**International Journal of Multidisciplinary Research and Development**
**Online ISSN: 2349-4182, Print ISSN: 2349-5979; Impact Factor: RJIF 5.72**
**Received: 12-05-2019; Accepted: 14-06-2019**
**www.allsubjectjournal.com**
**Volume 6; Issue 8; August 2019; Page No. 53-58**

# Audit paper on credit card fraud detection

**Ishrat Jameel**
PG Department of Computer Science of Swami Vivekananda Institute of Technology, Affiliated to MRSPTU, Bathinda, Punjab, India

**Abstract**
Because of the dramatic increment of extortion which results in loss of dollars worldwide every year, a few present day procedures in recognizing misrepresentation are tenaciously developed and connected to numerous business fields. Extortion identification includes observing the exercises of populaces of clients so as to gauge, see or maintain a strategic distance from unwanted conduct. Unfortunate conduct is a wide term including wrongdoing, misrepresentation, interruption, and record defaulting.
This paper exhibits a review of current strategies utilized in Credit extortion location and media transmission extortion. The objective of this paper is to give an exhaustive audit of various strategies to recognize extortion.

**Keywords:** fraud detection, data mining, support vector machine, anomalies

## Introduction

Credit card extortion can be characterized as "Unapproved account action by an individual for which the record was not proposed. Operationally, this is an occasion for which move can be made to stop the maltreatment in advancement and consolidate hazard the executives practices to secure against comparable activities in the future". In straightforward terms, Credit Card Fraud is characterized as when an individual uses another person's Credit Card for individual reasons while the proprietor of the card and the card backer are most certainly not mindful of the way that the card is being utilized. What's more, the people utilizing the card has not under any condition having the association with the cardholder or the guarantor and has no goal of making the reimbursements for the buy they done. Extortion discovery includes recognizing Fraud as fast as conceivable once it has been executed. Extortion recognition strategies are ceaselessly created to protect crooks in adjusting to their methodologies.

The advancement of new extortion recognition strategies is made more troublesome because of the extreme impediment of the trade of thoughts in extortion discovery. Informational collections are not made accessible and results are regularly not uncovered to the general population. The misrepresentation cases must be distinguished from the accessible enormous informational indexes, for example, the logged information and client conduct. At present, misrepresentation identification has been actualized by a number of strategies, for example, information mining, measurements, and man-made consciousness. Misrepresentation is found from abnormalities in information and examples. The various kinds of strategies for submitting charge card cheats are portrayed underneath.

**Sorts of Frauds**: Various kinds of cheats in this paper incorporate charge card fakes, media transmission fakes, and PC interruptions, Bankruptcy misrepresentation, Theft misrepresentation/fake extortion, Application misrepresentation, Social misrepresentation [2].

**Credit card Fraud:** Credit card misrepresentation has been partitioned into two sorts:

(1) Offline misrepresentation and On-line extortion. Disconnected misrepresentation is submitted by utilizing a stolen physical card at call focus or some other place

(2). On-line extortion is submitted by means of web, telephone, shopping, web, or without card holder.

**Media transmission Fraud:** The utilization of media transmission administrations to submit different structures of extortion. Buyers, organizations and correspondence specialist co-op are the people in question.

**PC Intrusion:** Intrusion is Defined the demonstration of entering without warrant or welcome; that as signifies "potential probability of unapproved endeavour to get to Information, Manipulate Data Purposefully. Interlopers might be from any condition, an untouchable (Or Hacker) and an insider who knows the design of the framework [1].

**Bankruptcy Fraud:** This section canters around liquidation misrepresentation. Bankruptcy extortion methods utilizing a Credit card while being missing. Bankruptcy misrepresentation is a standout amongst the most convoluted sorts of extortion to foresee [1].

