Intrusion Detection in Network using Anomaly Detection Technique in Data Mining

Mrs.Y.S. Kala Vani
Asst.professor
Dept.of.MCA
SaIT
Bangalore-97
kalaiys@rediffmail.com

Mr.T.Srinivasa Rao
Asst.professor
Dept.of.MCA
SaIT
Bangalore-97
sr_thummala@yahoo.co.in

Mrs. B M Hemalatha
Lecturer
Dept.of.MCA
SaIT
Bangalore-97
bm.hemalatha@gmail.com

Mr.Prabhu.G
Lecturer
Dept.of.MCA
SaIT
Bangalore-97
prabhugowda2@gmail.com

Abstract: **As the cost of information processing and Internet accessibility falls, organizations are becoming increasingly vulnerable to potential cyber threats such as network intrusions.Intrusions are caused by the Attackers accessing the system from Internet Insider attackers authorized users attempting to gain and misuse non-authorized privileges.Intrusion Detection System combination of software and hardware** that attempts to perform intrusion detection raises the alarm when possible intrusion happens .Using the traditional intrusion detection tools(IDS) having some limitations are they cannot detect emerging cyber threats,Signature database has to be manually revised for each new type of discovered intrusion. To overcome the problem in old intrusion detection tools the anomaly detectiontechnique **used to find out deviations from the normal behavior. Anomaly intrusion detection uses different approaches and finds the solutions for the old intrusion detection tools by comparing different anomaly detection procedures.**

Keywords **—cyber access, intrusion detection, anomaly detection, intrusion detection tools.**

I. INTRODUCTION

With an upsurge in financial accounting fraud in the current economic scenario experienced, financial accounting fraud detection (FAFD) [1] have received considerable attention from the investors, academic researchers, media, the financial community and regulators. Due to some high profile financial frauds discovered and reported at large companies like Enron, Lucent, WorldCom and Satyam over the last decade, the requirement of detecting, defining and reporting financial accounting fraud has increased.

Data mining is a sophisticated approach to search the data from the huge capacity of storage. It has different methodologies to mine the data [1]. Data mining has different set of applications in different areas such as Business, weather forecasting, financial and marketing, neural networks; intrusion detection such as credit card detection etc., Data mining has different strategies of analysis which is used to find the data in an effective way. Data mining is popularly used to combat frauds because of its effectiveness. It is a well-defined procedure that takes data as input and produces models or patterns as output Data mining is a process that uses a variety of data analysis tools to discover patterns and relationships in data that may be used to make a valid prediction.

Data mining is known as gaining insights and identifying interesting patterns[2] from the data stored in large databases in such a way that the patterns and insights are statistically reliable, previously unknown, and actionable [3]. Data mining is also define as a process that uses statistical, mathematical, artificial intelligence and machine learning techniques to extract and identify useful information and subsequently gaining knowledge from a large database.

The blending point between data mining and detecting accounting fraud is that, data mining as an advanced analytical tool may assist the auditors in decision making and detecting fraud. The data mining techniques have the potential to solve the contradiction between effect and efficiency of fraud detection [4]. Data mining plays an important role in the financial accounting fraud detection, as it is often applied to extract and discover the hidden patterns in very large collection of data.

II. Data mining Techniques for Intrusion Detection

A graphical conceptual framework is proposed for the available literature on the applications of data mining techniques to financial accounting fraud detection.The classification framework, which is shown in Fig. 1, is based on a literature review of existing knowledge on the nature of data mining research, fraud detection research.

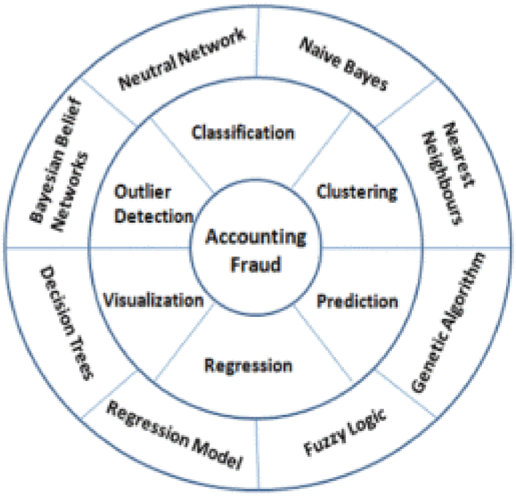

Fig 1.0 The Conceptual Framework for Application of Data Mining to FAFD

A classification framework for financial fraud suggested is based on the financial crime framework of the U.S. Federal Bureau of Investigation [7], which is one of the established frameworks for financial fraud Detection. Fig. 1 consists of two layers, the first comprising the data mining application classes of classification, clustering, prediction, outlier detection, regression, and visualization supported by a set of algorithmic approaches.

