International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 10 – No.2, December 2015 – www.ijais.org

A Comprehensive Survey of Fraud Detection Techniques

Lutfun Nahar Lata
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology
Dhaka-1208, Bangladesh

Israt Amir Koushika
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology
Dhaka-1208, Bangladesh

Syeda Shabnam Hasan
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology
Dhaka-1208, Bangladesh

ABSTRACT
To overcome the financial loss and threat, fraud detection is a must. New theories and many techniques have been introduced to overcome the fraud. Fraud detection techniques monitor the behavior of the user and inform the user if any harmful event occurs. These modern techniques help to lessen the fraud and unwanted behavior. Some techniques have lacking in some cases, so there are many studies and experiments to improve new methods to detect fraud detection. This paper is about a wide-ranging survey about different kinds of modern techniques used for computer intrusion, credit card fraud, telecommunication fraud and insurance fraud. The main goal of this paper is to assess most common and useful techniques used for different kinds of fraud detection now-a-days.

Keywords
Fraud detection, Intrusion, credit card, telecommunication, healthcare, insurance, data mining etc

1. INTRODUCTION
The Association of Certified Fraud Examiners (ACFE) defined fraud as the use of one's occupation for personal enrichment through the deliberate misuse or application of the employing organization's resources or assets [1]. Now a days, the uses of technological items has increased uncountably as well as fraudulent of using this items has also increased. But to reduce and detect this fraudulent there are many techniques. These frauds are now everywhere in credit cards banking, insurance, personal computers and other private sectors. These frauds invade the privacy and sometimes do hazardous deeds to harm the user. But to detect and remove these intelligent frauds there are many intelligent methods. In this paper different techniques that are used for detecting credit card fraud, computer intrusion, telecommunication fraud and health insurance fraud have been discussed.

Computer intrusion: Intrusion means to invade someone's privacy and computer intrusion defines invade the privacy of computer system. But there have been many techniques introduced to detect the intruder. Misuse and anomaly are the two classifications of intrusion detection techniques.

Insurance fraud detection: Insurance fraud detection techniques detect the fraudulent of untrusted claiming of insurance data. Healthcare insurance fraud detection techniques are discussed here. These techniques detects the incomplete data input, duplicate claims, and medically non-covered services.

Credit card fraud detection: Credit card fraud detection techniques detects whether any unwanted person is using or doing harmful effects to credit card systems by invading the security.

Telecommunication fraud detection: These techniques detect the frauds like ghosting, mobile phone cloning.

2. INTRUSION DETECTION
Many intrusion detection systems based on the analysis of audit data generated by the operating system. Generally, intrusion detection activities were performed by system administrators who examined audit logs of user and system events recorded by computer hosts. Activities such as super user login attempts, FTP transfers of sensitive files, or failed file accesses were flags for potential intrusive activity [2].

Intrusion Detective Systems (IDS) are called security tools such as antivirus software or firewall. IDWG (Intrusion Detection Working Group) defined a general IDS architecture of four functional modules [1]:

- E blocks (Event Boxes): This block has the senses element that monitors the target system and this information issues are analyzed by other block.
- D blocks (Database Boxes): Stores the information that has been monitored by E blocks.
- A blocks (Analysis Boxes): Processing modules for analyzing events and detecting potential hostile behavior, so that some kind of alarm will be generated if necessary.
- R blocks (Response Boxes): The main function of this block is execution and if any intrusion occurs send a response.

IDS may be either host or network based. When an IDS looks for these patterns in network traffic then it is network based [3]. When an IDS looks for attack signatures in log files, then it is host based.

IDS are classified in two sections. As misuse or signature-based and anomaly based detection. Misuse detection attempts to recognize the attacks of previously observed intrusions in the form of a pattern or a signature and directly monitor for the occurrence of these patterns. On the other hand, anomaly based detectors attempt to estimate the normal behavior of the system and generate an anomaly alarm whenever the deviation between a given observation at an instant and the normal behavior exceeds a predefined threshold.

