ATM FRAUD TRANSACTION WITH USER BEHAVIOUR PATTERN

Dr.V.Vasanthi,
Assistant Professor,
Department of MCA, Hindusthan College of Arts and Science, Coimbatore
Manimaran M,
Department of MCA, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT:

Banking sector has been a vital institution that contributes immensely to the sustainability and maintenance of the economy in any country. The cases attributed to bank transaction can be negative when infused by intruders or fraudsters. Fraud detection in online banking transactions such as in Automated Teller Machine (ATM) is one of the important strategies implemented by banks to protect customer’s account. Fraud detection requires a lot of investments, complex algorithms, training and testing. Algorithm which gives out behavioral profiling of the user bank account and transactions. The generalization and classification ability satisfied only at 73 % level of fraud analysis. Fraudsters have untiring times making illegal moneys while the propose algorithm in this work will combat most efforts of illegalities regarding funds by electronic data processing (EDP) in the Banking sector; this will be achieved by data mining the bio-data though biometric combinational operations at the initial opening of the accounts and as such will conform with the algorithm proposed; the paper worked carefully using the existing literatures and systems to combine the approaches of biometric to the already existing ones and making a complete proposal for a design of ATM engine.The proposed system with STPM shows out a exact classification among exotic amount of EDP data with a level of 93% of accuracy. The sequential extraction marked out each and every transaction proceeded and shown out correctly.

INTRODUCTION

OVERVIEW OF THE PROJECT

Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. A few of many ways that money can be thieved from the credit card are Phishing, Pharming, Skimming and Dumpster driving. Hackers and fraudsters are becoming more sophisticated and skillful at manipulating internet protocol, web languages and tools to or discover any weakness that they can exploit. Thus the internet transaction fraud is 12 times higher than instore fraud.

Credit-card-based purchases can be categorized into two types: 1) physical card and 2) virtual card. In a physical-card- based purchase, the cardholder presents his card physically to merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company. In the second kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the "usual" spending

CREDIT CARD FRAUD PROBLEMS

The advancements in our technology and ease of availment opened more opportunities for fraudsters' ability to speed-up their execution plan and retain their anonymity at the same time. Surely, a layer of security will not be enough to protect the card holders, merchants, and issuing banks from a possible attack. There should be another layer that must be available to proactively detect these anomalies. Credit card fraud transpires when a perpetrator uses somebody's credit card for personal gain and sometimes in absolute secrecy or anonymity; even the issuing banks are unconscious that the card is being utilized. Moreover, the perpetrator has no relationship with the cardholder or issuer, and has no intention of informing the card owner of the lost card and making repayments for the transactions made.

Evaluation of credit card related fraud cases in the past two (2) decades reveals that the top five (5) modus-operandi performed by the fraudsters are: (i) counterfeit credit cards, (ii) lost or stolen, (iii) no-card fraud (e.g., giving card information to non-legitimate telemarketer), (iv) stolen cards during mailing fraud, and lastly (v) identity-theft fraud. These fraud cases occupy 81% of the known fraud types in the credit card industry. It may seem very common to the banks and merchants but to date, they are still being victimized by such attacks. The issue of fraud pertaining to credit cards is not new to the public and private sectors. In fact, numerous studies and researches have been carried-out to provide a novel and innovative ways in solving such problem.

ONLINE BANKING TRANSACTIONS

The problem of fraud is a serious issue in e-banking services that threaten credit card transactions especially. Fraud is an intentional deception with the purpose of obtaining financial gain or causing loss by implicit or explicit trick. Fraud is a public law violation in which the fraudster gains an unlawful advantage or causes unlawful damage. The estimation of amount of damage made by fraud activities indicates that fraud costs a very considerable sum of money. Credit card fraud is increasing significantly with the development of modern technology resulting in the loss of billions of dollars worldwide each year. Fraud detection involves identifying scarce fraud activities among numerous legitimate transactions as quickly as possible. Fraud detection methods are developing rapidly in order to adapt with new incoming fraudulent strategies across the world. But, development of new fraud detection techniques becomes more difficult due to the severe limitation of the ideas exchange in fraud detection. On the other hand, fraud detection is essentially a rare event problem, which has been variously called outlier analysis, anomaly detection, exception mining, mining rare classes, mining imbalanced data etc. The number of fraudulent transactions is usually a very low fraction of the total transactions. Hence the task of detecting fraud transactions in an accurate and efficient manner is fairly difficult and challengeable. Therefore, development of efficient methods which can distinguish rare fraud activities from billions of legitimate transaction seems essential.