A brief description of the conceptual framework with references is provided and of the six data mining application classes (classification, clustering, outlier detection, prediction, regression and visualization),

A. Classification of Data Mining Applications

Each of the six data mining application classes is supported by a set of algorithmic approaches to extract the relevant relationships in the data. These approaches can handle different classes of problems. The classes are presented below

Classification: Classification builds up (from the training set) and utilizes a model (on the target set) to predict the categorical labels of unknown objects to distinguish between objects of different classes. These categorical labels are predefined, discrete and unordered. The research literature describes that classification[7] or prediction is the process of identifying a set of common features (patterns), and proposing models that describe and distinguish data classes or concepts. Common classification techniques include neural networks, the Naïve Bayes technique, decision trees and support vector machines. Such classification tasks are used in the detection of credit card, healthcare and automobile insurance, and corporate fraud, among other types of fraud and classification is one of the most common learning models in the application of data mining in fraud detection.

Clustering: Clustering is used to partition objects into previously unknown conceptually meaningful groups (i.e. clusters), with the objects in a cluster being similar to one another but very dissimilar to the objects in other clusters. Clustering is also known as data segmentation or partitioning and is regarded as a variant of unsupervised classification The most common clustering techniques are the K-nearest neighbour, the Naïve Byes technique and self-organizing maps.

Prediction - Prediction estimates numeric and ordered future values based on the patterns of a data set.

Outlier detection - Outlier detection is employed to measure the distance between data objects to detect those objects that are grossly different from or inconsistent with the remaining data set Data that appear to have different characteristics than the rest of the population are called outliers The problem of outlier/anomaly detection is one of the most fundamental issues in data mining. A commonly used technique in outlier detection is the discounting learning

Regression - Regression is a statistical methodology used to reveal the relationship between one or more independent variables and a dependent variable (that is continuous-valued)

Visualization- Visualization refers to the easily understandable presentation of data and to methodology that converts complicated data characteristics into clear patterns to allow users to view the complex patterns or relationships uncovered in the data mining process

B. Classification of Data Mining Techniques for Intrusion Detection

To determine the main algorithms used for financial accounting fraud detection, we present a Review of data mining techniques identified in literature applied to the detection of financial fraud. The most frequently used techniques are logistic models, neural networks, the Bayesian belief network, anomaly detection and misuse detection.

Regression Models: The regression based models are mostly used in financial accounting fraud detection. The majority of them are based on logistic regression, stepwise-logistic regression, multi criteria decision making method and exponential generalized beta two. Logistic model is a generalized linear model that is used for binomial regression in which the predictor variables can be either numerical or categorical [5]. It is principally used to solve problems caused by insurance and corporate fraud.

Neural Networks– The neural networks are non-linear statistical data modeling tools that are inspired by the functionality of the human brain using a set of interconnected nodes [6]. Neural networks are widely applied in classification and clustering, and its advantages are as follows. First, it is adaptive; second, it can generate robust models; and third, the classification process can be modified if new training weights are set. Neural networks are chiefly applied to credit card, automobile insurance and corporate fraud.

Bayesian Belief Network- The Bayesian belief network (BBN) represents a set of random variables and their conditional independencies using a directed acyclic graph (DAG), in which nodes represent random variables and missing edges encode conditional independencies between the variables [7]. The Bayesian belief network is used in developing models for credit card, automobile insurance, and corporate fraud detection.

Decision Trees – A decision tree (DT) is a tree structured decision support tool, where each node represents a test on an attribute and each branch represents possible consequences. In this way, the predictive model attempts to divide observations into mutually exclusive subgroups and is used for data mining and machine learning tasks.

Naïve Bayes - Naïve Bayes is used as simple probabilistic classifier based on Bayes conditional probability rule. Naïve Bayes follows strong (naive) statistical independence assumptions for the predictor variables. It is an effective classification tool that is easy to interpret and particularly suited when the dimensionality of the inputs is high. In a study. Naïve Bayes methods are widely used in banking and financial fraud detection and claim fraud detection.