**Robbery Fraud/Counterfeit Fraud:** In this segment, we canter around robbery and fake misrepresentation, which are identified with one other. Burglary extortion alludes utilizing a card that isn't yours. When the proprietor gives a few criticism and contact the bank, the bank will take measures to check the cheat as right on time as could be expected under the circumstances. In like manner, fake misrepresentation happens when the credit card is utilized remotely; where just the Credit card subtleties are required [2].

**Application Fraud:** When somebody applies for a Credit card with false data that is named as application extortion. For distinguishing application extortion, two unique circumstances must be grouped. At the point when applications originate from an equivalent client with the equivalent subtleties, that is called copies, and when applications originate from various people with comparable

subtleties, that is named as personality fraudsters. Phua et al. [3] portrays application misrepresentation as "exhibition of personality wrongdoing, happens when application structures contain conceivable, and engineered (personality misrepresentation), or genuine yet in addition stolen character data (wholesale fraud)."

**Credit card misrepresentation location strategies**

On doing the writing overview of different strategies for misrepresentation recognition we arrive at the resolution that to distinguish charge card extortion there are numerous methodologies like [11, 2].

- Gass calculation
- Bayesian systems
- Hidden markov model
- Genetic calculation
- A combination approach utilizing dempster-shafer hypothesis and bayesian learning.
- Decision tree
- Neural system
- Logistic Regression

**Gass calculation**

This calculation is a mix of hereditary calculation and disperse search [11]. In this area, we initially depict the essential working standards of hereditary calculations and dissipate search and after that clarify the means of the proposed GASS calculation. Hereditary calculations are enlivened from characteristic development. The essential thought is that the survival shot of more grounded individuals from a populace is bigger than that of the more fragile individuals and as the ages develop the normal wellness of the populace shows signs of improvement. Typically, the new ages will be delivered by the hybrid of two parent individuals. In any case, in some cases a few irregular changes can likewise happen on people which thusly increment the assorted variety in the populace. It begins with various starting arrangements which go about as the guardians of the current age. New arrangements are created from these arrangements by the traverse and change administrators. The less fit individuals from this age are wiped out and the fitter individuals are chosen as the guardians for the people to come. This strategy is rehashed until a pre-determined number of ages have passed, and the best arrangement found up to that point is chosen. The SS is another developmental calculation which offers a few regular attributes with the GA. It works on a lot of arrangements, the reference set, by consolidating these answers for make new ones. The primary instrument for consolidating arrangements is with the end goal that a new arrangement is made from the straight mix of two different arrangements [21]. In SS assorted variety in the reference set is significant and next time it will be resolved again initial various best arrangements are chosen and afterward these are coupled with various most assorted answers for structure the new reference set. Not at all like the number of inhabitants in the GA, the reference set of SS is generally kept littler as every arrangement in it is wanted to be exposed to the recombination administrator. The proposed GASS calculation essentially pursues the means of GA however it has a few parts from SS. When contrasted with regular GA executions we kept the size of the populace littler and we ensured some base degree of decent variety is accomplished at every age. Additionally, for the multiplication we utilized a standard recombination administrator as opposed to the traditional traverse administrator of GA. We likewise utilized the change administrator which is basic to both GA and SS usage. The means of the GASS and the parameter esteems utilized are point by point underneath:

a. Number of parent arrangements (size of the reference set): Number of beginning arrangements which additionally equivalent to the quantity of guardians chose for every age is a significant parameter which can impact the combination speed of the methodology. The populace size is resolved as indicated by the size of the issue, for example greater populace for bigger issue. We have taken this to be 50 where three of them are resolved as to be the arrangements which will create the most extreme number of alarms (MAX), the one that will create the base number of alarms (MIN) what's more, the one as of now utilized in the generation (PRD). The rest of the 47 arrangements are gotten by delivering arbitrary numbers for every one of the 43 parameters. Note that, MAX and MIN bring a specific degree of assorted variety to the reference set.
b. Number of kids: For the simplicity of execution we chose to recombine each conceivable pair of guardians and along these lines we acquired 1225 kids in every age.
c. Reproduction (recombination): We took the weighted normal of the parameter estimations of the two parent arrangements and gotten the tyke arrangement. For every age a arbitrary number somewhere in the range of zero and one is decided and this number is utilized as the weight of the principal parent in all recombination administrators utilized in that age. The heaviness of the second parent is equivalent to one short the decided irregular number. This kind of propagation isn't basic in GA usage yet it tends to be viewed as an ordinary administrator for SS.
d. Mutation administrator: One of the 43 parameters is gotten arbitrarily and its worth is changed haphazardly inside its suitable range.
e. Recombination and change probabilities: All kids are created by the recombination administrator. At that point, one of the kids arrangements is haphazardly grabbed and change administrator is connected to it.
f. Fitness work: As portrayed over, the wellness estimation of an individual arrangement is resolved as the aggregate sum of investment funds caused from misrepresentation misfortunes.
g. Selection: The best three individuals from the age are naturally chosen. To keep having assorted variety in all ages, the three named arrangements, MAX, MIN and PRD are too naturally moved to the people to come. The rest of the 44 arrangements are dictated by the roulette determination strategy.
h. Termination paradigm: We chose to run the ages until no upgrades are watched for at any rate 10 ages.

**Bayesian systems**

With the end goal of extortion discovery, two Bayesian systems to depict the conduct of client are developed. Initial, a Bayesian system is developed to display conduct under the supposition that the client is fake (F) and another model under the supposition the client is a genuine (NF). The

'misrepresentation net' is set up by utilizing master information. The 'client net' is set up by utilizing information from non fake clients. During activity client net is adjusted to a particular client dependent on rising information. By embeddings proof in these organizes and spreading it through the system, the likelihood of the estimation x under two previously mentioned speculations is acquired. This implies, it offers decisions to what degree watched client conduct meets run of the mill false or non fake conduct. These amounts we call p(X | NF) and p (X | F). By hypothesizing the likelihood of extortion P (F) and P (NF) =1-P(F) as a rule and by applying Bayes' rule, it gives the likelihood of misrepresentation, given the estimation x,

$$P(F/X) = P(F)P(F/X) / P(X/F) \quad (1)$$

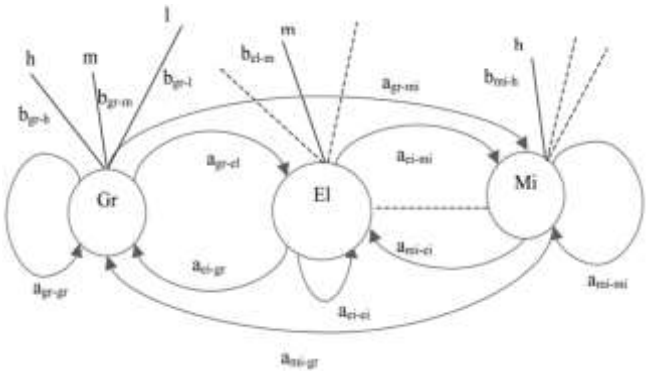
Where the denominator p(x) can be determined as

$$P(X) = P(F)\, P(X/F) + P(NF)\, P(N/XF) \quad (2)$$

The extortion likelihood P (F | X) given the watched client conduct x can be utilized as an alert level. On the one hand, Bayesian systems permit the reconciliation of master information, which we used to at first set up the models [4]. Then again, the client model is retrained in an unsupervised manner using data. Thus our Bayesian approach incorporates both, expert knowledge and learning.

**Hidden markov model**

A Hidden Markov Model is a double embedded stochastic process with used to model much more complicated stochastic processes as compared to a traditional Markov model. If an incoming credit card transaction is not accepted by the trained Hidden Markov Model with sufficiently high probability, it is considered to be fraudulent transactions. HMM [5], Baum Welch algorithm is used for training purpose and K-means algorithm for clustering. HMM sores data in the form of clusters depending on three price value ranges low, medium and high [6].




