ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Credit Card Fraud Detection Based on the Transaction by Using Data mining Techniques

B.Pushpalatha, C.Willson Joseph

Assistant Professor, Department of Computer Science, Karpagam University, Coimbatore, India

Assistant Professor, Department of Computer Science, Karpagam University, Coimbatore, India

ABSTRACT: Credit card fraud is rising significantly with the growth of recent technology and the global superhighways of communication. Credit card costs consumers and the financial company billions of dollars annually. The swindler continuously attempts to find new plan and procedure to commit illegal actions. Hence, fraud detection systems have become necessary for banks and financial institution, to reduce their losses. The most common techniques used to make the fraud detection model. Incidentally, detection and prevention of credit card frauds are one of the vital problems in the digital world that need exact transactions analysis. One method for detecting fraud is to check for suspicious changes in user behavior. The purpose of this paper is to investigate Data mining techniques like Bayesian networks, Bayes Minimum Risk, Genetic algorithm, Hidden markov model (HMM) and Ontology for improve fraud detection in credit cards. This work primarily aims to improve current fraud detection processes by improving the prediction of fraudulent accounts. Moreover, evaluation employed criterions in literature are collected and discussed. Consequently, open issues for credit card fraud detection are explained as guidelines for new researchers.

KEYWORDS: Credit Card Fraud, Types of fraud, Bayesian networks, Genetic algorithm, HMM, Ontology.

I. INTRODUCTION

Nowadays with the widening of credit cards along with online transactions, it is a significant problem for financial institutions in their attempt to prevent credit card fraud activities. There are a number of sundry methods for fraud can occur with any type of credit products such as tax evasion, illegal dealing of commodities, acquisition of loans via false information, money transfer under the head of fake business transactions, the donation to fake charity organizations, etc [1]. 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 [1]. This research addresses this problem by proposing an data mining algorithms for doubtful credit card transaction detection.

II. CREDIT CARD FRAUD

Credit card fraud detection is the process of monitoring the behavior of the customers‟ transaction level through a period of time [2].

Types of Credit Card Fraud:

- The first type which is the most common is the application fraud. The individual will falsify an application to acquire a credit card. The individual will give false information about his/her financial status in order to receive a credit card.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

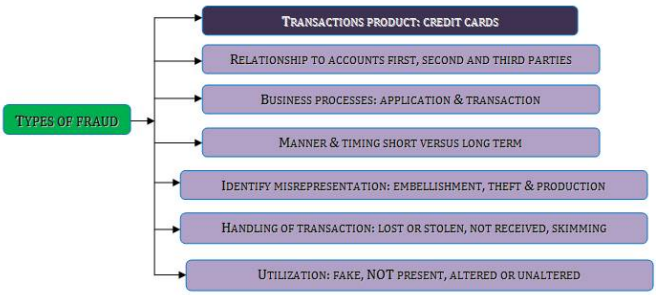

Fig.1. Types of fraud

- The second type is assumed identity. Assuming someone's identity has been in the long-run form for credit card fraud. The individual will falsify a name with a temporary address.
- The third type is financial fraud which happens when an individual wishes to gain more credit than he/she currently has. They will apply for a credit card under their own name, but the information regarding their financial status will be false.
- The fourth is skimming technology. Magnetic card skimming is a small handheld device with the sole purpose of collecting and storing the information on any credit card [2].
- The fifth type is never received issue. This type of credit card fraud involves the theft of the card while still in transit

III. CREDIT CARD FRAUD DETECTION METHODS

As of literature survey a variety of methods for fraud detection. Finally, we come to conclude that to detect credit card fraud there are multiple approaches like [3].

1. Bayesian networks
2. Bayes Minimum Risk
3. Genetic algorithm
4. Hidden markov model
5. Ontology

The data mining includes the various techniques and their properties that can be used to detect credit fraud. More details can be found in following section [3].