Fuzzy Logic: Fuzzy Logic is a mathematical technique that classifies subjective reasoning and assigns data to a particular group, or cluster, based on the degree of possibility the data has of being in that group. The expert fuzzy classification[8] techniques enable one to perform approximate reasoning that can improve performance in three ways. First, performance is improved through efficient numerical representation of vague terms, because the fuzzy technology can numerically show representation of a data item in a particular category. The second way performance is enhanced is through increased range of operation in ill-defined environments, which is the way that fuzzy methodology can show partial membership of data elements in one or more categories that may not be clearly defined in traditional analysis.

*Anomaly detection:*Anomaly Detection the process where to localize objects that are different from other objects (anomalies).It is a technique for improving the analysis of typical data Objects.These anomalous objects are exceptionalin some sense. Lie far away from other data points (outliers) have attribute values that deviate significantly from the expected or typical attribute values indicate errors in data.

This paper focuses on the anomaly detection which is used to find the fraud in credit card using online .Anomaly uses different strategies to find out the anomalous behavior in the credit card.

III. Anomaly detection in data mining to find intrusion in credit card system

Data mining automates the detection of relevant patterns in a database, using defined approaches and algorithms to look into current and historical data that can then be analyzed to predict future trends. Because data mining tools predict future trends and behaviors by reading through databases for hidden patterns, they allow organizations to make proactive, knowledge-driven decisions and answer questions that were previously too time-consuming to resolve the problem.

Anomaly Detection: Anomaly detection is the process where to localize objects that are different from other objects (anomalies).It is a technique for improving the analysis of typical data Objects. These anomalous objects are exceptionalin some sense, lie far away from other data points (outliers) have attribute values that deviate significantly from the expected or typical attribute values indicate errors in data.

A. ApplicationsAnomaly detection

Anomaly detection technique is used to detect the problems, to detect new phenomenon to discover unusual behavior in data .Many of the research papers are based on anomaly detection techniques and remaining based on misuse detection [9]. Anomaly detection has different set of applications which are Fraud Detection is looking for buying patterns different from typical behavior, Intrusion Detection is monitoring systems and networks for unusual behavior, Ecosystem Disturbances is used to try to predict events like hurricanes and floods, PublicHealth uses medical statistic reports for diagnosis, Medicine uses unusual symptoms or test result to indicate potential health problems.

B.Anomaly Detection Techniques

Anomaly is an Anomalous object (point) that is sensibly different from other objects (points) in statistic; an outlier is an observation that is numerically

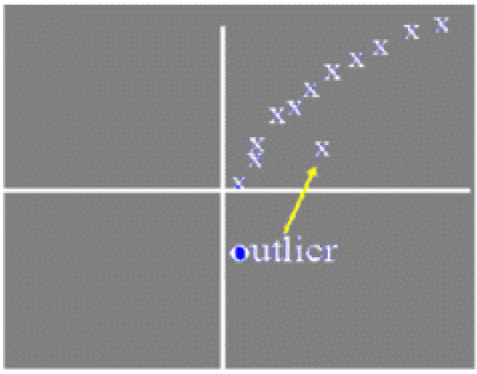

Fig.2.0 Graphical representation of outlier

Outlier: Hawkins' Definition of Outlier An outlier is an observation that differs so much from other observation as to arouse suspicion that it was generated by a different mechanism.Moore and McCabe (1999)an outlier is an observation that lies outside the overall pattern of a distribution Francesco.

Causes of anomalies: Common causes of anomalies are Data from Different Classes: objects different because they are of a different type or class. Natural Variation: of datasets modeled by statistical distributions, where are admitted variations in data Measurement and Collection Errors: errors in the data collection or during the measurement process.

C.Classification of Anomaly detection:

Anomaly Detection Techniques are classified into three categories such as Model-Based, Proximity-Based, Density-Based.

Model-Based Technique:

This technique follows the strategies to build a model of the data and the find the anomalies which are objects that do not fit the model.Example: if the model is a set of clusters, an anomaly is an object that does not strongly belong to any cluster Statistical Approaches are model-based:based on building a probability distribution model consider how likely objects are under that model. An outlier is an object that has a low probability with respect to a probability distribution model of the data.