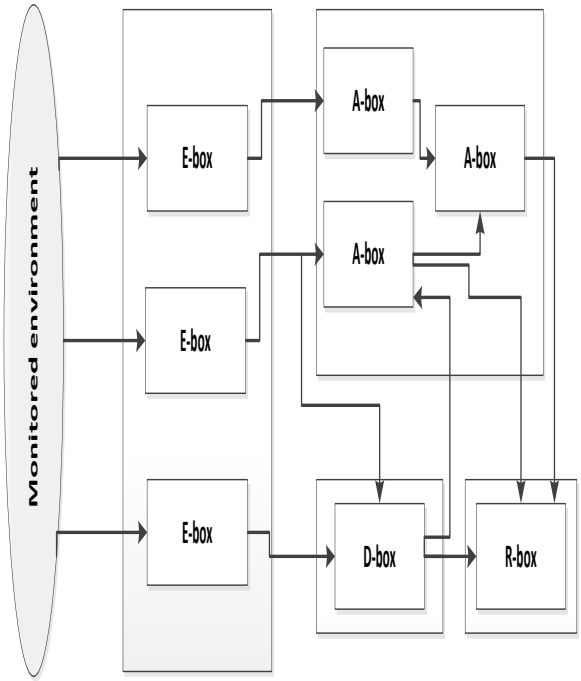

Fig: 1- General CIDF architecture for IDS systems

Anomaly detection tries to establish a historical normal profile for each user, and then use sufficiently large deviation from the profile to indicate possible intrusions. Misuse detection is simpler than anomaly detection. The difference of these methodologies can be defined by the concept of **attack** and **anomaly**. An attack can be defined as a sequence of activities that puts the security of the system at a risk and anomaly as an event that is suspicious from the perspective of security.

The advantages and disadvantages of these methodologies can be stated as misuse method which is very good at detecting results for specified, well-known attacks. But they are not capable of detecting new, unfamiliar intrusions. On the other hand, anomaly detection process has the capability of detecting previously unseen intrusions. But the rate of false positive is higher than the signature based system.

2.1 Intrusion Detection Techniques

A-NIDS (Anomaly based Network intrusion detection system) techniques:

A-NIDS is a principle focus of research and development in intrusion detection techniques. Parameterization, training stage and detection stage are the stages of A-NIDS [1]. A-NIDS techniques can be classified into three different categories: statistical based, knowledge based and machine learning based. In the statistical-based case, the behaviour of the system is represented from a random viewpoint. On the other hand, knowledge-based A-NIDS techniques try to capture the claimed behaviour from available system data (protocol specifications, network traffic instances, etc.). Finally, machine learning A-NIDS schemes are based on the establishment of an explicit or implicit model that allows the patterns analyzed to be categorized.

A) Statistical based	A.1) Univariate
	A.2)Multivariate
	A.3) Time series model
B) Knowledge based	B.1)FSM
	B.2) Description languages
	B.3) Expert systems
C) Machine learning	C.1)Bayesian networks
	C.2)Markov models
	C.3) Neural networks
	C.4)Fuzzy logic
	C.5) Genetic algorithms

Fig: 2– Classification of the anomaly detection techniques according to the nature of the processing involved in the ‘‘behavioural’’ model considered

A.1) Statistical based

Univariate model: This model is an earliest network and host oriented IDS that modelled Gaussian random variables.

Multivariate model: This model considers the correlations between two or more metrics were proposed (Ye et al., 2002). These are useful because experimental data have shown that a better level of discrimination can be obtained from combinations of related measures rather than individually.

Time series model: Time series models use an interval timer, event counter or resource measure, and take into account the order and the inter-arrival times of the observations as well as their values.

Advantages-disadvantages:

- Prior knowledge about normal activity not required. Accurate notification of malicious activities.

- Susceptible to be trained by attackers. Difficult setting for parameters and metrics. Unrealistic quasi-stationary process assumption.

B) Knowledge based

Finite state machine: Finite state machine is a formal tool [1]. This method includes some states and transitions appropriate for modeling network protocol.