The probabilities of introductory arrangement of exchange have picked and FDS checks whether exchange is certifiable or deceitful. Since HMM keeps up a log for exchanges it lessens dull work of representative however creates high false alert just as high false positive [7]. The underlying decision of parameters influences the exhibition of this calculation and, subsequently, they ought to be picked cautiously. We consider the extraordinary instance of completely associated HMM in which each condition of the model can be come to in a solitary advance from each other state, as appeared in Fig. 2. Gr, El, Mi., and so on, are names given to the states to signify buy types like Groceries, Electronic things, and random buys. Spending profiles of the person cardholders are utilized to acquire an underlying appraisal for likelihood lattice B Hereditary Calculation Hereditary calculations, propelled from regular advancement were first presented by Holland (1975). Hereditary calculations are transformative calculations which point at acquiring better arrangements as time advances.

Extortion discovery issue is order issue, in which some of factual techniques numerous information mining calculations have proposed to settle it. Among choice trees are increasingly mainstream. Misrepresentation location has been ordinarily in space of Ecommerce, information mining [8]. GA is utilized in information digging chiefly for variable determination [9] and is for the most part combined with other DM calculations [10]. Furthermore, their mix with other systems has a generally excellent exhibition. GA has been utilized in charge card extortion identification for limiting the wrongly ordered number of exchanges [10]. Also, is simple available for PC programming language execution, along these lines, make it solid in Visa misrepresentation location. However, this technique has elite and is very costly.

A combination approach utilizing Dempster-Shafer hypothesis and Bayesian learning. As referenced in [19] First methodology for example Dempster- Shafer Theory essentially proposes Fraud Detection Framework utilizing data combination and Bayesian taking in which confirmations from current just as past conduct are consolidated together and contingent upon particular sort shopping conduct builds up an action profile for each cardholder. It has favorable circumstances like: - high precision, handling speed, decreases false caution, improves identification rate, relevant in E-trade. Be that as it may, one drawback of this methodology is that it is very costly Dempster–Shafer hypothesis and Bayesian learning is a half and half methodology for credit card extortion recognition [18, 11] which joins confirmations from current just as past conduct. Each cardholder has a specific sort of shopping conduct, which sets up an action profile for them. This approach proposes an extortion identification framework utilizing data combination and Bayesian learning of so as to counter Credit card misrepresentation.

The FDS framework comprises of four segments, to be specific, rule-based channel, Dempster–Shafer viper, exchange history database and Bayesian student. In the standard based segment, the doubt level of every approaching exchange dependent on the degree of its deviation from great example is resolved. Dempster–Shafer's hypothesis is utilized to join different such confirmations and an underlying conviction is figured [20]. At that point the underlying conviction esteems are joined to get a general conviction by applying Dempster–Shafer hypothesis. The exchange is named suspicious or suspicious relying upon this underlying conviction. When an exchange is observed to be suspicious, conviction is additionally reinforced or debilitated by its similitude with false or veritable exchange.

**Decision tree**

Decision trees are factual information mining strategy that express free traits and a ward qualities intelligently AND in

a tree formed structure. Characterization rules, removed from choice trees, are IF-THEN articulations and every one of the tests need to succeed if each standard is to be created [11]. Decision tree as a rule isolates the complex issue into numerous straightforward ones and resolves the sub issues through more than once utilizing [11, 12]. Decision trees are prescient choice help apparatuses that make mapping from perceptions to conceivable results. There are number of well-known classifiers build choice trees to create class models. Decision tree strategies C5.0, C&RT and CHAID. The work shows the benefits of applying the information mining strategies including choice trees what's more, SVMs to the Visa extortion recognition issue to diminish the bank's chance. The outcomes demonstrate that the proposed classifiers of C&RT and other choice tree approaches outflank SVM approaches in settling the issue under scrutiny.

