ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue IV, April 2018

A Comprehensive study and analysis of Intrusion Detection using Machine Learning Techniques

Dr. B. Ben Sujitha[1],Dr. B. Ben Sujin[2],D.Roja Ramani[3]
Associate Professor, Kalasalingam University, India[1]
Professor,Nizwa College of Technology,Oman[2]
Assistant Professor,Sethu Institute of Technology, India

Abstract - Sharing of information on the internet plays a key role in today's computing world. The network is being affected with a major issue, namely Intrusion. Intrusion prepares the whole network to face the serious problem. It is very much essential to provide a safeguard mechanism for the network and resources. Intrusion Detection System (IDS) is the application gives monitoring and reporting to the existence of the Intrusion. Though, there is an availability of the best detection system with good performance, still the system could not able to identify all the variety of attacks due to the arrival of a new type of attack. Machine learning is the best approach will be used to identify all types of attack. This paper presents the various existing machine learning approaches and their performance analysis and also suggests the best method to adopt for detection and classification.

Keywords—Intrusion detection; Survey; Classifiers; Hybrid; Ensemble; Dataset; Feature Selections

1. INTRODUCTION

Security is the term deals with providing safer mechanisms to overcome the vulnerable activities. One of the mechanisms provides security through detection, identification and tracking the factors compromise the security. Intrusion is the vulnerable activity that violates the property of the security parameters. Intrusion Detection is the process of monitoring and identifying the malicious activities. The system which is developed to monitor and report to the administrator is the Intrusion Detection System. The best system is able to monitor the progress in the network by using the techniques. The systems have the strong reporting authority about the existence of the attack.

Kendall et al. [1] has given the four classes of attacks is given in the table 1.1.

\Attack type	Description
Denial of Service (DoS)	A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attack makes the resources of the computer is too busy. Examples of such attacks include Smurf, Teardrop, Back, Ping of death, Neptune, Land etc.
User to Root	The attackers make an attempt to the system as real users. Most common attack in this class of attack is buffer overflow attack. Other attacks include Loadmodule, Perl, Ps,Xterm etc.
Remote to User	Attackers gain the access rights through sending packets to the remote machine. Examples of remote to user attack are Dictionary, Ftp_write, Guest, Imap, Phf etc.
Probing	The attackers' scan the computers connected in the network or identify the weakness and they proceed to do attack on services or data. Examples of probing attack are Ipsweep, Mscan, Nmap, Saint, Satan etc.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue IV, April 2018

II.METHODS OF IDENTIFYING THE ATTACK

The attack is categorized as known and unknown. In case of known attack, the profile of the patterns is known already, but the unknown attack is the new arrival pattern. Identifying the unknown attack is the tedious process. Intrusion Detection System is built to detect known or unknown attack is classified as Misuse based detection and Anomaly based detection.

A. Misuse Based Detection

Signature-based detection, also known as misuse detection detects the attack based on the match with predefined attack signature [1] due to the pattern matching stream. In this type the existing attack feature is well known, thus the system is simple and efficient and also provides high accuracy for the known attacks. The false positive alarm rate is less. The signature database must be revised always, so the system is costly and time consuming. This system needs the help of experts to do update in the log or database of signatures.

B. Anomaly Based Detection

Anomaly Based Detection is also called as Behaviour Based Detection which models the behaviour of the network, users, and computer systems and raises an alarm whenever there is a deviation from this normal behaviour [2]. This performs the detection based on constructing profiles representing normal usage and then comparing it with the current behaviour of data to find out a likely mismatching the threshold calculation. The Anomaly Based Detection method identifies the attack based on the identification of the deviation measured using the threshold calculation. These approaches have the ability of identifying known and unknown attacks, and there is no need for a continuous update of the attack knowledge base. The main drawback of this method is the system raises a large number of false alarms; new pattern arrives from the network traffic and poor detection efficiency.

III.BASED ON THE MODE OF DEPLOYMENT

The designed IDS can be installed in the host system or network based detection. They are explained in the section below.