1. Bayesian networks

Bayesian Network is a Directed Acyclic Graph, where each node represents a random variable and is associated with the conditional probability of the node given its parents. This model shows each variable in a given domain as a node in the graph and dependencies between these variables as arcs connecting the respective nodes. That is, all the edges in the graphical model are directed and there are no cycles [4]. For the purpose of fraud detection, Bayesian networks have to be describing the behavior of auto insurance. First, a Bayesian network is constructed to model behavior under the assumption that the driver is fraudulent (F) and another model under the assumption the driver is a legitimate user (NF). The 'fraud net' is set up by using expert knowledge. The 'user net' is set up by using data from non fraudulent users. During operation user net is adapted to a specific user based on emerging data. By inserting evidence in these networks and propagating it through the network, the probability of the measurement x less than two above mentioned hypotheses is obtained. This means, it gives judgments to what degree observed user behavior meets typical fraudulent or non fraudulent behavior. These quantities we call $p(x \mid NF)$ and $p(x \mid F)$. By postulating the probability of fraud P (F) and P (NF) = 1-P(F) in general and by applying Bayes' rule, it gives the probability of fraud, given the measurement x,

$$P(F \mid x) = \frac{P(F)\, p(x \mid F)}{p(x)}$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Where the denominator p(x) can be calculated as

$$P(x) = P(F)\, p(x \mid F) + P(NF)\, p(x \mid NF)$$

The fraud probability P (F | x) given the observed user behavior x can be used as an alarm level. On the one hand, Bayesian networks allow the integration of expert knowledge, which we used to initially set up the models [5]. On the other hand, the user model is retrained in an unsupervised way using data. Thus our Bayesian approach incorporates both, expert knowledge and learning.

2. Bayes Minimum Risk

Bayes minimum risk as a method for cost sensitive credit card fraud detection. As defined in [12], the Bayes minimum risk classifier is a decision model based on quantifying tradeoffs between various decisions using probabilities and the costs that accompany such decisions. In the case of credit card fraud detection, there are two decisions; either predicts a transaction as fraud p_f or as legitimate p_l The risk associated with predicting a transaction as fraud is defined as

$$R(pf|x) = L(pf|yf)P(pf|x) + L(pf|yl)P(pl|x),$$

and when the transaction is predicted as legitimate it is

$$R(pl|x) = L(pl|yl)P(pl|x) + L(pl|yf)P(pf|x),$$

where y_f and y_l are the real labels for fraudulent and legitimate transactions respectively. $P(p_l|x)$ is the estimated probability of a transaction being legitimate given x, similarly $P(p_f|x)$ is the probability of a transaction being fraud given x. Finally $L(a, b)$ is the loss function when a transaction is predicted as a and the real label is b. Once both risks are calculated, a transaction is classified as fraud if $R(p_f|x) \leq R(p_l|x)$, meaning if the risk associated with that decision is lower than the risk associated with classifying it as legitimate. Confusion Matrix of a Binary Classification System [6]:

		True Class (y_i)	
		Fraud	Legitimate
Predicted Class (p)	Fraud	TP	FP
	Legitimate	FN	TN

Table I

		True Class (y_i)	
		Fraud	Legitimate
Predicted Class (p)	Fraud	C_a	C_a
	Legitimate	$100 \cdot C_a$	0

Table II

		True Class (y_i)	
		Fraud	Legitimate
Predicted Class (p_i)	Fraud	C_a	C_a
	Legitimate	Amt_i	0

Table III

Since in the credit card fraud detection case the losses are equal to the cost, first we use the cost matrix with fixed cost for FN as defined in Table II [6]. Then a transaction will be classified as fraud if:

$$C_a P(pf|x) + C_a P(pl|x) \leq 100 \cdot C_a P(pf|x)$$

and as legitimate otherwise. Lastly, we test while using the proposed cost matrix with real financial costs as in Table III. A transaction will be classified as fraud if the following condition is true:

$$CaP(pf|x) + CaP(pl|x) \leq AmtiP(pf|x)$$

and as legitimate if false [7].

3. Genetic Algorithm

Genetic algorithms are evolutionary algorithms which aim at obtaining better solutions as time progresses. Following figure shows the flow of Genetic Algorithm process. The best solution using genetic algorithm is found by repeating this procedure until a pre-specified numbers of generations have passed. To get a better performance, a parametric procedure needs to be undertaken where list of the parameters and the settings are needed to generate fraud transaction.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

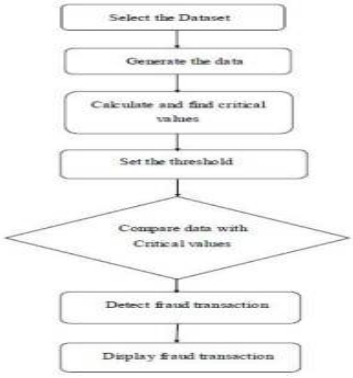

Fig. 2. Flow of Genetic Algorithm Process

In this paper discovery of credit fraud is based on customer behavioral variables. The Sample data set has been considered for the generating the fraud transactions and discovery of fraud in the electronic payment systems. The various parameters involved in the data set are as follows:

- C_Freq – Frequency of Credit Card used,
- C_Loc – Location at which Credit Card are in the hands of fraudulent,
- C_OD – Rate of Over Draft time,
- C_BB – Balance available at the Bank of Credit Card,
- C_Ds – Average Daily spending amount.