DIFFICULTIES OF FRAUD DETECTION

Fraud detection systems are prune to several difficulties and challenges enumerated bellow. An effective fraud detection technique should have abilities to address these difficulties in order to achieve best performance.

Imbalanced data: The credit card fraud detection data has imbalanced nature. It means that very small percentages of all credit card transactions are fraudulent. This causes the detection of fraud transactions very difficult and imprecise.

Different misclassification importance: In fraud detection task, different misclassification errors have different importance. Misclassification of a normal transaction as fraud is not as harmful as detecting a fraud transaction as normal. Because in the first case the mistake in classification will be identified in further investigations.

Overlapping data: Many transactions may be considered fraudulent, while actually they are normal (false positive) and reversely, a fraudulent transaction may also seem to be legitimate (false negative). Hence obtaining low rate of false positive and false negatives is a key challenge of fraud detection systems.

Lack of adaptability: classification algorithms are usually faced with the problem of detecting new types of normal or fraudulent patterns. The supervised and unsupervised fraud detection systems are inefficient in detecting new patterns of normal and fraud behaviors, respectively.

Fraud detection cost: The system should take into account both the cost of fraudulent behavior that is detected and the cost of preventing it. For example, no revenue is obtained by stopping a fraudulent transaction of a few dollars.

Lack of standard metrics: there is no standard evaluation criterion for assessing and comparing the results of fraud detection systems.

VIRTUAL WORLD MACHINE LEARNING

In the virtual world, like that of banking transactions, knowing the user of a card, return to an authentication, a code or a phone number combined. However, each person has habits, preferences or even limits in his use of the credit card. For this, several researches are focused on the study of the behavior of the client or consumer to establish a known profile. In the field of fraud detection, the use of machine learning techniques (ML) is attractive for many reasons. First, they allow the discovery of patterns in large data streams, i.e. transactions arrive as a continuous stream and each transaction is defined by many variables. Second, fraudulent transactions are often correlated both in time and in space. For example, scammers usually attempt to commit fraud in the same store with cards within a short period of time. Third, machinelearning techniques can be used to detect and model existing fraudulent strategies and identify new strategies associated with cardholder behaviors

In credit card fraud detection system (CCFD), it is important in the analysis of a transaction to compute its risk factor in order to know which kind of analysis to carry out, whether deep or light. In a previous work we proposed an architecture of a credit card fraud detection system and we proposed a multilevel strategy for transaction classification. Notably, we proved the performance of the support vector machine (SVM) and bidirectional GRU (BiGRU) models at the classification level. Also the problems of unbalanced data were raised and dealt with in another work. The scope of this work of scoring cardholder’s behavior is not limited to an analysis of the customer profile, to give a score but also to evaluate the integration of the behavior layer in the whole process of credit card fraud detection system.

ONLINE TRANSACTION PATTERN MINING

An online transaction system includes several web applications and services to provide OLTP (OnLine Transaction Processing stages), FDS (Fraud Detection System), a database storing transaction data, and a database replication in order to provide minimum performance degradation on OLTP by backend data process or analysis. FDS is a backend process, whose impact on the front end of the online system is minimized, since it only talks to the replication database. Fraud Detection System consists of three major modules; (1) Data engine serves as an interface between the replication database and the FDS. It collects and pre-formats the recent transactions of all individual customers in the online system (2)The rule engine module mines the recent transactions to generate a profile, an association rule set stored in an FP-tree, for each user.(3)The rule monitor module monitors the new transaction for every user. Any new transaction of a particular user is compared against the FP-tree for that user to indicate the anomaly.