A. Network Based IDS

The designed IDS can be installed in the host system or network based detection. They are explained in the section below. Network based IDS (NIDS) can work with real-time traffic feature and can observe the complete network. NIDS performs the checking with a wide variety of features collected from the different architectural patterns. Few existing techniques are Clustering, Bayes Classifier, Genetic algorithm, ANN, Association rules, Fuzzy systems, etc. Minnesota Intrusion Detection System (MINDS) [3] use data mining techniques for detection of attack. It consists of two modules namely; anomaly detection module and association pattern analysis. The anomaly detection module uses Local Outlier Factor (LOF) to identify anomalies and get a score to each data point based on the factor. The user verifies whether the data point is a real intrusion or normal behaviour. Association pattern analysis is used to review the anomalous.

B. Host Based IDS

Host based intrusion detection systems [4] runs the separate machine which is not connected with other devices or systems. It collects and checks the incoming and outgoing data or message from the device and give response to the administrator on detection of suspicious activity. Host-based IDS is designed to collect or analyze the information on a particular host or system. The virus detector system can monitor the activities in the system; its strength of detecting intrusion is less. However, HIDS checks and collects system data, including System calls; events regard to the network and file system and do verification about the deviation in the data. This system has got the capability to detect the malicious activities based on the audit trail and system log HIDS makes the detection of unauthorized usage of resources. When the similar pattern of the existing attack is matched, activity with that workstation can be stopped, thus blocking the attack. The major drawback of these systems is

(1) They cannot see the network traffic.
(2) HIDS rely heavily on audit trails which can weaken a lot of resources and make wastage of the memory space server.
(3) Lack of cross-platform interoperability.

IV.MACHINE LEARNING APPROACH

Machine learning provides extensive study on the design and establishment of algorithm makes the computer to do the task automatically. This method provides high accuracy and good efficiency. The machine learning has the broad categories as supervised, unsupervised and semi supervised learning approach.

A. Supervised Learning

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue IV, April 2018

The categories of machine learning methodology are supervised and unsupervised learning [5]. Supervised learning approach contains a set of correctly classified instances that makes the trainer to supervise the algorithm. This approach has the hope of classification of new or previously unknown instances. Supervised learning implies to obtain a training data set in which every entry is labelled. For example, each entry in the KDD'99 Data set is originally labelled with the type of attacks, it belongs to or normal when the example corresponds to a harmless packet. The output of the classifier belongs to one of the classes defined by the labels of the Dataset. The percentage of accuracy is high. Some of the traditional supervised learning methods are Naïve Bayes (NB), Bayes Network, Learning Vector Quantization, SVM, Random Forest , k- Nearest Neighbour (KNN), C4.5, and RBF Network

1. Naïve Bayes Classifier

Naïve Bayes classifier [6] makes the assumption of strict independence among the features leading to less accuracy when the features are correlated. On the basis of the class label, the Naive Bayes mechanism assumes that the attributes are conditionally independent and thus tries to estimate the class-conditional probability. Naive Bayes requires only one scan of the training data and thus it eases the task of classification a lot. The detection rates of the classes are very high.

2. Bayesian Network

A Bayesian network is a model that encodes probabilistic relationships among important variables. This technique is generally used for intrusion detection in combination with statistical schemes, a procedure that yields several advantages [7], including the capability of encoding interdependence between variables and of predicting events, as well as the ability to incorporate both prior knowledge and data. , the size of the network increases, as there is an increase in the future. The system feels harder to handle continuous features and may not contain any good classifiers if prior knowledge is wrong.

3. Artificial Neural Network

Artificial Neural Network (ANN) is a processing unit for information which was inspired by the functionality of human brains [8]. Typically neural networks are organized in layers which are made up of a number of interconnected nodes which contain function activation. The input layer accepts the patterns as input, and then passes to the hidden layer where the actual processing occurs. The hidden layers, then link to an output layer for producing the detection result as output. Multilayer perception (MLP) act as a non-linear discriminate function can form any classification decision boundary in feature space. The algorithm, namely back propagation rule is a gradient descent method and based on an error function provides the rule. The error function has been defining using Mean Squared Error (MSE). The output of the system depends on this error value.