Description language: N-grammars, UML and LOTOS are standard description languages for this method and ot combines all knowledge.

Expert System: An expert system is defined as a computing system capable of representing and reasoning about some knowledge-rich domain with a view to solving problems and giving advice [4]. Expert systems classify the audit data according to a set of rules, involving three steps. First, different attributes and classes are identified from the training data. Second, a set of classification rules, parameters or procedures are deduced. Third, the audit data are classified accordingly.

Advantages and disadvantages:

- robustness and flexibility.
- the development of high-quality knowledge is often difficult and time-consuming (Sekar et al., 2002).

C)Machine learning based
Machine learning technique is anstatistical technique that analyzes patters from training data set. This scheme is very efficient, though it has expensive resource. A machine learning A-NIDS has the ability to change its execution strategy as it acquires new information [1].

Several machine learning-based schemes have been applied to A-NIDS.

C.1) Bayesian networks
Bayesian networks technique is generally used for intrusion detection with statistical schemes, including the capability of encoding interdependencies between variables and of predicting events, as well as the ability to incorporate both prior knowledge and data. Bayesian networks are graphically represented models that show a probabilistic relationship between a set of variables under the domain of uncertainty.

However, as pointed out in Kruegel et al. (2003), a serious disadvantage of using Bayesian networks is that their results are similar to those derived from threshold-based systems, while considerably higher computational effort is required.Although the use of Bayesian networks has proved to be effective in certain situations, the results obtained are highly dependent on the assumptions about the behaviour of the target system.

C.2) Markov models (Markov chain and hidden Markovmodel)
A Markov chain is a set of states that are interconnected through certain transition probabilities. During a first training phase, the probabilities associated to the transitions are estimated from the normal behaviour of the target system. The detection of anomalies are then compared with the anomaly score (associated probability) obtained for the observed sequences with a fixed threshold.

In the case of a hidden Markov model, the states and transitions are hidden. Markov-based techniques have been extensively used in the context of host IDS, normally applied to system calls (Yeung and Ding, 2003). In network IDS, the inspection of packets has led to the use of Markov models in some approaches (Mahoney and Chan, 2002; Este´vez-Tapiador et al., 2005). In all cases, the model derived for the target system has provided a good approach for the claimed profile, while, as in Bayesian networks, the results are highly dependent on the assumptions about the behaviour accepted for the system.

C.3) Neural Networks
Neural Networks can be trained with the network traffic data, then use these neural networks to recognize the patterns in network data. This detection approach has been employed to create user profiles, to predict the next command from a sequence of previous ones, to identify the intrusive behaviour of traffic patterns, etc. It is implemented by a backpropagation neural network. Neural Network is very popular because of their flexibility and adaptability to environmental changes. But in the case of neural network to self-organizing maps, they do not provide a descriptive model that explains why a particular detection decision has been taken.

C.4)Fuzzy Logic Techniques
Fuzzy logic is derived from fuzzy set theory under which reasoning is approximate rather than precisely deduced from classical predicate logic. This kind of processing scheme considers an observation as normal if it lies within a given interval.

Although fuzzy logic has proved to be effective, especially against port scans and probes. The main disadvantage is the high resource consumption involved and it has been rejected by some engineers and by most statisticians because of the rigorous mathematical description of uncertainty.

C.5) Genetic algorithms
A genetic algorithm is a method of artificial intelligence problem solving based on the theory of Darwinian evolution applied to mathematical models by evolutionary biology such as inheritance, mutation, selection and recombination [4]. However, genetic algorithm uses this revolutionary method and selects appropriate rules or optimal parameters for detection.

The main advantage of this method is flexibility and robustness where no prior knowledge about the system behaviour is assumed. Its main disadvantage is the high resource consumption involved.