LITERATURE SURVEY

In [1] Credit card fraud and detection techniques: a review Banks and Bank Systems Linda Delamaire, Hussein Abdou and John Pointon 2009 Fraud is one of the major ethical issues in the credit card industry. The main aims are, firstly, to identify the different types of credit card fraud, and, secondly, to review alternative techniques that have been used in fraud detection. The sub-aim is to present, compare and analyze recently published findings in credit card fraud detection. This article defines common terms in credit card fraud and highlights key statistics and figures in this field. Depending on the type of fraud faced by banks or credit card companies, various measures can be adopted and implemented. The proposals made in this paper are likely to have beneficial attributes in terms of cost savings and time efficiency. The significance of the application of the techniques reviewed here is in the minimization of credit card fraud. Yet there are still ethical issues when genuine credit card customers are misclassified as fraudulent.

In [2] on Credit Card Fraud Detection Method Int. Conf. on Computer, Communication and Electrical Technology – ICCCET2011 Benson Edwin Raj S and Annie Portia A 2011 Analysis Due to the rise and rapid growth of E-Commerce, use of credit cards for online purchases has dramatically increased and it caused an explosion in the credit card fraud. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. Implementation of efficient fraud detection systems has thus become imperative for all credit card issuing banks to minimize their losses. Many modern techniques based on Artificial Intelligence, Data mining, Fuzzy logic, Machine learning, Sequence Alignment, Genetic Programming etc., has evolved in detecting various credit card fraudulent transactions. A clear understanding on all these approaches will certainly lead to an efficient credit card fraud detection system. This paper presents a survey of various techniques used in credit card fraud detection mechanisms and evaluates each methodology based on certain design criteria.

In [3] A review of Fraud Detection Techniques: Credit Card Khyati Chaudhary, Jyoti Yadav and Bhawna Mallick 2012 credit card fraud clicks to mind so far. With the great increase in credit card transactions, credit card fraud has increasing excessively in recent years. Fraud detection includes monitoring of the spending behavior of users/ customers in order to determination, detection, or avoidance of undesirable behavior. As credit card becomes the most prevailing mode of payment for both online as well as regular purchase, fraud relate with it are also accelerating. Fraud detection is concerned with not only capturing the fraudulent events, but also capturing of such activities as quickly as possible. The use of credit cards is common in modern day society. Fraud is a millions dollar business and it is rising every year. Fraud presents significant cost to our economy worldwide. Modern techniques based on Data mining, Machine learning, Sequence Alignment, Fuzzy Logic, Genetic Programming, Artificial Intelligence etc., has been introduced for detecting credit card fraudulent transactions. This paper shows how data mining techniques can be combined successfully to obtain a high fraud coverage combined with a low or high false alarm rate.

In [4] Credit Card Fraud Detection using Hidden Markov Model In modern retail market environment, electronic commerce has rapidly gained a lot of attention and also provides instantaneous transactions. In electronic commerce, credit card has become the most important means of payment due to fast development in information technology around the world. As the usage of credit card increases in the last decade, rate of fraudulent practices is also increasing every year. Existing fraud detection system may not be so much capable to reduce fraud transaction rate. Improvement in fraud detection practices has become essential to maintain existence of payment system. In this paper, we show how Hidden Markov Model

(HMM) is used to detect credit card fraud transaction with low false alarm. An HMM based system is initially studied spending profile of the card holder and followed by checking an incoming transaction against spending behavior of the card holder, if it is not accepted by our proposed HMM with sufficient probability, then it would be a fraudulent transaction.

In [5] Study of Hidden Markov Model in Credit Card Fraudulent Detection, Bhusari V and Patil S The most accepted payment mode is credit card for both online and offline in today’s world, it provides cashless shopping at every shop in all countries. It will be the most convenient way to do online shopping, paying bills etc. Hence, risks of fraud transaction using credit card has also been increasing. In the existing credit card fraud detection business processing system, fraudulent transaction will be detected after transaction is done. It is difficult to find out fraudulent and regarding loses will be barred by issuing authorities. Hidden Markov Model is the statistical tools for engineer and scientists to solve various problems. In this paper, it is shown that credit card fraud can be detected using Hidden Markov Model during transactions. Hidden Markov Model helps to obtain a high fraud coverage combined with a low false alarm rate.

