web, or in absence of card holder

Credit Card Fraud

Wondering United States, with its high number Credit Card transactions has minimum fraud rate. Ukraine tops the list with staggering 19% fraud rate closely followed by Indonesia at 18.3% fraud rate amongst the high risk countries facing Credit Card Fraud threat, some other countries are Yugoslavia (17.8%), Malaysia (5.9%). and Turkey (9%).Authorized users are permitted for credit card transactions by using the parameters such as credit card number, signatures, card holders address, expiry date etc. The unlawful use of card or card information without the knowledge of the owner itself and thus is an act of criminal deception refers to Credit card fraud. Credit card fraud detection is quite confidential and is not much disclosed publicly. Commonly used fraud detection methods are, rule-induction techniques, decision trees, Support Vector Machines (SVM), LR, ANNs and meta-heuristics such as, k-means clustering, genetic algorithms and nearest neighbor algorithms. Fraud is some kind of human behavior that relate to larceny, misinterpretation, misrepresent, unethical, craftiness false suggestions etc. Sometimes companies deal with millions of external parties, it is cost prohibitive to check the majority of the external parties‟ activities and identity manually. Certainly, for investigating each suspicious transaction, they incur a direct overhead cost for each of them. If in case, transaction amount is smaller than overhead cost, investigating is not worthwhile. Transaction involve among banking institutions offering financial transaction services, Logistics companies offering various kind of transportation services. These transactions contain sensitive information in the form of data so there must be a technique which is applied on these financial transactions. So our basic necessity is to achieve these basic goals of information security

A. *Privacy*: Information must be kept secret from unauthorized parties.

B. *Integrity*: Assurance that received data not contains any kind of alteration, addition, scoring through or replay.

C. *Authentication*: The assurance that the communication entity is the one that is claimed to be.

D. *Non-repudiation*: Sender and receiver prove their identities to each other.

E. *Access control*: This service controls that have access to a resource and under what condition access can occurs. The frequent use of plastic cash card is the most sensitive and vulnerable part of transaction system. It leads to the violation of all the above security issues and attracts skimmers. But the most important and prominent part is that when the costumer access the ATM machine for transaction.

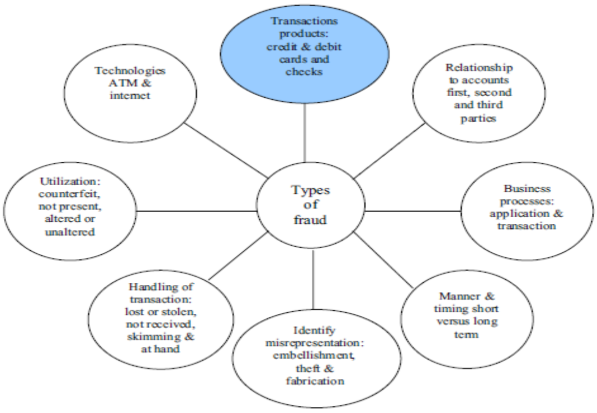

Transactions products: credit & debit cards and checks
Technologies ATM & internet
Relationship to accounts first, second and third parties
Utilization: counterfeit, not present, altered or unaltered
Types of fraud
Business processes: application & transaction
Handling of transaction: lost or stolen, not received, skimming & at hand
Identify misrepresentation: embellishment, theft & fabrication
Manner & timing short versus long term