Data Set, T= {t1, t2, t3… tn} D - One data object, D € T If p parts of data set named P such that P € T and is far away from object D, then D is considered to be a common object. The proposed system overcomes the credit card fraud in an efficient way using genetic algorithm through which the false alert is minimized and it produces an optimized result. In the proposed system fraud is discovered based on customer's behaviour. A new classification problem which has a variable misclassification cost is introduced [8]. Hence the genetic algorithms is made where a set of interval valued parameters are optimized. The number of true can be maximized by determining the current values of the parameters C_Freq, C_Loc, C_OD, C_BB, and C_Ds and then the critical values are compared with the data set parameters provided that the numbers of alerts do not exceed a certain level.

The Experiment process is carried out with four steps:-

Step 1: Group of data credit card transactions as input with every transaction record with n attributes, and standardizes the data, get the sample finally, which includes the confidential information about the card holder, store in the data set.
Step 2: Calculate the critical values, C_Freq, C_Loc, C_OD, C_BB and C_Ds.
Step 3: After limited number of generations find the critical values.
Step 4: Discover fraud transactions using this algorithm. This process and detection procedure analyzes the feasibility of credit card fraud detection based on critical values.

In this study with the given sample data set fraud discovery and fraud transactions are generated. With the help of this algorithm the probability of fraudulent transactions can be predicted soon after credit card transactions by the banks with a series of anti-fraud strategies can be adopted to reduce risks and to prevent banks from great losses [9].

4. Hidden markov model (HMM)

Hidden Markov Model is probably the simplest and easiest models which can be used to model sequential data, i.e. data samples which are dependent from each other. An HMM is a double embedded random process with two different levels, one is hidden and other is open to all. The Hidden Markov Model is a finite set of states, each of which is associated with a probability distribution. Transitions among the states are governed by a set of probabilities called

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

transition probabilities. In a particular state an outcome or observation can be generated, according to the associated probability distribution. It is only the outcome, not the state visible to an external observer and therefore states are "hidden" to the outside; hence the name Hidden Markov Model [10, 11].

HMM has been successfully applied to many applications such as speech recognition, robotics, bio-informatics, data mining etc [12, 13].

In order to define an HMM completely, following elements are needed.

• The number of states of the model, N. We denote the set of states S = {S1; S2; S3; . . SN}, where i =1; 2; . . .; N, is a number of state and Si , is an individual state. The state at time instant t is denoted by qt .
• The number of observation symbols in the alphabet, M. If the observations are continuous then M is infinite. We denote the set of symbols V = {V1; V2; . . . VM} where Vi , is an individual symbol for a finite value of M.

$$\Lambda = \{aij\}$$

• A set of state transition probabilities.

$$a_{ij} = P\{q_{t+1} = S_j \mid q_t = S_i\},\ 1 \le i, j \le N,$$

Where q_t denotes the current state, Transition probabilities should satisfy the normal stochastic constraints,

$$a_{ij} \ge 0,\ 1 \le i, j \le N$$

And

$$\sum_{j=1}^{N} a_{ij} = 1,\ \ 1 \le i \le N,$$

• The observation symbol probability matrix B,

$$B = \{b_j(k)\}$$

A probability distribution in each of the states,

$$b_j(k) = P\{a_t = V_k \mid q_t = S_j\},\ 1 \le j \le N,\ 1 \le k \le M$$

Where, V_k denotes the k^{th} observation symbol in the alphabet, and a_t the current parameter vector. Following stochastic constraints must be satisfied.

$$b_j(k) \ge 0,\ 1 \le j \le N,\ 1 \le k \le M \text{ and}$$

$$M \sum bj\,(k) = 1,\ 1 \le j \le N$$

If the observations are continuous then we will have to use a continuous probability density function, instead of a set of discrete probabilities. In this case we specify the parameters of the probability density function. Usually the probability density is approximated by a weighted sum of *M* Gaussian distributions $\mathcal{N}$,

$$b_j(a_t) = \sum c_{jm}\ \mathcal{N}(\mu_{jm}, \sum jm, a_t)$$

Where,
c_{jm} = weighting coefficients,
μ_{jm} = mean vectors,
$\sum_{jm}$ = Covariance matrices
c_{jm} should satisfy the stochastic constrains,