EXISTING SYSTEM

EXISTING SYSTEM

The issue of fraud pertaining to credit cards is not new to the public and private sectors. In fact, numerous studies and researches have been carried-out to provide a novel and innovative ways in solving such problem. In retrospect, data-mining techniques are now well established. Nevertheless, researches pertaining to this area are very limited due to privacy issues. Bank customers are well protected by several laws that prohibit the disclosure of their personal information without proper consent. However, these papers were able to acquire data – their strategy is to combine information from customers, accounts, cards, and transaction datasets. This study will focus primarily on the transaction details made by the card holder. The intention of this study is to fully explore the effectiveness of utilizing the credit card transaction logs to differentiate anomalous from legitimate transactions. With this, various learning algorithms available in Weka will be evaluated by measuring their effectiveness in predicting the correct classification of the input dataset. Credit card fraud transpires when a perpetrator uses somebody's credit card for personal gain and sometimes in absolute secrecy or anonymity; even the issuing banks are unconscious that the card is being utilized. Moreover, the perpetrator has no relationship with the cardholder or issuer, and has no intention of informing the card owner of the lost card and making repayments for the transactions made

Disadvantages

- The accuracy level of the system is completely at low range
- The identification system is tends to give out efficient manner analysis
- The exact fraud classification are not given on real transactions

PROPOSED SYSTEM

PROPOSED METHOD

In the proposed system, banking sector has been a vital institution that contributes immensely to the sustainability and maintenance of the economy in any country. The cases attributed to bank transaction can be negative when infused by intruders or fraudsters. The proposed system on STPM algorithm exactly classifies the identification of the fraudulent made in the transactions**.** The detection of the fraud based traitors will be exactly classified with their problems. It facilitates cashless shopping everywhere in the world. It is the most widespread and reasonable approach with regards to web based shopping, paying bills, what's more, performing other related errands. Thus danger of fraud exchanges utilizing credit card has likewise been expanding. In the Current Fraud Detection framework, false exchange is recognized after the transaction is completed. As opposed to the current system, the proposed system presents a methodology which facilitates the detection of fraudulent exchanges while they are being processed, this is achieved by means of Behaviour and Locational Analysis(Neural Logic) which considers a cardholder's way of managing money and spending pattern. A deviation from such a pattern will then lead to the system classifying it as suspicious transaction and will then be handled accordingly

Advantages

- The classification works out with 94% accuracy system where the transaction maintenance is correct
- The identification of the transaction plotting is done
  The user plotting system is done with efficient planning system

MODULES DISCRIBTION

MODULES

- **DATASET COLLECTION**
- **DATA ACQUISITION**
- **PRE-PROCESSING**
- **ATTRIBUTE EXTRACTION**
- **BEHAVIORAL PATTERN CLASSIFICATION**
- **FRAUD DETECTION**

MODULE DESCRIPTION:

DATASET COLLECTION

A data set is a collection of related, discrete items of related data that may be accessed individually or in combination or managed as a whole entity. A data set is organized into some type of data structure. A dataset in machine learning is, quite simply, a collection of data pieces that can be treated by a computer as a single unit for analytic and prediction purposes. This means that the data collected should be made uniform and understandable for a machine that doesn't see data the same way as humans do