A-NIDS with data mining
For detecting anomalies with data mining, classification model with association rules algorithm and frequent episodes is developed. This approach can automatically generate concise and accurate detection models from large amount of audit data [4]. However, it requires a large amount of audit data in order to compute the profile rule sets. A team of researchers at Columbia University proposed the detection models using cost-sensitive machine learning algorithms [5].Audit data is analyzed by association rules algorithm in order to determine static features of attack data.

An important advantage of data mining approach is that it can develop a new class of models to detect new attacks before they have been seen by human experts.

3. HEALTHCARE FRAUD DETECTION

The National Health Care Anti-fraud Association (NHCAA) defines health care fraud as "an intentional deception or misrepresentation made by a person or an entity, with the knowledge that the deception could result in some kinds of unauthorized benefits to that person or entity" (NHCAA, 2012) [6]. Since 2008 global average fraud and error losses in healthcare have risen 25% from 5.59% of expenditure to 6.99%. Affordable Care Act (ACA) — an estimated 22 million people will be insured [7]. Over the period of 2015-2021, health spending is projected to grow at an average rate of 6.2 percent annually.

Supervised and unsupervised are the classifications of fraud detection in healthcare which use statistical methods.

3.1 Supervised Fraud Detection Methods

There are several supervised fraud detection methods such as:Bayesian networks, neural networks (NNs), decision trees, and fuzzy logic. NNs and decision trees are the most popular fraud detection methods (fig.3) because of their high tolerance of noisy data and huge data set handling.

3.1.1 Bayesian Fraud Detection Method

Bayesian Networks provide a graphic model of causal relationships on which class membership probabilities(Han et al. 2000) are predicted, so that a given instance is legal orfraud (Prodromidis, 1999). Naïve Bayesian classification assumes that the attributes of an instance are independent, given the target attribute.

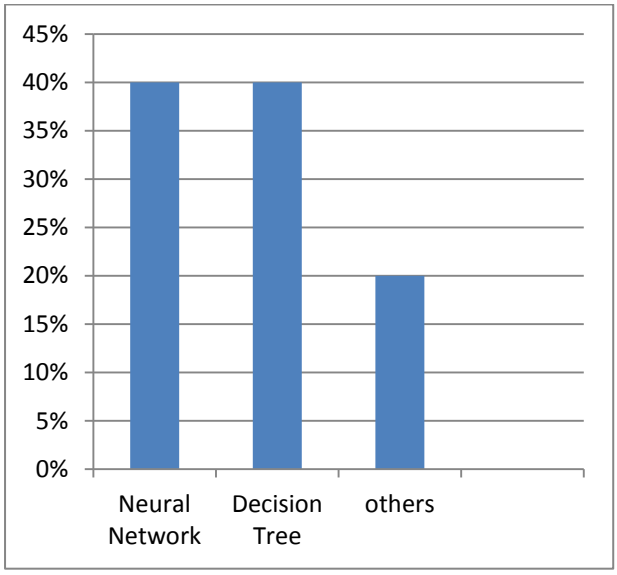

Fig: 3. Percentages of papers on different supervised methods

The aim is to assign a new instance to the class that has the highest posterior probability. Ormerod et al. [8] proposed to detect fraud by a Bayesian network (BN), whose weights were refined by a rule generator called Suspicion Building Tool (SBT). He et al. [8] proposed the use of a k-nearest neighbor algorithm whose distance metric was optimized by a genetic algorithm in detecting two types of fraud: inappropriate practice of service providers and "doctor-shoppers." A model that combined fuzzy sets theory and a Bayesianclassifier was designed to detect suspicious claims in the NHI of Taiwan.

3.1.2 Neural Network (NN):

NNs have been used extensively in detecting health care fraud due to their capability of handling complex data structures and non-linear variable relationships. Backpropagation neural networks can process a large number of instances with tolerance to noisy data and has the ability to classify patterns on which they have not been trained. However, backpropagation require long training hours, extensive testing, retaining parameters like the number of hidden neurons, learning rate. Cooper [9] used an NN to identify fraudulent medical claims submitted to a Chilean health insurance company. One of the common concerns with NNs is overfitting, which produces a relatively small error on the training dataset but a much larger error when new data is presented to the network. Overfitting is especially prominent with skewed data [10] such as health care claims, which have many more legitimate than fraudulent cases.