$$c_{jm} \ge 0,\ 1 \le j \le N,\ \ 1 \le m \le M$$

And

$$\sum_{m=1}^{M} c_{jm} = 1,\ \ 1 \le j \le N$$

- The initial state distribution, $\Pi = \{\Pi_i\}$ where,

$$\Pi_i = P\{q_i = S_i\},\ 1 \le i \le N$$

$$\sum_{i=1}^{N} \Pi_i = 1$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Therefore we can use the compact notation

$$\lambda = (\Lambda, B, \Pi)$$

To denote an HMM with discrete probability distributions, while

$$\lambda = (\Lambda, c_{jm}, \mu_{jm}, \sum jm, \Pi)$$

to denote one with continuous densities.

- Hidden Markov Model assumes that current output (observation) is statistically independent of the previous outputs (observations). We can formulate this assumption mathematically, by considering a sequence of observations,

$$O = O_1, O_2, O_3, \ldots O_R,$$

$$Q = q_1, q_2, q_3 \ldots\ldots q_R,$$

Where R, is a number of observation in the sequence and Q, is a one particular sequence.

- Then according to the assumption for an HMM, probability that O is generated from this state sequence is given by

$$P\{O|q_1,q_2,q_3,\ldots q_R, \lambda\} = \prod_{t=1}^{R} P(O_t|q_t, \lambda)$$

$$P(O|Q,\lambda) = b_{q1}(O_1).b_{q2}(O_2)\ldots\ldots b_{qR}(O_R).$$

Thus, the probability of generation of the observation sequence O by the HMM with respect to λ will be written as follows:

$$P(O|\lambda) = \sum_{All\ Q} P(O|Q, \lambda).P(Q|\lambda).$$

Calculation of probability $P(O|\lambda)$ is an intensive computing process. Hence, a forward backward algorithm [14] is used to calculate probability $P(O|\lambda)$.

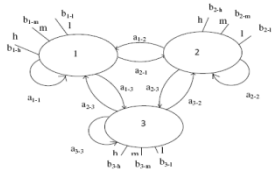

Fig. 3: Transition of different states in HMM

5. *Ontology*

Ontology is widely defined as “a specification of a conceptualization”. Conceptualization refers to the “abstract, simplified view of the world”. A specific real-world domain can be represented at a higher level of abstraction using ontologies. Therefore ontology can be seen as a formal representation of concepts along with their relationships [15]. It can express semantics in a much richer way than other representation models. Ontologies consist of classes, their instances and properties between these instances. They also use logic languages like first order logic or description logic to formalize axioms and increase their expressiveness. They are widely used in the area of Semantic Web to express meaning.

1	***Individuals***	Individuals also known as instances. It can be seen as the objects of the conceptualized domain.
2	***Classes***	The classes of ontology are the “sets that contain individuals”. A class ‘c’ consists of formal mathematical statements which describe the conditions which an individual needs to satisfy for being member of ‘c’. Similar to object oriented programming. A class may have a number of subclasses.
3	***Properties***	The properties are simply the relations between two individuals.

Table IV. Classes, Properties and Individuals of Ontology

Ontologies are content theories about the classes of individuals, properties of individuals, and relations between individuals that are possible in a specified domain of knowledge. They define the terms for describing our knowledge about the domain. An ontology of a domain is beneficial in establishing a common vocabulary for the describing the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

domain of interest. This is important for unification and sharing of knowledge about the domain and connecting with other domains [15] [16].

Ontology algorithm

Generally, every concept in ontology has its explicit definition which is sufficiently detailed to capture the semantics of the domain. In our paper, four kinds of elementary factors are used to distinguish a concept within an ontology and they are concept name (N), property (P), instance (I), and relation (R). Since N, P, I are features related only with the concept, and R are features related the concept with another one, these four kinds of features can be classified as two kinds: intension for local information and extension for global information [17].

Definition 1: Intension of a concept c is defined as a tuple $InTc$:□□(n_c, P_c, I_c) , which describes the essence features of the concept, where

- n_c is a name of the concept c . Every concept has only one distinctive name.
- P_c is a set of properties related with the concept.
- I_c is a set of instances associated with the concept.

Definition 2: Extension of a concept c is defined as ExT_c :□□R_c , which profiles the structural property of the concept by its relations with other concepts, i.e. determines situation of the concept in the whole ontology, where

- R_c is a set of relations that related the concept with other concepts in the ontology [18].