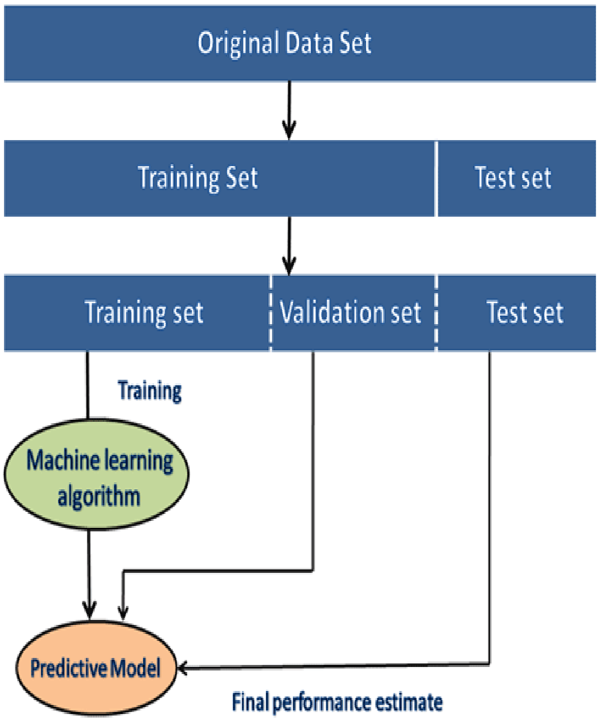


Fig 4.4 Dataset Creation

It is important that credit card companies are able to recognize fraudulent credit card transactions so that customers are not charged for items that they did not purchase.

The dataset contains transactions made by credit cards on real live cardholders. This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) account for 0.172% of all transactions.

It contains only numerical input variables which are the result of a SPTM transformation. Unfortunately, due to confidentiality issues, we cannot provide the original features and more background information about the data. Features V1, V2, … V28 are the principal components obtained with SPTM, the only features which have not been transformed with SPTM are 'Time' and 'Amount'. Feature 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature 'Amount' is the transaction Amount, this feature can be used for example-dependant cost-sensitive learning. Feature 'Class' is the response variable and it takes value 1 in case of fraud and 0 otherwise.

Given the class imbalance ratio, we recommend measuring the accuracy using the Area Under the Precision-Recall Curve (AUPRC). Confusion matrix accuracy is not meaningful for unbalanced classification.

DATA ACQUISITION

Data acquisition (commonly abbreviated as DAQ or DAS) is the process of sampling signals that measure real-world physical phenomena and converting them into a digital form that can be manipulated by a computer and software.

The systems, used for data acquisition are known as data acquisition systems. These data acquisition systems will perform the tasks such as conversion of data, storage of data, transmission of data and processing of data. Data acquisition systems consider the following analog signals.

PRE-PROCESSING

Data Preprocessing is a technique that is used to convert the raw data into a clean data set. In other words, whenever the data is gathered from different sources it is collected in raw format which is not feasible for the analysis.

Data preprocessing is the process of transforming raw data into a useful, understandable format. Real-world or raw data usually has inconsistent formatting, human errors, and can also be incomplete. Data preprocessing resolves such issues and makes datasets more complete and efficient to perform data analysis.

Preprocessing data is a common first step in the deep learning workflow to prepare raw data in a format that the network can accept. For example, you can resize data input to match the size of an image input layer. You can also preprocess data to enhance desired features or reduce artifacts that can bias the network.

ATTRIBUTE EXTRACTION

Attribute is an important type of semantic properties shared among different objects or activities. It is a representation in a higher level than the raw feature representation directly extracted from the credit card dataset. This system reduce the complexities will be reduce and the time extraction will be low with the system. With this considered, and to eliminate the issue of data imbalance, a new dataset was created to contain legitimate transactions based from the card/account included in the recorded fraud case report. The newly generated dataset has a total count of 9,992 records; 9,733 of which are legitimate and 259 are fraudulent. Although this setup comprises of 3% fraudulent and 97% legitimate transactions, later, this dataset will be manipulated to formulate new datasets with different class distribution – this will confirm the effectiveness of the classifiers under evaluation. For the meantime, the dataset for the model creation and evaluation stage will use a 25% fraud and 75% normal transaction type concoction.