**Neural Networks**

Misrepresentation discovery techniques dependent on neural system are the most prominent ones. A counterfeit neural arrange [13, 14] comprises of an interconnected gathering of counterfeit neurons .The rule of neural system is propelled by the elements of the cerebrum particularly design acknowledgment and cooperative memory [15]. The neural system perceives comparable examples, predicts future qualities or occasions in view of the cooperative memory of the examples it was found out. It is generally connected in arrangement what's more, grouping. The benefits of neural systems over different strategies are that these models are ready to gain from an earlier time and along these lines, improve results over the long haul. They can likewise concentrate rules furthermore, foresee future movement dependent on the current circumstance. By utilizing neural systems, viably, banks can recognize fake utilization of a card, quicker and all the more proficiently. Among the revealed charge card misrepresentation ponders generally have concentrated on utilizing neural systems. In additional useful terms neural networks are non-direct measurable information displaying apparatuses. They can be utilized to model complex connections among information sources and yields or to discover designs in information. There are two stages in neural networks [16] preparing and acknowledgment. Learning in a neural networks is called preparing. There are two sorts of NN preparing strategies managed and unsupervised. In managed preparing, tests of both deceitful what's more, non-false records are utilized to make models. Interestingly, unsupervised preparing just looks for those exchanges, which are generally divergent from the standard. On other hand, the unsupervised procedures needn't bother with the past learning of fake and non-deceitful exchanges in database. NNs can create best outcome for as it were enormous exchange dataset. What's more, they need a long preparing dataset.

**Logistic Regression**

Two propelled information mining approaches, support vector machines and irregular timberlands, together with the outstanding calculated relapse [18], as a component of an endeavor to more readily recognize (and subsequently control and indict) credit card extortion. The investigation depends on genuine information of exchanges from a universal

credit card activity. It is surely known, simple to use, and stays a standout amongst the most regularly utilized for information mining by and by. It in this manner gives a valuable benchmark for contrasting execution of more up to date strategies. Administered learning techniques for extortion identification face two difficulties. The first is of uneven class sizes of real and fake exchanges, with genuine exchanges far dwarfing fake ones. For model advancement, some type of examining among the two classes is normally used to acquire preparing information with sensible class appropriations. Different testing methodologies have been proposed in the writing, with arbitrary oversampling of minority class cases and arbitrary under testing of greater part class cases being the least difficult and most normal in use; others incorporate coordinated examining The second issue in creating administered models for misrepresentation can emerge from possibly undetected misrepresentation exchanges, prompting mislabeled cases in the information to be utilized for structure the model. For the reason of this investigation, fake exchanges are those explicitly distinguished by the institutional examiners as those that caused an unlawful exchange of assets from the bank supporting the credit cards. These exchanges were seen to be fake ex post. Our investigation depends on genuine information of exchanges from a worldwide credit card activity. The exchange information is amassed to make different inferred properties.

**Support vector machine**

The fundamental thought of SVM order calculation is to develop a hyper plane as the decision plane which making the separation between the positive also, negative mode greatest [17]. The quality of SVMs originates from two significant properties they have - piece portrayal and edge improvement. Portions, for example, outspread premise work (RBF) portion, can be utilized to learn complex areas. A part capacity speaks to the speck result of projections of two information focuses in a high dimensional component space. In SVMs, the characterization capacity is a hyper-plane isolating the various classes of information. The fundamental system finds the littlest hyper circle in the part space that contains all preparation examples, and afterward decides on which side of hyper circle a test example lies. In the event that a test example lies outside the hyper circle, it is affirmed to be doubt. SVM can have preferable forecast execution over BPN (Back proliferation arrange) in anticipating the future information.