Fig: Types Of Transaction & Frauds

CORELATED WORK ON CREDIT CARD SCAM DETECTION

Researchers developed many credit card fraud detection techniques based on data mining approach. **Ghosh and Rilly** have proposed credit card fraud detection with a three-layer approach, feed-forward neural network (FFNN), which requires long training time. **CARDWATCH:** presented by **Aleskerov** et al. proposed that a neural network based database mining system which was a prototype for database mining system developed for credit card fraud detection application and is concerned that it requires one network per customer. **Amalan Kundu** et al suggested a model BLAST-SSAHA Hybridization technique of credit card fraud by online detection. BLAST-SSAHA approach improves the fraud detection by combining both peculiarities as well as misuse detection techniques. **Phua** et al have done a major survey of existing data mining based Fraud Detection System (FDSs). **Chiu** et al have introduced web-services based collaborative scheme for fraud detection in the Banks. The proposed scenario supports the sharing of knowledge about fraud pattern with the participant banks in a heterogeneous and distributed environment. **Abhinav srivastava** et al have proposed Hidden Markov model (HMM) for credit card fraud detection which shows 80% accuracy over a large variation in the input data. **Syeda** et al have enhanced the speed by using equivalent coarse neural network of data mining and knowledge discovery process (KDP) for credit card fraud detection and achieve reasonable speed up to 10 processors only & more number of processors introduces load imbalance problem. Markov Model and time series are not scalable to large size data sets due to their time complexity. **Fan** et al recommend the application of distributed data mining in credit card fraud detection and improve the efficiency of highly distributed databases and detection system as this approach uses Boosting algorithm name Ada Cost. Ada Cost uses large number of classifiers and requires more computational resources during detection. **Brause** et al combine advanced data mining techniques and neural network algorithms**. Stolfo** et al intimate a credit card fraud detection system using various meta-learning techniques to learn models of fraudulent credit card transactions**.** To achieve high fraud detection along with low false alarm **Elkan** et al suggest Naïve Bayesian approach for credit card fraud detection. Further, **Elkan and Witten** presents that NB algorithm is very effective in many real world data sets as well as extremely capable in linear attributes. Bayesian networks were faster and accurate to train but are slower when applied to new instances/occurrence In a online system **Vatsa** et al. have currently proposed a game-theoretic approach to credit card fraud detection. . **Wen-Fang** have recommended a research on credit card swindle detection model which is based on outlier detection mining on distance sum, which shows that it can detect credit card fraud better than anomaly detection based on clustering. **Jianyun** et al have shows framework for detecting fraudulent transactions. In his paper work describes an FP tree based method to effectively create user profile for detection of fraud. But on the other hand, this technique doesn't be familiar with abnormal patterns i.e. short term behavioral changes of genuine card holders. Today, some of the existing credit card fraud detection techniques which use labeled data to train the classifiers are unable to detect new kinds of frauds. Supervised learning has some disadvantage, that they require human involvement to optimize parameters. On another hand, decision tree do not require any parameter setting from the user and can build faster compared to other techniques.

2. Research Challenges

The approach used in detect a credit card fraud mainly include neural network, data mining, meta-learning, ,AI, Genetic algorithm, game theory and support vector machine.
[1] Artificial neural networks (ANN) have been considered for credit card fraud detection by Ghosh and Reilly Aleskerov et al. and Dorronsoro et al. . Ghosh and Reilly carried out a feasibility study for Mellon Bank to determine the effectiveness.

Majority of the FDSs as described above show a lot of variation in their precision. The main dispute identified by most of them is that the vastness of the transactions flagged as fraudulent by the FDSs are in fact genuine. A significant amount of instant and money is exhausted by bankers in investigating a large number of legitimate cases. It also causes customer inconvenience and potential dissatisfaction. In credit card application, since occurrence of fraud is sparse, it involves detecting a relatively rare event from a very large collection of routine transactions. Meta-learning is a common strategy that provides a means for combining and integrating a number of separately learned classifiers or models. A meta-learning system allows financial institutions to share their models of fraudulent transactions by exchanging classifier agents.
[2]Stolfo et al. suggest a meta-learning technique to learn patterns of fraudulent credit card transactions. They apply four base classifiers, namely, ID3, CART, Bayes and RIPPER and use the class-combiner strategy [5] to select the best classifier for meta-learning. It has been made known that meta-learning with Bayes gives good accuracy.
[3]Prodromidis and Stolfo describe an artificial intelligence based approach that combines inductive learning algorithms and meta-learning methods to build accurate classification models for electronic fraud detection. The field of game theory has also been explored for credit card fraud detection.

[4]Liu and Li suggest a game-theoretic approach for prediction of attacks on IDS protected systems and a specific prediction model for credit card fraud. Vatsa et al. have modeled the interaction between an attacker and an FDS as a repeated game between two players, each trying to maximize its payoff. Such game-theoretic models make a number of assumptions, like availability of strategies, actions and payoffs to both the players, which are not often applicable in put into practice. For example, it is somewhat unusual for a bank to publicize its strategy for fraud detection.