4.Neural Networks

The neural network has been used for both anomaly and misuse intrusion detection [9]. In anomaly intrusion detection the neural networks were modelled to recognize statistically significant variations from the user's recognized behaviour also identify the typical characteristics of system users. In misuse intrusion detection the neural network would collect data from the network stream and analyze the data for instances of misuse [10]. This approach is good to identify the unknown attacks and has the ability to learn complex nonlinear input output relationships [11].

5. Bayesian Classifier

A Bayesian Classifier [12] provides high accuracy and speed for handling large database. In network model Bayesian classifier encodes the probabilistic relationship between the variable of interest. In intrusion detection this classifier is combined with statistical schemes to produce higher encoding interdependencies between the variables and predicting events. The graphical model of casual relationships performs learning technique. The components of this technique are a directed acyclic graph and a set of conditional probability tables. Direct Acyclic Graph (DAG) represents a random variable, which may be discrete or continuous. For each variable classifier maintains one conditional probability table (CPT) and higher computational effort.

6. Random Forest (RF)

RF is the excellent algorithm proposed by Bremen [13]. A bootstrap sample of the data is used to build the tree. The branch of the tree can be constructed using the random data subset of the variables. The classification is maintained based on the voting, the tree gets the majority vote is encountered as the new instance. RF has the ability to compute the importance of the variable and proximities. The proximities are used in replacing missing values and outliers. There is no removal

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue IV, April 2018

of variables and the number of sample variable is less than the number of predictors.

7. Learning Vector Quantization

A Supervised Learning Vector Quantization (LVQ) [14] consists of two layers with two different transfer functions, competitive and linear. Competitive (hidden) and output layers contain a specific number of neurons which are the sub attack types and the main attack types respectively. This method does not suffer from a black box data, but are spontaneous. The characteristics of the attributes are determined by prototype. Hence, the method can be tested with the other type of data. The LVQ method is done using Hebbian Learning (HB).This method is most likely to be applicable for real time pattern.

8. Decision Trees (DT)

Decision Trees [15] select the best features from each decision node on the construction of a tree with some criteria such as gain ratio and information gain. This system is simple and easier implementation. Decision trees can be expanded in 2 types: (i) Classification tree, with a range of symbolic class labels and (ii) Regression tree, with a range of numerically valued class labels. The algorithm performs learning and modelling based on the training data .The main advantage is the algorithm can work well with huge amount of data .This approach performs the classification, with high speed and the detection rate is high. The model needs more memory space and is not suitable for all types of attribute. Based on the experimental result the DR is 92.28 %.

9. Support Vector Machines (SVM)

SVM [16] can deal large dimensionality of data and do multi-class classification. By the method of nonlinear mapping real valued input feature vectors are mapped on to higher dimensional feature space. The accuracy of machine learning and data mining approaches depends on the amount of audit patterns available during training. It uses a hypothesis space of linear functions and maps input feature vectors into a higher dimensional space all the way through some nonlinear mapping [17].SVM constructs a hyper plane or set of hyper planes only the good separation is achieved by the hyper plane. The hyper plane searching process in SVM is achieved by the leading margin [16] [18]. The related margin gives the major separation between classes.

SVM has the advantage of high training rate and decision rate irrespective of the dimension of the input data, continuous correction of various parameters to increase in training data which endows the system with self-learning ability. Based on the analysis, this is one of the best classification approaches. There are three ways to apply SVM for intrusion detection.

i. SVM can be applied directly to locate the pattern of normal activities of a computer system. The incremental approach for monitoring network traffic is developed by proposed a rough set enhanced SVM model based on both sequences based and feature-based Data sets.

ii. ii. SVM is applied to find out the important features. The paper proposes the ranking of feature for an identification of attack.

SVM also have the ability to update the training patterns dynamically whenever there is a new pattern during classification.

10. Pattern Matching

Pattern Matching technique provides the assumption of independence among events, works with predefined set of patterns (known as signatures) to detect attacks. The system is efficient to detect the known intrusions and makes an alert, if exists an exact match of an attack, signature is determined by the result of less false alarm. The system cannot find the unseen attacks for which, signatures available are nil [19]. SNORT system [20] is constructed based on this technique.