SVMs are set of related directed learning techniques utilized for order and relapse they have a place with a group of summed up direct order. An exceptional property of SVM is, SVM Simultaneously limit the experimental grouping blunder and expand the geometric edge. So SVM called Maximum Margin Classifiers. SVM depends on the Structural hazard Minimization (SRM). SVM guide input vector to a higher dimensional space where a maximal isolating hyper plane is built. Two parallel hyper planes are built on each side of the hyper plane that different the information. The isolating hyper plane is the hyper planes that augment the separate between the two parallel hyper planes. An supposition that is made that the bigger the edge or separate between these parallel hyper planes the better the speculation mistake of the classifier will be. We consider information purposes of the structure {(X1, Y1), (X2, Y2), (X3 Y3), (X4, Y4)… … ., (Xn,, Yn)}.

Where Yn=1/ - 1, a consistent indicating the class to which

that point Xn has a place. n = number of test. Every X n is P - dimensional genuine vector. The scaling is critical to watch against variable (traits) with bigger differences. We can see this preparation information, by methods for the partitioning hyper plane, which takes W. X + b = O - (1) Where b is scalar and W is p-dimensional Vector. The vector W focuses opposite to the isolating hyper plane. Including the counterbalance parameter b enables us to increment the edge. Missing of b, the hyper plane is constrained to go through the starting point, confining the arrangement. As we are intriguing in the greatest edge, we are intrigued SVM and the parallel hyper planes [11]. Parallel hyper planes can be depicted by condition

$$W.X + b = 1$$

$$W.X + b = - 1$$

On the off chance that the preparation information are straightly distinct, we can select these hyper planes so that there are no focuses among them and after that attempt to amplify their separate.

**Random Forest**

The ubiquity of choice tree models in information mining emerges from their convenience, adaptability in terms of dealing with different information property types, and interpretability. Single tree models, be that as it may, can be flimsy and excessively delicate to explicit preparing information. Group strategies look to address this issue by building up a lot of models and totaling their forecasts in deciding the class name for an information point. An irregular woodland model is a troupe of order (or relapse) trees. Troupes perform well when person individuals are disparate, and irregular backwoods acquire variety among individual trees utilizing two sources for irregularity: first, each tree is based on independent bootstrapped tests of the preparation information; also, just a haphazardly chosen subset of information traits is considered at every hub in structure the individual trees. Irregular woods hence join the ideas of packing, where individual models in a gathering are created through inspecting with substitution from the preparation information, and the arbitrary subspace strategy, where each tree in a troupe is worked from an arbitrary subset of qualities. Given a preparing informational index of N cases portrayed by B properties, each tree in the group is created as pursues:

- Obtain a bootstrap test of N cases
- At every hub, haphazardly select a subset of bbB traits. Decide the best split at the hub from this diminished arrangement of b properties

- Grow the full tree without pruning

Irregular woodlands are computationally proficient since each tree is assembled freely of the others. With enormous number of trees in the outfit, they are moreover noted to be strong to over fitting and commotion in the information.

**Conclusion**

Debit card misrepresentation has turned out to be to an ever increasing extent wild as of late. To improve vendors', hazard the executives level in a programmed and powerful way, fabricating an exact and simple taking care of charge card hazard checking framework is one of the key assignments for the trader banks. One point of this investigation is to recognize the client model that best recognizes extortion cases. There are numerous methods for identification of Debit card extortion. In the event that one of these or mix of calculation is connected into bank debit card misrepresentation location framework, the likelihood of misrepresentation exchanges can be anticipated not long after charge card exchanges by the banks. What's more, an arrangement of against misrepresentation methodologies can be embraced to anticipate banks from incredible misfortunes previously and decrease dangers.

This paper gives commitment towards the successful methods for credit card fake identification.