Data in the transaction logs underwent several preprocessing tasks such as data-sanitation, normalization, binning, and handling null values. Prior to these activities, few attributes were removed from the dataset such as:

- Account number, card number - this will eliminate the possibility of having a customer centric model.
- Fields pertaining to dates - this will reduce the possibility of building a model focusing on date related events.
- And, control number pertaining to reported disputes this will eliminate the possibility of creating a model directly referencing to this control number since this field represents a potential fraud instance. Before the modeling and testing phase begin, a feature selection procedure was performed to evaluate the importance of each attributes of the transaction log

file. Furthermore, this will resolve the common issue of handling huge dimension of data the curse of dimensionality

BEHAVIORAL PATTERN CLASSIFICATION

To ensure a good behavior scoring we analyze the user profile. The feature engineer will define the client profile through his card transaction habits. Therefore, for each client we have the information of frequency of transaction by type, time range of purchases, number of transactions and the usual inter-transaction time gap. All of this information will be extracted from system database and stored in a duplicate database, to be used in our behavior analysis. The goal is to check if the user's profile is compatible with the behavior rules already stored in the rules database. For example, if the user has never been abroad and we receive a transaction from an automatic terminal machine (ATM) in foreign country, perhaps with an amount not expected. We will check the rules of our database and label this transaction as suspicious. We, note that the stored rules concerns the suspicious transaction behave. For each incoming transaction, we will check all stored rules, and a counter incremented for every respected rule, that mean suspected transaction, so the expression of score is: Score=number of rules respected/number of all rules If the score is equal 0, that mean the risk of the transaction behavior is null, but if the score is reaches 1, that mean this transaction behave have a high risk to be fraudulent.

The preferred distribution must be 50:50 to be able to produce the ideal model. With this considered, and to eliminate the issue of data imbalance, a new dataset was created to contain legitimate transactions based from the card/account included in the recorded fraud case report. The newly generated dataset has a total count of 9,992 records; 9,733 of which are legitimate and 259 are fraudulent. Although this setup comprises of 3% fraudulent and 97% legitimate transactions, later, this dataset will be manipulated to formulate new datasets with different class distribution – this will confirm the effectiveness of the classifiers under evaluation. For the meantime, the dataset for the model creation and evaluation stage will use a 25% fraud and 75% normal transaction type concoction.

FRAUD DETECTION

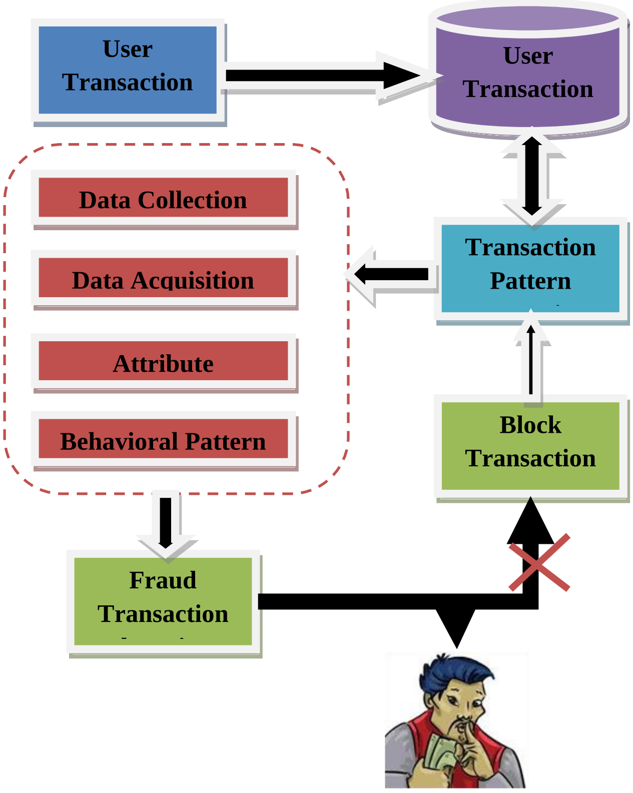
The fraud alert value is calculated by: AlertValue = ∑i=1 n-1(s(Ti) × f(Ti) × amount(Ti)), where Ti is a transaction in the accumulation window. **T**he output of FDS is an alert value indicating the suspicious level of analyzed transactions. Here, the number of states is three representing three clusters. This block generates synthetic transaction amounts for genuine cardholder. The values associated with STPM and IPD can be changed to capture the spending behavior of a cardholder properly

ALGORITHMS AND METHODS

System design is the process of planning a new system to complement or altogether replace the old system. The purpose of the design phase is to plan a solution for the problem. The phrase is the first step in moving from the problem domain to the solution domain. The design process also helps the programmer to decompose our project into various parts to complete to the work and separates the conceptual representation from the data structure.