11. Markov Models

Markov Chain [21] and Hidden Markov Model [22] can deal only with sequential representation of audit patterns. These models are useful in modelling sequences of system calls of a privileged process. The model cannot cope with a long range of dependencies between the observations [23]. The complexity of the system increases with modelling the ordering property of events, but it has good accuracy.

12.Genetic Programming

Genetic Programming (GP) [24] is an extension of Genetic Algorithm to detect the intrusion. In GA, fixed length of vectors is used to represent a solution, whereas GP encodes each chromosome using parse tree. The GP and GNP have the flexibility to represent the complex individuals. The Genetic Network Programming (GNP) based fuzzy class-association rule mining with sub-attribute utilization has been proposed by

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue IV, April 2018

Jiu et al. [25] for network intrusion detection. They used a graph based evolutionary optimization technique for GNP, which leads to enhance the representation ability with compact programs derived from the reusability of the nodes in the graph. It has the potential ability to derive the best classification rules and selecting optimal parameters. Genetic algorithm cannot assure constant optimal response time and also this mechanism leads to Over-fitting.

13.Fuzzy Logic

For reasons, purpose, dual logic's truth values can be either absolute false (0) or absolutely true (1), but in Fuzzy logic these kinds of restrictions are being relaxed [26]. That means in Fuzzy logic the range of the degree of truth, of a statement can hold the value between 0 and 1 along with '0' and '1'. Reasoning is Approximate rather than precise. Effective, especially against port scans and probes. The main drawback of the systems is high resource consumption Involved. The dynamic rule update at runtime is a difficult task with effective and very potential technique. Human decision making and reasoning is used in many engineering applications, but mainly in anomaly IDS which effective in port scans and probes involving high resource consumption.

B. Unsupervised Learning

An unsupervised learning algorithm is provided with the set of unknown features there exist [27]. The labelling mechanism is not essential factor in the Unsupervised Learning algorithm. This algorithm is robust to big variations than supervised approach. This has the ability to generalize the new types of attacks. The major drawback of this approach is the manual choice of the number of clusters. The important techniques are Cluster analysis (K-means clustering, Fuzzy clustering), Hierarchical clustering, Self-organizing map, Apriori algorithm, Eclat algorithm and Outlier detection (Local outlier factor).

1. Clustering

Clustering [28] is the fast classification method is able to apply on both Misuse detection and Anomaly detection. The similar members or attributes are grouped as a cluster and easy to make a label. Clustering is the most efficient approach for labelling and classifies the large amount of input data.

K-means clustering [29] is one of the simplest unsupervised clustering algorithms. The algorithm takes input parameter k and partition the 'n' dataset into 'k' cluster so that the intra-cluster similarity is high and intercluster similarity is low. K is a positive integer number given in advance. K means clustering takes less time as compared to the hierarchical clustering and yields better results.

2. Genetic Algorithms

Chittur [30] implemented intrusion detection using genetic algorithm. This technique also includes a machine learning approach called Genetic Algorithm for the identification of harmful or unwanted attacks on the network. The genetic algorithm detects intrusion on the basis of protocol used in the connection, the services used in the network and status. The genetic algorithm approach generates a set of rules where each of the rules identifies an attack type. The classification of network connection intrusions is also detected using these rules. There are six rules generated to classify various six different types of attacks. It will efficiently identify 100% accuracy for the detection and classification of intrusions.

Gonzalez and Dasgupta [31] applied a genetic algorithm, though they were examined host based IDS, not network based. They used the algorithm only for the Meta learning step instead of running algorithm directly on the feature set. It uses the statistical classifiers for labelled vectors. A 2-bit binary encoding methodology is used for identifying the abnormality of a particular feature, ranging from normal to abnormal. Hart and Stork [32] used a genetic algorithm with decision tree. The decision tree is used to represent the datawith the high detection rate and less false positive rate. The false positive occurrence was minimized by utilizing human input in a feedback loop.

C. Semi-Supervised Learning Methods for Detection

The lack of proper labelled Datasets and the speed at which hackers invent new attacks could make unsupervised and semi-supervised learning good candidates for future development of IDS. In fact, the IDS should be trained with traffic found on the network where it will be deployed in order to take into account the particular configuration of the network .Tawfiqet al. [33] conducted experiments and suggested to use semi-supervised method to solve the problem of test data being drawn from various sources. The four categories of semi-supervised learning methods are generative model, self-training, co-training and

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue IV, April 2018

graph-based learning methods. Data Mining uses two learning, supervised learning and unsupervised learning.