**References**


1. Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK), "Credit card fraud and detection techniques: a review, Banks and Bank Systems. 2009; 4:2.
2. Khyati Chaudhary, Jyoti Yadav, Bhawn Mallick. A review of Fraud Detection Techniques: Credit Card, International Journal of Computer Applications (0975 – 8887), 2012, 45-1.
3. Vladimir Zaslavsky, Anna Strizhak. credit card fraud detection using self-organizing maps, information & security. An International Journal, Vol.18, 2006.
4. Mukhanov L. Using bayesian belief networks for credit card fraud detection, in Proc. of the IASTED International conference on Artificial Intelligence and Applications, Insbruck, Austria, 2008, 221-225.
5. Abhinav Srivastava, Amlan Kundu, Shamik Sural and Arun K. Majumdar, "Credit Card Fraud Detection Using Hidden Markov Model" IEEE, Transactions On Dependable and Secure Computing. 2008; 5:1.
6. Bhusari V, Patil S. Study of Hidden Markov Model in Credit Card Fraudulent Detection, International Journal of Computer Applications (0975 – 8887) Volume 20– No.5, 2011.
7. Bhusari V, Patil S. Study of Hidden Markov Model in Credit Card Fraudulent Detection, International Journal of Computer Applications (0975 - 8887) Volume 20- No. 5, 2011.
8. RamaKalyani K, Uma Devi D. Fraud Detection of Credit Card Payment System by Genetic Algorithm", International Journal of Scientific & Engineering Research. 2012; 3:7.
9. Bidgoli BM, Kashy D, Kortemeyer G, Punch WF. Predicting student performance: An Application of data mining methods with the educational webbased system LON-CAPA. In Proceedings of ASEE/IEEE frontiers in education conference, 2003.
10. Ekrem Duman, Hamdi Ozcelik M. Detecting credit card fraud by genetic algorithm and scatter search. Elsevier, Expert Systems with Applications. 2011; 38:13057-13063.
11. Benson Edwin Raj S, Annie Portia A. Analysis on Credit Card Fraud Detection Methods, International Conference on Computer, Communication and Electrical Technology – ICCCET2011, 18th & 19th, 2011.
12. Sahin Y, Duman E. Detecting Credit Card Fraud by Decision Trees and Support Vector Machines, International Multiconference of Engineers and computer scientists, 2011.

13. Benson Edwin Raj S, Annie Portia A. Analysis on Credit Card Fraud Detection Methods. IEEE-International Conference on Computer, Communication and Electrical Technology; 2011, 152-156.
14. Ray-I Chang, Liang-Bin Lai, Wen- De Su, Jen-Chieh Wang, Jen-Shiang Kouh. Intrusion Detection by Backpropagation Neural Networks with Sample-Query and Attribute-Query. Research India Publications, 2006, 6-10.
15. Raghavendra Patidar, Lokesh Sharma. Credit Card Fraud Detection Using Neural Network. International Journal of Soft Computing and Engineering (IJSCE). 2011; 1:32-38.
16. Tao Guo, Gui-Yang Li. Neural Data Mining For Credit Card Fraud Detection. IEEE, Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, 2008, 3630-3634.
17. Joseph King-Fung Pun. Improving Credit Card Fraud Detection using a Meta- Learning Strategy, Chemical Engineering and Applied Chemistry University of Toronto, 2011.
18. Siddhartha Bhattacharyya, Sanjeev Jha, Kurian Tharakunnel, Christopher Westland J. Data mining for credit card fraud: A comparative study, Decision Support Systems. 2011; 50:602 613.
19. Sandeep Pratap Singh, Shiv Shankar Shukla P, Nitin Rakesh, Vipin Tyagi. Problem Reduction in Online Payment System Using Hybrid Model International Journal of Managing Information Technology (IJMIT), 2011; 3:3.
20. Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun Majumdar K. Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning, Special Issue on Information Fusion in Computer Security. 2009; 10(4):354-363.
21. Hung WNN, Song X, Aboulhamid EM, Driscoll MA. BDD minimization by scatter search. IEEE Transactions on Computer- Aided Design on Integrated Circuits and Systems. 2002; 21(8):974-979.