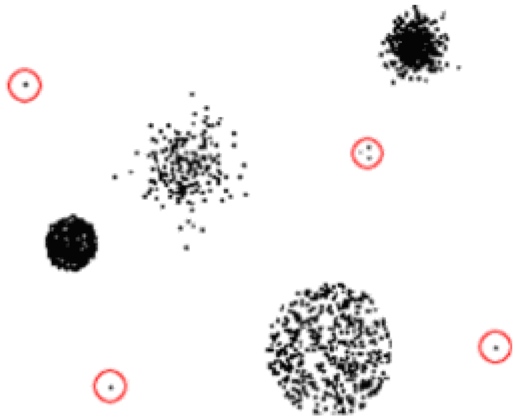

Fig.2.0 Model based anomaly detection

Proximity-Based Technique

This technique defines a proximity measure between objects Anomalies are objects that are distant from most of the other objects Proximity measure: often is chosen distance-based outlier detection techniques. Simplest way to measure proximity: distance to the k-nearest neighbors outlier score is given by the distance to its k-Nearest Neighbors .An object is an anomaly if it is distant from most points (k) this scheme is simple it's easier to determinate a "good" measure than to determinate the statistical distribution

Density-Based Technique

This technique used to estimate the density of objects and anomalies are objects that are in regions of low density .Low density is relatively distant from their neighborsProblems when we have several regions with widely differing densities. The outlier score of an object is the inverse of the density around an object an object is anomalous if it's in a region of low density Density-Based outlier detection. Closely related to Proximity-Based outlier detection since, density is usually defined in terms of Proximity

IV. Basic approaches to anomaly detection

We need a training set with both anomalous and normal objects. *Unsupervised*: class labels are not available. We assign a score to eachinstance (degree of anomaly):▲ Problems with many similar anomalies: can be labeled as normal or have allowed outlier score.*Semi-supervised*: training data contains labeled normal data but hasno information about an anomalous objects.▲we try to find a label or score for anomalous object by using the informationfrom labeled normal objects.outlier score is given by the distance to its k-Nearest Neighbors .An object is an anomaly if it is distant from most points (k)this scheme is simpleit's easier to determinate a "good" measure than to determinate thestatistical distribution

V. Intrusion detection tools in data mining

Data mining automates the detection of relevant patterns in a database, using defined approaches and algorithms to look into current and historical data that can then be analyzed to predict future trends. Because data mining tools predict future trends and behaviors by reading through databases for hidden patterns, they allow organizations to make proactive, knowledge-driven decisions and answer questions that were previously too time-consuming to resolve

Organizations that wish to use data mining tools can purchase mining programs designed for existing software and hardware platforms, which can be integrated into new products and systems as they are brought online, or they can build their own custom mining solution. For instance, feeding the output of a data mining exercise into another computer system, such as a neural network, is quite common and can give the mined data more value. This is because the data mining tool gathers the data, while the second program (e.g., the neural network) makes decisions based on the data collected.

Different types of data mining tools are available in the marketplace, each with their own strengths and weaknesses. Internal auditors need to be aware of the different kinds of data mining tools available and recommend the purchase of a tool that matches the organization's current detective needs. This should be considered as early as possible in the project's lifecycle, perhaps even in the feasibility study.

Most data mining tools can be classified into one of three categories: traditional data mining tools, dashboards, and text-mining tools. Below is a description of each.

*A.Traditional Data Mining Tools.*Traditional data mining programs help companies establish data patterns and trends by using a number of complex algorithms and techniques. Some of these tools are installed on the desktop to monitor the data and highlight trends and others capture information residing outside a database. The majority are available in both Windows and UNIX versions, although some specialize in one operating system only. In addition, while some may concentrate on one database type, most will be able to handle any data using online analytical processing or a similar technology.

Dashboards. Installed on computers to monitor information in a database, dashboards reflect data changes and updates on screen — often in the form of a chart or table — enabling the user to see how the business is performing. Historical data also can be referenced, enabling the user to see where things have changed (e.g., increase in sales from the same period last year). This functionality makes dashboards easy to use and particularly appealing to managers who wish to have an overview of the company's performance.

Text-mining Tools. The third type of data mining tool sometimes is called a text-mining tool because of its ability to mine data from different kinds of text — from Microsoft Word and Acrobat PDF documents to simple text files, for example. These tools scan content and convert the selected data into a format that is compatible with the tool's database, thus providing users with an easy and convenient way of accessing data without the need to open different applications. Scanned content can be unstructured (i.e., information is scattered almost randomly across the document, including e-mails, Internet pages, audio and video data) or structured (i.e., the data's form and purpose is known, such as content found in a database). Capturing these inputs can provide organizations with a wealth of information that can be mined to discover trends, concepts, and attitudes.