1. Data Mining and Machine Learning

Data Mining (DM) and Machine learning, deals with analyzing the audit pattern properties [34]. Some existing approaches are classier, decision trees, Bayesian classifiers and cluster analysis. Clustering is the preferable technique used in the building of frameworks such as K-means and Fuzzy C means [35].This technique forms the clusters based on the calculation of distance between the counterpoint of the cluster and the feature nearer to the specific cluster. This method is simple and efficient and has good performance in detecting known attacks. The main drawback of the system is the input must be numeric, since the distance measure is done for classification. Moreover, the system assumes the future as independent, so it is difficult to get the relationship among various features of a record which leads to less accurate. Euclidean distance is the familiar distance measures. Data mining approaches [36] build the classifiers by identifying the relevant patterns of the program and user behaviour to perform the detection based on mining association rules [36] and frequent episodes [37]. The record patterns are learned to describe the user behaviour using association rules and frequent episodes. The accuracy of detection is less when the rule is not in the database to compare for clustering.

2. StatisticalMethods

Statistical methods deal with the categorization based on the variables, and the test measure is done on those selected variables [38].There is any deviation of the calculated values with the normal values, then it is concluded regarding the existence of an attack. Modelling process is done and properties such as duration, frequency and user identity are exploited. Another important measure used in these systems is to identify the deviation with the help of the threshold value. The value of threshold fixing makes the task of classification crucial. The system cannot reliably detect the attack when the threshold value is high; otherwise the system raises large number of false alarms. To improve the performance of the system, the best features are selected like Intrusion Detection Expert System (IDES) [39].

Data sets

The data set provided for the 1999 KDD Cup was originally prepared by MIT Lincoln labs for the 1998 Defence Advanced Research Projects Agency (DARPA) Intrusion Detection, Evaluation Program, with the objective of evaluating research in intrusion detection, and it has become a benchmark data set for the evaluation of IDS. It contains approximately 49, 00,000 data instances. Attacks fell into one of the following categories: DOS-Denial of Service (e.g. a mail bomb), R2LUnauthorized access from a remote machine (e.g. sendmail), U2R-Unauthorized access to super user or root functions (e.g. a buffer overflow attack), Probing surveillance and other probing for vulnerabilities (e.g. port scanning) [40].

V. PROPOSED APPROACH

From the study, it is observed that the semi supervised learning approach provides the effective mechanism to do the classification. Support Vector Machine is the suitable algorithm for classification. In general, the classification time is high due to the task of training and testing. Training time can be reduced by pre-processing the input data set and selection of features. The proposed method uses the pre-processing method, such that the data is converted to work in a nonlinear transformation feature space and SVM can easily handle the data. The computation time for the detection of attack is reduced, because of the feature selection approach. Feature selection performs the removal of redundant and irrelevant features.

VI.CONCLUSION

The performance of the detection of the attack depends on the classification algorithm. The algorithm must handle large amount of data and works with the large number of rules. Always there is a focus to achieve a high percentage of accuracy and less percentage of false identification of attack. The machine learning algorithm has the ability to detect new type of attack and achieve high accuracy.

Abbreviations

ANN:Artificial Neural Network;DAG:Direct Acyclic Graph;DOS: Denial of Service ;DR: Detection Rate ;GNP:Genetic Network Programming;GP:Genetic Programming ;HB:Hebbian Learning ;HIDS: Host-based IDS;IDES:Intrusion Detection Expert System ;IDS: Intrusion Detection System ;LOF:Local Outlier Factor ;LVQ:Supervised Learning Vector Quantization ;MINDS: Minnesota Intrusion Detection System ;MLP:Multilayer perception ;MSE:MeanSquared Error ;NB: Naïve Bayes;NIDS :Network based IDS ;RF:Random Forest ;SVM:Support Vector Machines .

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue IV, April 2018

Competing interests
The authors declare that they have no competing interests.