Some survey papers have been published which categorize, compare and summarize articles in the area of fraud detection. Phua et al. did an extensive survey of data mining based FDSs and presented a comprehensive report. Kou et al. have reviewed the various fraud detection techniques including credit card fraud, telecommunication fraud as well as computer intrusion detection. Bolton and Hand describe the tools available for statistical fraud detection and areas in which fraud detection technologies are most commonly used. Majority of the FDSs as described above show a lot of variation in their accurateness. The main confront identified by most of them is that the bulk of the transactions flagged as fraudulent by the DSs are in fact genuine. A large amount of time and money is spent by bankers in investigating a large number of legitimate cases. It also causes customer inconvenience and potential dissatisfaction. In credit card application, since occurrence of fraud is sparse, it involves detecting a relatively rare event from a very large collection of routine transactions. Axels son has pointed out that due to the base-rate fallacy problem; the factor limiting the performance of an intrusion detection system is not the ability to identify intrusive behavior correctly but its ability to minimize false sound the alarm. While breakdown to detect a fraud causes direct loss to the company, follow up actions needed to pursue false alarms also tend to be costly. Any devise option that attempt to improve the rate of accurate detection of fraud, usually causes a rise in the false alarm as well. One of the motivations of our present research is to address this challenge.
It is well known that every cardholder has a certain shopping behavior, which establishes an activity profile for him. Almost all the existing fraud detection techniques try to capture these behavioral patterns as rules and check for any violation in subsequent transactions. However, these rules are largely stagnant in nature. As a result, they become ineffective when the cardholder develops new patterns of behavior that are not yet known to the FDS. The goal of a reliable detection system is to learn the behavior of users dynamically so as to minimize its own loss. Thus, systems that cannot develop or ''be trained", may soon become outdated resultant in large number of false sound the alarm. A impostor can also challenge new types of attack which should still get detected by the FDS. For example, a fraudster may aim at deriving maximum benefit either by making a few high value purchases or a large number of low value purchases in order to evade detection. Thus, there is a need for developing fraud detection systems which can integrate multiple evidences including patterns of genuine cardholders as well as that of fraudsters.

[5]Recent research for Credit Card Fraud Detection using Hidden Markov Model was done by Abhinav Ssrivastava, Amlan kundu, shamik saral, Arun mujumdar. A Hidden Markov Model is a double surrounded stochastic process with two hierarchy levels. It can be worn to model much more complex stochastic processes as compared to a traditional Markov model. HMM has a restricted set of states governed by a set of evolution probability. In a particular state, an

upshot or inspection can be generated according to an associated probability distribution. It is only the conclusion and not the state which is perceptible to an external spectator. But there were several problems related to the fraud detection using HMM (Hidden Markov Model). For the credit card fraud detection problem, DST is more relevant as compared to other fusion methods since it introduces a third option: ‘‘unrevealed”, which is the Hidden Markov Model & it doesn’t supports the same. Moreover it provides a rule for computing the confidence measures of three states of knowledge: fraud, fraud and suspicious (unknown) based on data from new as well as old evidence. Furthermore, in DST, evidence can be associated with multiple possible events unlike traditional probability theory where evidence is associated with only one event. This makes DST far more superior the HMM for credit card fraud detection. More recently, Syeda et al. have suggested the use of parallel granular neural Networks for speeding up the data mining and knowledge discovery process. Maes et al. have outlined an automated credit card fraud detection system by ANN as well as Bayesian belief networks (BBN). They show that BBN gives better results related to fraud detection and the training period is faster whereas the actual detection process is substantially faster with ANN. The neural network based methods are, in general, fast but not so accurate.The retraining of the neural networks is also a major log jam since the training time is quite high.