3.1.3 Decision trees

Decision trees are machine learning techniques that express independent attributes and a dependent attribute in a tree-shaped structure that represents a set of decisions. Classification rules, extracted from decision trees, are IF-THEN expressions in which the preconditions are logically ANDed and all the tests have to succeed if each rule is to be generated. Yang [11] used the C4.5 algorithm to train decision trees for identifying service providers' fraud for the NHI in Taiwan. As an extension to C4.5, the C5.0 algorithm offers several advanced mechanisms. They constructed several classifiers, each of which was driven by a different policy in audit planning. The C5.0 algorithm was also used by William and Huang [11] in detecting insurance subscribers' fraud for the Health Insurance Commission (HIC) of Australia. Due to the huge amount of data (40,000 insurance subscribers), they faced the challenge that an overly complex decision tree with thousands of rules was generated, which made it difficult to interpret.

3.2 Unsupervised Fraud Detection Methods:

There are some unsupervised methods used for detecting healthcare fraud. Some are given below:

3.2.1 SmartSifter

SmartSifter, used to detect outliers in the pathology dataset provided by the HIC of Australia. SmartSifter uses a probabilistic model to represent the underlying data-generating mechanism. In the probabilistic model, a histogram is used to represent the probability distribution of categorical variables; for each histogram, a finite mixture model is used to represent the probability distribution of continuous variables. When a new case is coming, SmartSifter updates the probabilistic model by employing an SDLE (Sequentially Discounting Laplace Estimation) and an SDEM (Sequentially Discounting Expectation and Maximizing) algorithm.

3.2.2 Electronic Fraud Detection

Electronic Fraud Detection (EFD)[12] is an expert system assisting in detecting service providers' fraud, and includes several steps. First, discriminating features (called "behavioral heuristics") are defined by experts. Then, the information gain for a provider is computed as $\int \log (f_p(x)/f_A(x))\ f_p(x)dx$, where, $f_p(x)$ and $f_A(x)$ are probability density functions of the features for the provider and the aggregate peer group, respectively. The information gain measures how different the distribution of the provider is from that of all the peers taken together [13].

Healthcare fraud detection in data mining:

Data mining has a tremendous impact in improving healthcare fraud detection system. Below there are some techniques of healthcare fraud detection in data mining.

Using Spectral Analysis

In this approach, the health care claim datasets are passed into Nodes list and Edges list. The Nodes list consists of two sets of nodes, one is a list of all the primary care physicians (PCPs) and another is a list of all the specialists. The Edge list is a list of edges that connect all the PCPs and Specialists. A two-mode network is constructed using the Nodes list and Edges list. This network is transformed in to a Laplacian matrix, L(u,t). Thus, the connectivity feature of this network is obtained.

It is simple and efficient in the spectral analysis to divide the nodes in to communities of unknown numbers. The goal is to detect the suspicious communities between PCPs and specialists in health care claim datasets.

Multilayer Neural Network (MNN)

In multilayer neural networks (MNN) there are various entities included. Each one of the entities involved in the fraud or abuse problem (medical claims, affiliates, medical professionals &employers). This divides and conquers strategy allows to feedback information over time, combining affiliates, doctors and employer's behavior. MNN has less accuracy than spectral analysis in this section [14].

4. CREDIT CARD FRAUD

Credit card fraud can be defined as "Unauthorized account activity by a person for whom the account was not intended. Operationally, this is an event for which action can be taken to stop the abuse in progress and incorporate risk management practices to protect against similar actions in the future". In simple terms, Credit Card Fraud is defined as when an individual uses another individual s credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. And the persons using the card has not at all having the connection with the cardholder or the issuer and has no intention of making the repayments for the purchase they done.