METHODS

A two-dimensional diagram explains how data is processed and transferred in a system. The graphical depiction identifies each source of data and how it interacts with other data sources to reach a common output. Individuals seeking to draft a data flow diagram must identify external inputs and outputs, determine how the inputs and outputs relate to each other, and explain with graphics how these connections relate and what they result in. This type of diagram helps business development and design teams visualize how data is processed and identify or improve certain aspects.



EXPREMENTAL ANALYSIS

INPUT DESIGN

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider the input devices such as PC, MICR, OMR, etc. Therefore, the quality of system input determines the quality of system output. Well designed input forms and screens have following properties −

It should serve specific purpose effectively such as storing, recording, and retrieving the information.

- It ensures proper completion with accuracy.
- It should be easy to fill and straightforward.
- It should focus on user’s attention, consistency, and simplicity.

All these objectives are obtained using the knowledge of basic design principles regarding −

CREDITCARD
FRAUD
HOME
ADMIN
USER
Creditcard Fraud Detection
All rights reserved | Design by Admin
Activate Windows

OUTPUT DESIGN

The design of output is the most important task of any system. During output design, developers identify the type of outputs needed, and consider the necessary output controls and prototype report layouts. Manufacturers create and design external outputs for printers. External outputs enable the system to leave the trigger actions on the part of their recipients or confirm actions to their recipients.

Some of the external outputs are designed as turnaround outputs, which are implemented as a form and re-enter the system as an input.

FUTURE ENHANCEMENT

By further analysis of the two (2) classifiers by inducing randomness in the dataset revealed that J48 yielded a tight bound with respect to its variance in accuracy values. The fraud exchanges/transactions if the impostor is a new user in the bank because one of the pre-requisites for a neural network to work is having a lot of data to chew through since without the initial data input feed the neural networked cannot be trained or deployed.

CONCLUSION

Fraud analysis is of critical importance in the banking industry and the biggest challenge remains the cost of fraud, whether to analyze it, detect it or prevent it. Since transactions take place in real-time, require a process that consumes little time and is as efficient as the size and infrastructure of the financial institute that adapts it. In this paper, we presented our behavioral analysis to credit card fraud detection based on a hybrid methods using Apriori, rough set and fuzzy techniques that gave a promising results. The comparative study proved that our approach is the best combination to generate rules in a context where fraud remains low compared to legitimate transactions. The Proposed SPTM hopes that in the near future, this paper will be used as a reference by some banks or individuals to implement fraud detection system in the financial sector. Benefits of implementing such detection system will lessen the phone and SMS costs shouldered by the banks; instead of sending SMS transaction notifications to all customers, message will be sent to those customers with detected anomalous transaction. In the evaluation of classifiers during the model creation, the Random Tree produced the highest accuracy rate over J48.

REFERENCES

[1] Linda Delamaire, Hussein Abdou and John Pointon 2009 Credit card fraud and detection techniques: a review Banks and Bank Systems 4(2)

[2] Benson Edwin Raj S and Annie Portia A 2011 Analysis on Credit Card Fraud Detection Method Int. Conf. on Computer, Communication and Electrical Technology – ICCCET2011

[3] Khyati Chaudhary, Jyoti Yadav and Bhawna Mallick 2012 A review of Fraud Detection Techniques: Credit Card Int.J. of Computer Applications (0975 – 8887) 45

[4] Abhinav Srivastava, AmlanKundu, Shamik Sural and Arun K. Majumdar 2008 Credit Card Fraud Detection using Hidden Markov Model. IEEE Transactions on dependable and secure Computing 5 37-48

[5] Bhusari V and Patil S 2011 Study of Hidden Markov Model in Credit Card Fraudulent Detection Int. J. of Computer Applications 20

[6] Bhusari V and Patil S 2011 Study of Hidden Markov Model in Credit Card Fraudulent Detection.Int. J. of Computer Applications. 20