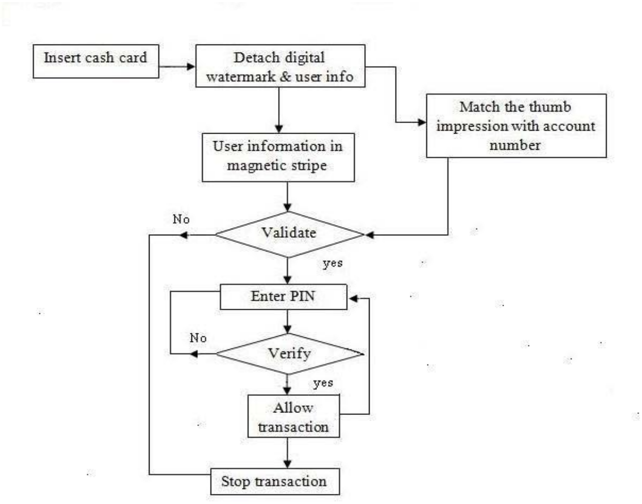
[6] Khayati Chaudhari,Jyoti yadav, Bhawna mallick GCET, noida:A review for fraud detection technique:

This represents a solution to fraud detection by monitoring spending behavioural patterns of customers & avoided it by implementing CARD WATCH , FDS & HMM except of cost based model which is further implementable.

[7] Linda delemaire (uk), join pointon(uk).This presents a framework for detecting fraud in personal loans & home loans & bankruptcy fraud.using a learned information from decision trees & genetic algorithm it can be further expanded for implementing suspicious scorecard on real datasets & its evaluation.

3. Proposed work

In the proposed system a cost model is developed for organization so logical level security is enhanced more by asking secret questions in case of credit card & SMS FEEDBACK system in case of ATM cards to implement it Genetic algorithm & neural network concept is used.


Insert cash card
Detach digital watermark & user info
Match the thumb impression with account number
User information in magnetic stripe
No
Validate
yes
Enter PIN
No
Verify
yes
Allow transaction
Stop transaction

4. Conclusion

In this project, we will propose a system which will find the exact user not only by its security pin no. for banks transaction but by asking secret question in case of credit card for judging the original user identification & SMS feedback system for ATM CARDS .To implement this genetic algorithm, neural network, ADA COST algorithm is useful for which Two filters are required for filtering the user database :Simple database filter for user info & credit card info. The Rule base filter is also required for updating the database of both user & credit card & analyzing transactional behavior patterns.

References:

[1]Aleskerov, E., Freisleben, B. & B Rao. 1997. ‘CARDWATCH: A Neural Network-Based Database Mining System for Credit Card Fraud Detection’, Proc. of the IEEE/IAFE on *Computational Intelligence for Financial Engineering*, 220-226.

[2]Anderson, R. 2007. *The Credit Scoring Toolkit: theory and practice for retail credit risk management and decision automation*. New York: Oxford University Press.

[3] APACS, Association for Payment Cleaning Services, no date. Card Fraud Facts and Figures Available at: http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html (Accessed: December 2007).

[4]Bellis, M. no date. Who Invented Credit Cards-the History of Credit Cards? Available at: http://inventors.about.com/od/cstartinventions/a/credit_cards.htm (Accessed: October 2008).

[5] Bentley, P., Kim, J., Jung. G. & J Choi. 2000. Fuzzy Darwinian Detection of Credit Card Fraud, Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society.

[6] Bolton, R. & Hand, D. 2002. 'Statistical Fraud Detection: A Review'. *Statistical Science*, 17; 235-249.

[7]Bolton, R. & Hand, D. 2001. Unsupervised Profiling Methods for Fraud Detection, Credit Scoring and Credit Control VII.

[8] Brause R., Langsdorf T. & M Hepp. 1999a. Credit card fraud detection by adaptive neural data mining, Internal Report 7/99 (J. W. Goethe-University, Computer Science Department, Frankfurt, Germany).

[9] Brause, R., Langsdorf, T. & M Hepp. 1999b. Neural Data Mining for Credit Card Fraud Detection, Proc. of 11th IEEE International Conference on Tools with Artificial Intelligence.

[10] Caminer, B. 1985. 'Credit card Fraud: The Neglected Crime'. *The Journal of Criminal Law and Criminology*, 76; 746-763.

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

[12] A. Shen, R. Tong, and Y. Deng, "Application of classification models on credit card fraud detection," June 2007.