REFERENCES

[1]. Kendall, K., A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, Master's Thesis,1999.

[2].D.E.Denning, "An Intrusion Detection Model," *IEEE Transactions on Software Engineering*,vol.13,no. 2,pp. 222–232,1987.

[3]. L.Ertoz, E.Eilertson, A.Lazarevic, P.Tan, J.Srivastava, V.Kumar and P.Dokas, *MINDS - Minnesota Intrusion Deduction System*, MIT Press 2004.

[4].Vishal Parande and SharadaKori,"*HostBased Intrusion Detection System*," International Journal of Science and Research, vol,4,no.4,pp.559-561,2015.

[5].Abhinav Jain, Sanjay Sharma and Mahendra Singh, "*Network Intrusion Detection by using Supervised and Unsupervised Machine Learning Techniques: A Survey*," International Journal of Computer Technology and Electronics Engineering, vol. 1.no.3, pp.1-13,2011.

[6] D.Heckerman, A Tutorial on learning wth Bayesian networks, Microsoft Research,Technical Report,pp.4-19,1995.

[7].J.M.Jemili, M.Zaghdoud and M.Ahmed, "Intrusion Deduction Based on Hybrid propagation in Bayesian Networks," *In proceedings of the IEEE international conference on Intelligence and security informatics,* Dallas.137-142,2009.

[8]. K. Jayakumar, T. Revathi and S. Karpagam,"*Intrusion Detection using Artificial Neural Networks with Best Set of Features,"* The International Arab Journal of Information Technology, vol.12,no.6A,pp. 728- 735,2015.

[9].R.Battiti, "Using Mutual Information for Selecting Features in Supervised Neural Net Learning*," IEEE Transactions of Neural Network*,vol. 5.no.4,pp.537-550,1994.

[10].Srinivas Mukkamala, Guadalupe Janoski and Andrew H Sung ,"Intrusion Deduction Using Neural Networks and Support Vector Machines," *In Proceedings of the International Joint Conference on Neural Networks*, IEEE, 2002,pp.1702–1707.

[11].R.Rojas,"A Systematic Approach," *Neural Networks*,Springer-Verlag, 1996.

[12]. S.Saravanan and R.M.Chandrasekaran, "Intrusion Detection System using Bayesian Approach,"*International Journal of Engineering and Innovative Technology*, vol.4,no.2,pp.107-110,2015.

[13]. L.Breiman,"Random Forests," *Machine Learning*,vol.45,no.1,pp. 5-32,2001.

[14]. T.Kohonen, *Learning Vector Quantization*, The Handbook of Brain Theory and Neural Networks, MIT Press, Cambridge, MA, USA. 537 – 540 ,1998.

[15].J.Markey,*Using Decision Tree Analysis for Intrusion Detection: A How-To Guide,*.SANS Institute InfoSec Reading Room,2011.

[16].C.Cortes and V.Vapnik,"Support Vector Networks," *Machine Learning*,vol.20,no.3,pp. 273-282,1995.

[17].Andrew H Sung and Srinivas Mukkamala, "Identifying Important Features for Intrusion Deduction Using Support Vector Machine's and Neural Networks," *In Proceedings of Symposium on Applications and the Internet,*IEEE,200),pp.209–216.

[18]. Srinivas Mukkamala, Guadalupe Janoski and Andrew H Sung, "Intrusion Deduction Using Neural Networks and Support Vector Machines," *In Proceedings of the International Joint Conference on Neural Networks* , IEEE,2002,pp.1702–1707.

[19]. Rebecca Bace, Peter Mell,*Intrusion Deduction Systems*, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology,2001.

[20].Mark D. Tollison,*An Analysis of the Snort Network Intrusion Detection System* ,Global Information Assurance Certification Paper,2000.

[21].K.Jha, Tan and R.A.Maxion,"Markov chains, Classifiers, and Intrusion Deduction," *In Proceedings of the 14th IEEE Computer Security Foundations Workshop*, IEEE,2001, pp.206-219.