4.1 Classification of Credit Card Fraud:

Credit card fraud has been divided into two types:

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

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

4.2 Credit Card Fraud Detection Methods:

A.Neural Network

B. Genetic Algorithom

C.Logistic Regression

A. Neural Network

Fraud detection methods based on neural network are the most popular ones. An artificial neural network consists of an interconnected group of artificial neurons [15] .The principle of neural network is motivated by the functions of the brain especially pattern recognition and associative memory [16]. The neural network recognizes similar patterns, predicts future values or events based upon the associative memory of the patterns it was learned. It is widely applied in classification and clustering. The advantages of neural networks over other techniques are that these models are able to learn from the past and thus, improve results as time passes. They can also extract rules and predict future activity based on the current situation. By employing neural networks, effectively, banks can detect fraudulent use of a card, faster and more efficiently. Among the reported credit card fraud studies most have focused on using neural networks. In more practical terms neural networks are non-linear statistical data modeling tools. They can be used to model complex relationships between inputs and outputs or to find patterns in data. There are two phases in neural network training and recognition [17]. Learning in a neural network is called training. There are two types of NN training methods supervised and unsupervised. In supervised training, samples of both fraudulent and non-fraudulent records are used to create models. In contrast, unsupervised training simply seeks those transactions, which are most dissimilar from the norm. On other hand, the unsupervised techniques do not need the previous knowledge of fraudulent and non-fraudulent transactions in database. NNs can produce best result for only large transaction dataset. And they need a long training dataset.

B. Genetic algorithms

For predictive purposes, algorithms are often acclaimed as a means of detecting fraud. In order to establish logic rules which is capable of classifying credit card transactions into suspicious and non-suspicious classes, one algorithm that has been suggested by Bentley et al. (2000) that is based on genetic programming. However, this method follows the scoring process. In the experiment as described in their study, the database was made of 4,000 transactions along with 62 fields. As for the similarity, tree, training and testing samples were employed. For this purpose, different types of rules were tested with the different fields. The best rule among these is with the highest predictability. Their method has proven results for real home insurance data and could be one best method against credit card fraud [18]. Chan et al. (1999) has developed an algorithm for prediction of suspect behavior. Origin of their research is that cost model evaluated and rated b whereas other studies use evaluation based on their prediction rate/the True Positive Rate (TPR) and the error rate/the False Negative Rate (FNR). Wheeler & Aitken (2000) formed the idea of combining different algorithms to maximize the power of prediction [19]. Article by, Wheeler & Aitken, presents different algorithms: diagnostic algorithms, diagnostic resolution strategies,best match algorithms, density selection algorithms, probabilistic curve algorithms and negative selection algorithms. As a conclusion from their investigation that probabilistic algorithms and neighborhoodbased algorithms have been taken to be appropriate techniques for classification, and further it may be improved using additional diagnostic algorithms for decision-making in borderlines cases as well as for calculation of confidence measures and relative risk measures. The inspiration for GANN, by combining genetic algorithms with neural networks comes from nature. In GANN, the genetic algorithm is used to find some parameters. Main query is how exactly Genetic Algorithm and Neural Network can be combined. Neural Network has been encoded in the genome of the Genetic Algorithm. In GANN the procedure involves generation of number of random individuals. Designing of neural network is according to the genome information which helps in evaluation of parameter strings. Performance can be easily determined after back-propagation training. To find an optimal network, few GANN strategies rely only on the GA. In this case no training set takes place which are further evaluated and ranked according to parameter performance. Genetic Algorithm (GA) is a search heuristic that copies the process of natural evolution and is used to generate useful and appropriate solutions for optimization problems and search problems. Genetic algorithms (GA) belongs to the larger class of Evolutionary Algorithms (EA), generate solutions to optimization problems using some techniques such as mutation, inheritance, selection, and crossover.

C. Logistic Regression

To better detect fraud two advanced data mining approaches are support vector machines and random forests, together with the well known logistic regression[20][21]. Logistic regression (LR) is useful for situations in which it is wanted to be able to predict the presence or absence of a characteristic or outcome based on values of a set of predictor variables. It is similar to a linear regression model but is suited to models where the dependent variable is dichotomous. Logistic regression coefficients can be used to estimate odds ratios for each of the independent variables in the model and it is applicable to a broader range of research situations than feature analysis. (Ohlson, 1980; Martin, 1997) estimating the odds of a firm's failure with probability.