Definition 3: An ontology with k concepts is modeled as a tuple OM :□□□V_c, $OntoInT_{Vc}$ $OntoExT_{Vc}$) , where C□□$c_i|1\leq i \leq k$ } is concept set of the ontology, and c_i is one concept in the ontology, such that:

- V_c □ vci□vci□□i,$1\leq i \leq k$□□is a set of sequence number of concept. Where v ci denotes that the ith concept in the ontology is ranked with a sequence number of i ;

- $OntoInT_{Vc}$ = { vci , $Ttype$, xci>} is a set of intensional features of the ontology, where $1\leq i \leq k$, $Type$ □□{'N','P',' I '} and { vci , $Ttype$, xci>} =

$$\begin{cases} < v_{c_i}, 'N', n_{c_i} > & \text{if } Type='N' \\ < v_{c_i}, 'P', p_{c_i} > \; p_{c_i} \in P_{c_i} & \text{if } Type='P' \\ < v_{c_i}, 'I', i_{c_i} > \; i_{c_i} \in I_{c_i} & \text{if } Type='I' \end{cases}$$

- $OntoExT_{Vc}$ = □□ vci□vci ,$Type$,r_{ij} >} is a set of extensional features of the ontology, Where $1\leq i \leq k$, $Type$ □'R', r_{ij} ∈ Rci and , < vci , vci ,' R', r_{ij} > represents that there exists a relationship from concept c_i to concept c_j .

Definition 4: An overall feature set of an ontology F_0 is defined as a combination of the intensional features set $OntoInT_{Vc}$ and the extensional features set

$OntoExT_{Vc}$, that is, $F_O = OntoInT_{Vc} \cup OntoExT_{Vc}$

Definition 5: Mapping function M: Vc->V'_c□is defined as a mapping from one ontology O_1 to another ontology O_2, in which V_C is the sequence number set in O_1, and V'_C□□is the sequence number set in O_2 [18].

As defined in Definition5, a mapping is a correspondence relationship between the taxonomies of two given ontologies. It states that any of concepts in O_1 should have a corresponding concept in O_2, and two different concepts in O_1 may correspond to the same concept in O_2.

IV. OBSERVATION AND ANALYSIS ON EXISTING SYSTEM

Research Reference	Investigated Method	Accuracy
[4], [5]	Bayesian networks	90.3%
[6]3	Bayes Minimum Risk	97.8%
[8],[9]	Genetic algorithm	89.27-94.14%
[10-14]	Hidden markov model	95.64-98.09%
[15 - 18]	Ontology	95.5-99.6%

Table V. Accuracy results for fraud detection practices

Most of the research showed a large difference between each method's sensitivity and specificity results. Modern techniques like Bayesian networks, Bayes Minimum Risk, Genetic algorithm, Hidden markov model and Ontology are

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

elucidated in this table. Table V and Fig 4 illustrates the accuracy results for fraud detection practices for above mentioned methods.

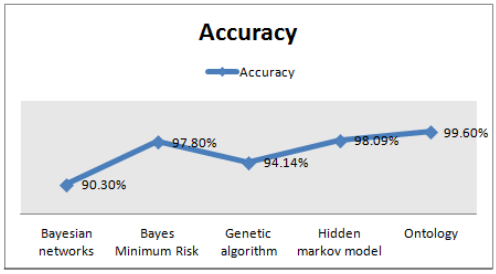

Fig. 4: Accuracy graph for fraud detection techniques

Techniques	Advantages	Disadvantages
Bayesian Network	High processing and detection speed/high accuracy	Excessive training need/ Expensive [19]
Bayes Minimum Risk	Estimates converge towards correct values with enough data	Histogram becomes big with high dimension so requires too much data
Genetic Algorithm	Works well with noisy data/easy to integrate with other systems/ usually combined into other techniques to increase the performance of those techniques and optimize their parameters/ easy in build and operate/In expensive/fast in detection/ Adaptability/Maintainability/knowledge discovery and data miming	Requires extensive tool knowledge to set up and operate and difficult to understand [19]
Hidden Markov Model	Fast in detection	Highly expensive/ low accuracy/not scalable to large size data sets [19]
Ontology	This method is detecting fraudulent transactions online and offline and fraud detection is their being real-time and high accuracy.	It is high computational overload and time-consuming detection process because of using all legal and illegal acts performed by a user through registered history of transactions in a system [20]

Table VI. Advantages and disadvantages of fraud detection methods

V. CONCLUSION

These days one of the biggest threats to commercial institutes is fraud in credit cards. Understanding of fraud mechanism for fighting back its effects is subsequently a necessarily salient task. This paper explains the approach to credit card fraud detection using data mining system by monitoring individual transactions. The findings in this work highlight the fraud detection improvement that a learning strategy can provide when it is used in conjunction with an established fraud detection system. This paper has examined various data mining techniques like Bayesian networks, Bayes Minimum Risk, Genetic algorithm, Hidden markov model and Ontology which have the potential to aid the credit card fraud detection. Table V present the selected data mining techniques among the existing systems and also display the finding rate of fraud detection.