[22].Wei Wang, Xiao-Hong Guan and Xiang-Liang Zhang, "Modelling Program Behaviours by Hidden Markov Models for Intrusion Deduction," *In Proceedings ofInternational Conference on Machine Learning and Cybernetics,* IEEE,2004,pp.2830–2835.

[23].John Lafferty, Andrew McCallum and Fernando Pereira,"Conditional Random Fields: Probabilistic Models for Segmenting and Labelling Sequence Data," *In Proceedings of Eighteenth International Conference on Machine Learning*, Morgan Kaufmann.pp.282-289,2001.

[24]. Mohammad Sazzadul Hoque ,Abdul Mukit and Abu NaserBikas," An Implementation of Intrusion Detection System using Genetic Algorithm," *International Journal of Network Security & Its Applications,*vol.4,no.2,pp.109 - 120,2012.

[25] .Jiu-Ling Zhao, Jiu–Fen Zhao and Jian –Jun Li,"Intrusion Detection Based on Clustering Genetic Algorithm," *International Conference Based on Machine Learning and Cybernetics, IEEE, Guangzhou,2005,*pp.3911-3914

[26].J.Luo and S.M.Bridges,"Mining Fuzzy Association Rules and Fuzzy Frequency Episodes for Intrusion Detection," *International Journal of Intelligent* Systems,vol. 15,no. 8,pp.687-704,2000.

[27]S..Zanero and S.M.Savaresi, "Unsupervised learning Techniques for an Intrusion Deduction System," *In SAC '04: Proceedings of the 2004 (ACM symposium on Applied computing*, New York,2004,pp.412-419

[28]. Manish Somani and RoshniDubey, "Hybrid Intrusion Detection Model Based on Clustering and Association," *International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering* ,vol.3,no.3,pp.154-164,2007.

[29].E.Portnoy, Eskin and S.Stolfo, *"Intrusion Deduction with Unlabeled Data using Clustering," In Proceedings of the ACM Workshop on Data Mining Applied to Security, ACM*.,2001.

[30]. Chittur, "A Model generation for an Intrusion DetectionSsystem using Genetic Algorithms," Ph.D. dissertation , Columbia University ,2001.

[31]. A.Gonzalez and D.Dasgupta, "An Immunity-based Technique to Characterize Intrusions in Computer Networks," *IEEE Trancactions on Evolutionary Computation,*vol. 6no.3,pp. 281-291,2002.

[32].R.O.Hart and D.G. Stork, *Pattern Classification*, 2nd edition. Wiley, Hoboken,2000.

[33].S.Tawfiq,Barhoom, A.Ramzi and A.Matar, "Network Intrusion Detection Using Semi - Supervised Learning

Based on Normal Behaviour's Standard Deviation," *International Journal of Advanced Research in Computer and Communication Engineering*, vol.4,no.1,pp.375-385,2015.

[34].Nahla Ben Amor, Salem Benferhat and ZiedElouedi, "Naive Bayes vs Decision Trees in Intrusion Deduction Systems," *In Proceedings of the ACM Symposium on Applied Computing, (ACM,2004)*,pp.420-424.

[35].Paul Dokas, LeventErtoz, Vipin Kumar, AleksandarLazarevic, JaideepSrivastava and Pang-Ning Tan, "Data Mining for Network Intrusion Deduction," *InProceedings of the NSF Workshop on Next Generation Data Mining*,pp.21-30,2002.

[36].R.T.Agrawal and Imielinski,"Swami, Mining Association Rules between Sets of Items in Large Databases," *In Proceedings of the International Conference on Management of Data ,(ACM,1993)*,pp.207-216.

[37]. H.Mannila, H.Toivonen and A.I.Verkamo, "Discovering Frequent Episodes in Sequences," *In Proceedings of the 1st International Conference on Knowledge Discovery and DataMining, pp.*210-215,1995.

[38].Animesh Patcha, Jung-Min Park, "An Overview of Anomaly Deduction Techniques,Existing Solutions and Latest Technological Trends,"*Computer Networks*, vol.51,no.12, pp.3448-3470 ,2007.

[39]. Robert Kolacki, *A Real-Time Intrusion-Detection Expert System (IDES*), SRI International,no.63,1992.

[40]. KDD, KDD Cup, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, Accessed October 2007