5. TELECOMMUNICATION FRAUD

Fraud is costly to a network carrier both in terms of lost income and wasted capacity. The various types of

telecommunication fraud can be classified into two categories: subscription fraud and super imposed fraud. Subscription fraud denotes the behavior of using false identity to subscribe a service and evade payment. Cases of bad debt are also included in this category. Superimposed fraud is the use of a service without having the necessary authority and is usually detected by the appearance of 'phantom' call on a bill. Superimposed fraud includes mobile phone cloning, ghosting (making free calls by deceiving the billing systems), insider fraud, and tumbling (randomly or serially changing the serial number of a cell phone).

5.1 Telecommunication Fraud Detection Methods

Previous work in the telecommunication frauddetection has concentrated mainly on identifying superimposed fraud. Most techniques use Call Detail Record data to create behavior profiles for the customer and detect deviations from these profiles.These approaches are discussed as follows.

Rule-based Approach

A combination of absolute and differential usage is verified against certain rules in the rule-based approach mapped to data in toll tickets. With differential analysis, flexible criteria can be developed to detect any usage change in a detailed user behavior history. Rule-based approach works best with user profiles containing explicit information, where fraud criteria can be referred as rules. Rule-discovery methodology combining two data levels, which are the customer data and behavior data(usage characteristics in a short time frame)is proposed in [22]. A rule set is selected by using a greedy algorithm with the adjusted thresholds. PDAT is a rule-based tool for intrusion detection developed by SiemensZFE.Due to its flexibility and broad applicability, PDAT is used for mobile fraud detection.

Rule-based analysis can be very difficult to manage because the proper conjuration of such rules requires precise, laborious, and timeconsuming programming for each imaginable fraud possibility. The dynamic appearance of multiple new fraud types demands that these rules be constantly adapted to include existing, emerging, and future fraud options. Moreover, it also presents a major obstacle to scalability. The more data the system must process, the more drastic is the performance downfall.

Neural Networks

In recent years, neural networks have played an important role in fraud detection. Neural Networks can actually calculate user profiles in an independent manner, thus adapting more elegantly to the behavior of the various users. Neural Networks are claimed to substantially reduce operation costs. A project of the European Commission, ASPeCT, investigated the feasibility of the implementations with a rule-based approach and neural networks approach, both supervised and unsupervised learning based on data in toll tickets .Three approaches were presented in [23] based on toll tickets (call records stored for billing purposes).First, a feed-forward neural network based on supervised learning is used to learn a non-linear discriminative function to classify subscribers using summary statistics. Second, density estimation with Gaussian mixture model is applied to modeling the past behavior of each subscriber and detecting any abnormalities from the past behavior. Third, Bayesian networks are used to define probabilistic models given the subscribers' behavior.

Visualization Methods

Visualization techniques rely on human pattern recognition to detect anomalies and are provided with close-to-real-time data feeds.The idea is that while machine-based detection methods are largely static, the human visual system is dynamic and can easily adapt to the ever changing techniques used by the fraudsters.Visual data mining is developed to combine human detection with machine recognition. It usually provides a graphical user interface to visualize the call information of different subscribers across large geographical locations. Visual data mining has been applied to detect international calling fraud.

6. CONCLUSION AND FUTURE RESEARCH

In this paper four types of areas have been discussed. The techniques discussed for intrusion Bayesian network, neural network, genetic algorithms give a good result. Though sometimes it's difficult to remove potential attacks and it has poor portability because of the system. In the case of healthcare fraud detection techniques rather than all other techniques neural network and decision tree gives most satisfactory solution. For the case of credit card fraud detection neural network is a very popular method.

There are other various kinds of fraud detection areas like; e-commerce fraud, media fraud, voting irregularities etc.