B. Intrusion detection in credit card transaction.

Cyber credit-card fraud or no card present fraud is increasingly important in the recent years for the reason that thecredit-card i s majorly used to request payments from these companies on the internet. Therefore the need to ensure secure transactions for credit-card owners when consuming their credit cards to make electronic payments[10] for goods and services provided on the internet is a criterion. Data mining has popularly gained recognition in combating cyber credit-card fraud because of its effective using one of the data mining technique anomaly detection. This system implements the supervised anomaly detection algorithm of Data mining to detect fraud in a real time transaction on the internet, and thereby classifying the transaction as legitimate, suspicious fraud and illegitimate Transaction.

C. What Is Cyber Credit-Card Fraud Or No Card Present Fraud?

Recent and current scholars investigating credit-cardfraud have divided credit-card fraud into two types: the online credit card fraud (or no card present fraud) and the offline credit card fraud (card present fraud) [1]. The online credit-card fraud (in this paper is cyber creditcard fraud) is committed with no presence of a credit-card but instead, the use of a credit-card information to make electronic purchase for goods and services on the internet.Cyber Credit-Card Fraudsters:

*Credit-card information buyers:*They are fraudsters with little or no professional computer skills (ex:Computer Programming, Networking, etc.,) who buy hacked (or stolen) credit-card information on an illegal "credit-card sales" website. They buy this credit-card information with the intention of making electronic payment for some good and services on the internet.

Black hat hackers: Recent research on Hackers in terms

Of Computer Security defined a "black hat hacker" (also known as a cracker) as a hacker who violates computer security with malicious intent or for personal gain [**8**]. They choose their targets using a two-pronged process known as the "pre-hacking stage"; Targeting, Research and Information Gathering, [10] and finishing the Attack. These types of hackers are highly skilled in Computer Programming and Computer Networking and with such skills can intrude a network of computers. The main purpose of their act of intrusion or hacking is to steal personal or private information (such as credit-cardinformation, bank-account information, etc.) for their ownpersonal gain (for instance creating a "credit-card sales"website where other cyber credit-card fraudsters with little or no computer skills can buy credit-card information.

VI. Methodology

A. Implementing Data mining Techniques for Credit CardFraud Detection System

Data mining is popularly used to effectively detect fraud because of its efficiency in discovering or recognizing unusual or unknown patterns in a collected dataset. Data mining is simply a technology that allows the discovery of knowledge in a dataset. In other words, with Data mining, knowledge can be discovered in a dataset. Data is collected from different sources into a dataset and then with Data mining.

Anomaly detection (sometimes called deviation detection) is an algorithm implemented to detect patterns in a given data set that do not conform to an established normal behavior [**11**]. The patterns, thus detected are called anomalies and often translate to critical and actionable information in several application domains. The Anomaly detection is categorized into three; Unsupervisedanomaly, Semi-supervised and Supervised anomaly detection. Unsupervised anomaly detection techniques detect anomalies in an unlabeled test [12] data set under the assumption that the majority of the instances in the data set is normal by looking for instances that seem to fit least to the remainder of the data set. Supervised anomaly detection techniques require a data set that has been labeled as "normal" and "abnormal" and involves training a classifier (the key difference to many other statistical classification problems is the inherent unbalanced nature of outlier detection). Semi-supervised anomaly detection techniques to construct a model representing the normal behavior of a given normal training data set, and then testing the likelihood of a test instance to be generated by the learnt model[**13**]. As seen in the diagram on , this data mining application uses Supervised Anomaly detection to detect credit card fraud in a transaction and thereby classifies a transaction as Ok, suspicious fraud or illegitimate transaction.

B. *Credit Card Fraud detection model:*

This Data mining application applies the anomaly detection algorithm to detect cyber credit card fraud in an online credit-card transaction implementing Pattern recognition with Neural Networks. An anomaly detection algorithm is a technique used in Data mining applications to detect specific patterns or relations within the data provided for Fraud detection process. There is a fixed pattern to how credit-card owners consume their credit-card on the internet. This fixed pattern can be drawn from legitimateregular activities of the credit-card owner for the past oneor two years on its credit-card; the regular merchantwebsites the credit-card owner regularly makes electronic payment for goods and services, the geographicallocation where past legitimate[14] transactions have beenmade, the geographical location where goods havebeen shipped to by the credit-card owner, theemail-address and phone number regularly used by thecredit card owner for notification.