REFERENCES

1. Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK) "Credit card fraud and detection techniques: a review:" Banks and Bank Systems, Volume 4, Issue 2, 2009.
2. Manjunath K.V, Patharaju S.D"Data Mining for Fraud Detection" ijarcsse, Volume 5, Issue 8, August 2015, ISSN: 2277 128X.
3. Khyati Chaudhary, Jyoti Yadav, Bhawna Mallick, "A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications (0975 – 8887) Volume 45– No.1, May 2012.
4. David Heckerman , Redmond "Bayesian Networks for Data Mining"Journal Data Mining and Knowledge Discovery, Volume 1 Issue 1, 1997
5. L. Mukhanov, "Using bayesian belief networks for credit card fraud detection," in Proc. of the IASTED International conference on Artificial Intelligence and Applications, Insbruck, Austria, Feb. 2008, pp. 221– 225.
6. C. Elkan, "The Foundations of Cost-Sensitive Learning," in Seventeenth International Joint Conference on Artificial Intelligence, 2001, pp. 973–978.
7. Alejandro Correa Bahnsen, Aleksandar Stojanovic, Djamila Aouada and Bj¨orn Ottersten "Cost Sensitive Credit Card Fraud Detection using Bayes Minimum Risk" 12th International Conference on Machine Learning and Applications, 2013 IEEE
8. M. Hamdi Ozcelik, Mine Isik, Ekrem Duman, Tugba Cevik, 2010, "Improving a credit card fraud detection system using genetic algorithm", IEEE International Conference on Networking and Information, 436-437
9. Mayuri Agrawal, Sonali Rangdale "Discovering Fraud in Credit Card by Genetic Programming" www.ijird.com November, 2014 Vol 3 Issue 11.
10. Rabiner, Lawrence R., (1989) "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition", Proc. of IEEE, Vol. 77, No. 2, pp. 257-286.
11. Srivastava, Abhinav, Kundu, Amlan, Sural, Shamik and Majumdar, Arun K., (2008) "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 1, pp. 37-48.
12. Chan, Philip K., Fan, Wei, Prodromidis, Andreas L. & Stolfo, Salvatore J., (1999) "Distributed Data Mining in Credit Card Fraud Detection", IEEE Intelligent Systems, Vol. 14, No. 6, pp. 67-74.
13. Fonzo, Valeria De, Aluffi-Pentini, Filippo and Parisi, Valerio, (2007) "Hidden Markov Models in Bioinformatics", Current Bioinformatics, Vol. 2, pp. 49-61.
14. V. Bhusari, S. Patil "Application of Hidden Markov Model in Credit Card Fraud Detection" International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, November 2011
15. Quratulain Rajput, Nida Sadaf Khan, Asma Larik & Sajjad Haider "Ontology Based Expert-System for Suspicious Transactions Detection" Computer and Information Science; Vol. 7, No. 1; 2014, ISSN 1913-8989 E-ISSN 1913-8997.
16. C. Martinez-Cruz, I. J. Blanco and M. A. Vila, "Ontologies versus relational databases: are they so different? A comparison," Artificial Intelligence Review, pp. 271-290, 2012.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

17. Chandrasekaran B., J. R. Josephson, and V. R. Benjamins. What are ontologies, and why do we need them? IEEE Intelligent Systems, 14(1):20–26, 1999.
18. M. Horridge, "A Practical Guide To Building OWL Ontologies Using Protègè 4 and CO-ODE Tools, Edition 1.3," The University of Manchester, 2011.
19. SamanehSorournejad, Zahra Zojaji, Reza Ebrahimi Atani, Amir Hassan Monadjemi "A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective" Department of Information Technology, University of Guilan, Iran.
20. Ali Ahmadian Ramaki , Reza Asgari2 , Reza Ebrahimi Atani " CREDIT CARD FRAUD DETECTION BASED ON ONTOLOGY GRAPH" International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 5, October 2012.