As a future goal, implementation of algorithms at any specific area of fraud detection can be done to see how they work and comparison of the algorithms that have already been introduced at that area can be made.

7. REFERENCES

[1] Anomaly-based network intrusion detection: Techniques, systems and challenges; P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez. P. 1-5.

[2] Learning Program Behavior Proles for Intrusion Detection; Anup K. Ghosh, Aaron Schwartzbard & Michael Schatz.

[3] Intrusion Detection Framework for Cyber Crimes using Bayesian Network Chaminda Alocious, Nasser Abouzakhar, Hannan Xiao, Bruce Christianson University of Hertfordshire, Hatfield, UK. P. 4.

[4] Survey of Fraud Detection Techniques; Yufeng Kou, Chang-Tien Lu, Sirirat Sirwongwattana Dept. of Computer Science; Yo-Ping Huang Dept. of Computer Science and Engineering. P. 1-5.

[5] Mahoney M., Chan P.K.; An analysis of the 1999 DARPA/Lincoln laboratory evolution data for network anomaly detection. Florida tech. report CS-2003-02; 2003.

[6] Application of Bayesian Methods in Detection of Healthcare Fraud Tahir Ekin[a], Francesca Leva*[,b,] Fabrizio Ruggeri [c], Refik Soyer [d]. P. 1,3.

[7] Cooper C (2003) Turning information into action. Computer Associates: The Software That Manages e-Business, Report, available at http://www.ca.com

[8] A survey on statistical methods for health care fraud detection; Jing Li & Kuei-Ying Huang & Jionghua Jin & Jianjun Shi. P. 7-9.

[9] Phua C, Alahakoon D, Lee V (2004) Minority report in fraud detection: classification of skewed data. SIGKEE Explorations 6 (1):50–59

[10] Yang WS (2003) A Process Pattern Mining Framework for the Detection of Health Care Fraud and Abuse, Ph.D. thesis, National Sun Yat-Sen University, Taiwan

[11] Credit Card Fraud Detection Using Neural Network, Raghavendra Patidar, Lokesh Sharma

[12] Association of certified fraud examiners (ACEF); http://www.acfe.com/article.aspx?id=4294976280

[13] Survey of Insurance Fraud Detection Using Data Mining Techniques; H.Lookman Sithic, T.Balasubramanian. P. 1-2.

[14] Data Mining Techniques in Fraud Detection; Rekha Bhowmik University of Texas at Dallas. P. 4-5.

[15] Ray-I Chang, Liang-Bin Lai, WenDe 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).

[16] Raghavendra Patidar, Lokesh Sharma "Credit Card Fraud Detection Using Neural Network". International Journal of Soft Computing and Engineering (IJSCE), (2011). Volume-1, Issue; (32-38).

[17] Raghavendra Patidar, Lokesh Sharma, "Credit Card Fraud Detection Using Neural Network" 2011.

[18] 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).

[19] Review Paper on Credit Card Fraud Detection, Suman Research Scholar, GJUS&T Hisar HCE Sonepat, Nutan Mtech. CSE, HCE Sonepat.

[20] Survey of Fraud Detection Techniques, YufengKou,Chang-TienLu,Sirirat Sirwongwattana,Yo-Ping Huang.

[21] S.Rosset, U. Murad, E. Neumann, Y. Idan, and G. Pinkas. Discovery of fraud rules for telecommunications challenges and solutions. In Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining, pages409-413.ACMPress,1999.

[22] M.Taniguchi, M.Haft, J.Hollmen, and V.Tresp. Fraud detection in communication networks using neural and probabilistic methods. In Proceedings of the 1998 IEEE International Conference in Acoustics, Speech and Signal Processing,volume2,pages1241-1244,1998.

[23] S. Benson Edwin Raj, A. Annie Portia "Analysis on Credit Card Fraud Detection Methods" 2011. S. Benson Edwin Raj, A. Annie Portia "Analysis on Credit Card Fraud Detection Methods" 2011.