VII. CONCLUSION

In this paper the data mining uses its technique to detect the intrusion in the network in the form of credit card fraud detection. This data mining techniques[8] which consists of the conceptual view of the applications. This paper focuses on the anomaly detection technique and Intrusion detection tools (IDS)Based on one of the data mining technique. Many research papers are based on the anomaly detection using different strategies and algorithms which are used to detect the intrusion in the network. Network applications are so vast, so the data mining technique taken into consideration in the field of cyber credit card intrusion detection system.A data mining application has been modeled as a subsystem which can be used with software systems and applications in financial institutions to detect credit-fraud in a transaction on the internet. Many Intrusion detection tools developed based on the data mining technique to detect the intrusions.

VIII. REFERENCES

[1] R. Agrawal, T. Imielinski, and A. Swami. Mining association rules between sets of items in large databases. In Proceedings of the ACM SIGMOD Conference on Management of Data, pages 207–216, 1993.

[2] Adnan M. Al-Khatib, Electronic payment fraud detection techniques, World of Computer Science and Information Technology Journal (2012), vol. 2, no. 4. pp. 137-141.

[3] Francisca NouyelumOgwueleka, Data mining application in credit-ca rd Fraud detection system, Journal of Engineering Science and Technology (2011), vol, 6, no. 3, pp. 311 - 322.

[4] Dr. Yashpal Singh and Singh Chauhan, Neural networks indata mining. Journal of Theoretical and Applied InformationTechnology (2005-2009), vol, 5, no. 6. pp. 37-42.

[5] Khyati Chaudhary and Bhawna Mallick. Exploration of data mining techniques in fraud detection: credit-card, International Journal of Electronics and Computer Science Engineering. vol. I, no. 3. pp. 1765-1771.

[6] V.Dheepa and Dr. RDhanapal, Analysis of credit-card frauddetection methods, International Journal of Recent Trends in Engineering (2009), vol, 2. No. 3, pp.126-128.

[7] Khyati Chaudhary, JyotiYadav and Bhawna Mallick, A Review of fraud detection techniques: credit-card, International Journal of Computer Applications (2012), vol. 45, no. I, pp.39-44.

[8] Sam Maes, Karl Tuyls and Bram Vanschoenwinkel, Credit-card Fraud Detection Using Bayesian and NeuralNetworks.[ONLINE]Available at:http://www.personeel.unimaas.nl/ktuylslpublicationslpaperslmaenf02.pdf. [Accessed 12December 2012].

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

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

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

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

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

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

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

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

[17] Brause, R., Langsdorf, T. & M Hepp. 1999b. Neural Data Mining for Credit Card Fraud Detection,

"Study on Fraud Risk Prevention of Online Banks" By Qinghua Zhang. 2010 International Conference on Networks Security, Wireless Communications and Trusted Computing.

[18] "Fraudulent Internet Banking Payments Prevention using Dynamic Key" By Osama Dandash Yiling Wang anaphor Dung Leand Bala Srinivasan. "JOURNAL OF NETWORKS, VOL. 3, NO. 1, JANUARY 2008".

[19] Ghosh, S., and Reilly, D.L., 1994. Credit Card Fraud Detection with neural-Network, 27th Hawaii International l Conference on Information Systems, vol. 3 (2003), pp. 621- 630.

[20] Stolfo, S. J., Fan, D. W., Lee, W., Prodromidis, A., and Chan, P. K., 2000.Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project, Proceedings of DARPA Information SurvivabilityConference and Exposition, vol. 2 (2000), pp. 130-144.

[21] L.R. Rabiner, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," Proceedings of the IEEE, vol. 77, no. 2, pp. 257-286, 1989.

[22] K. S. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, Second Edition, John Wiley and Sons, New York, 2001.

[23] Iyer, Divya.; Mohanpurkar, Arti; Janardhan, Sneha; Rathod, Dhanashree; Sardeshmukh, Amruta," Credit Card Fraud Detection" Proceedings of the IEEE, pp. 1062-1066, 2011.

[24] V. Paxon. Bro: A system for detecting network intruders in real-time. In Proceedings of the 7th USENIX Security Symposium, San Antonio, TX, 1998.

[25] P. A. Porras and P. G. Neumann. Emerald: Event monitoring enabling responses to anomalous live disturbances. In National Information Systems Security Conference, Baltimore MD, October 1997.

[26] S. Stainford-Chen. Common intrusion detection framework. http://seclab.cs.ucdavis.edu/cidf.