Volume 5, Issue 3, March 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review of Various Classification Techniques Based on Data Mining for Intrusion Detection

[1]Anju, [2]Pardeep Kumar Mittal, [3]Shalini Aggarwal
[1]Scholar, [2]Astt. Professor, [3]Teacher Fellow
[1, 2, 3] Department of Computer Science & Application Kurukshetra University,
Kurukshetra, Haryana, India

Abstract- Security of information system has become an important issue these days because of increasing number of public and private services used through the internet. Due to the increasing risk, Intrusion Detection Systems (IDS) have become a critical component to secure the systems and network. Data mining is a technique that provides higher automated capabilities to detect intrusion. Data mining techniques such as classification, clustering and association rule are used for intrusion detection. This review paper aims to present various data mining classification techniques for intrusion detection.

Keywords- Intrusion Detection System, Misuse Detection, Anomaly Detection, Classification, Decision Tree.

I. INTRODUCTION

In the present era, due to the increase in use of internet for services, risk of intrusion and authentication has also increased. An intrusion is defined as set of actions that attempts to compromise the integrity, confidentiality or availability of resources*[1] [2]*. Intrusion detection is defined as a process of monitoring the events that occur in a computer system or network and analyzing them for detect intrusions*[3]*. Intrusion detection is categorized into two types-misuse detection and anomaly detection. In anomaly detection new threats are detected based on the detection of any deviation from the existing model of normal and expected behavior of the system*[1] [4]*. A basic assumption of anomaly detection is that attacks differ from normal behavior *[5]*. In misuse detection, IDS detect attacks on the basis of predefined and existing model for specific known attacks*[3]*. It has high speed of detection and low percentage of false alarm. In anomaly detection technique new threats can be detected whereas in misuse detection only known threats arediscovered*[1] [4] [6]*.

Data mining is defined as the process of discovering interesting knowledge from large amount of data *[7]*. It is an automated technique used to discover the undetected relationships among the data items. Various data mining techniques are classification, clustering and association rule. Classification maps the data into various predefined categories*[8]*. The goal of classification is to find a general mapping to predict classes for unknown data objects and to find a compact and understandable class model for each class *[9][2]*.

II. LITERATURE REVIEW

Peyman and Ali *[1]* have shown that anomaly based intrusion detection is best. But due to occurrence of high false positives in these systems hybrid approach is used. In hybrid approach, misuse detection approach is used with anomaly based approach. Mitchell and Deepali*[2]* presented a survey on clustering algorithms namely K-means, Y-means and Fuzzy C-means. Among these Fuzzy C-means can be considered as an efficient algorithm since it allows an item to belong to more than one cluster and measures the quality of partitioning. Fuzzy C-clustering also offers high detection rate and lower false positive rate for intrusion detection. Tripti and Khomlal *[3]* have presented the basic concepts and requirements for IDS. Functional requirements and classification of IDS have also been presented.

V. Jaiganesh, S. Mangayarkarasi and Dr. P. Sumathi *[4]* have proposed different types of intrusion detection system and highlights techniques of intrusion detection. In this paper various data mining algorithms for IDS implementation have been presented such as Support Vector Machine, kernelized support vector machine, extreme learning machine and kernelized extreme learning machine. Manoranjan, Sateesh and Sudhir *[5]*have shown that neural network can be used as a method for training and learning IDS with classification rate of 100% and false positive rate of 0%. To classify traffic correctly neural network does not need huge amount of training data and detect unknown attacks.

Amanpreet, Gaurav and Gulshan *[6]*have presented a survey on various types of intrusion, intrusion detection methodologies, data mining classification and clustering techniques. Sneha and Maneesh *[7]*have presented a study of various types of attacks and data mining classification techniques. A comparative approach is proposed to get the performance rate of four data mining approach. Comparative approach shows that in user to root attacks detection rate is less in all these classifier.S. Neelima, N. Satyanaeayana and P. Krishna *[8]*have presented a survey of various data mining techniques. Different data mining techniques are classification, clustering and rule based association. These techniques are mainly used because of their capability to drastically improve the performance and usability of IDS.

Kamini and Divakar *[9]* have shown the vulnerabilities on data mining based IDS in mobile and ad hoc networks and introduced the security schemes for them.After reviewing various techniques, their merits and demerits are shown. Ajayi, Idown and Anyaehie *[10]* have shown various data mining algorithm. Due to each of the approach has its own advantages and disadvantages, it has been suggested that combining more than one algorithm may be used to remove the disadvantages of other. P. Amudha, S. Karthik and S. Sivakumari *[11]*have proposed various classification techniques for evaluating the performance of intrusion detection model. Most of researchers performed experiments using 10% of the overall KDD cup'99. Decision tree obtained higher accuracy but naïve bayes obtained a higher detection rates. SVM received 99.50% accuracy during training. To obtain better detection rate with SVM in less time hybrid approach is used. Abhaya, Kaushal, Ranjeeta and Sumaiya*[12]*have analyzed different classification and clustering data mining techniques for intrusion detection based on the detection rate, accuracy, execution time and false alarm rate. Execution time of SVM is less and produces a higher accuracy with smaller dataset while decision tree has higher detection rate in case of large dataset. Execution time of K-Means clustering is less in case of smaller dataset but for larger data set K-Medoids performs better.

Patel, Bharat and Hiren *[13]* have presented the comparative review of different algorithms like decision tree, naïve bayes (NB), NB tree for intrusion detection. A NB tree analyses the large volume of network data and considers the complex properties of attack behavior. Shyara and Saroj *[14]* have shown Naïve Bayes Classifier for analyzing large number of network logs or audit data. It also improves the performance of IDS. The authors have testednaïve bayes algorithm on KDD99 dataset and it was observed that the balance detection rate was maximized and false positive rate was minimized at acceptable level.

Mrutyunjaya and Manas *[15]*have proposed a framework of network IDS based on naïve bayes algorithm. Compared to neural network approach this approach achieve higher detection rate, less time consuming and has low cost factor. Dewan, Mohammad and Chowdhary*[16]* have introduce a new algorithm for adaptive intrusion detection based on boosting and naïve Bayesian classifier. Authors tested the performance of proposed algorithm with existing data mining algorithm and the experimental results manifest that the proposed algorithm has achieved higher detection rates and reduced the performance of false positives for different types of network intrusions. Reema et al. *[17]*have presented various data mining classification techniques and performed their comparison using WEKA. The results show that Artificial Neural Network has outperformed all the other techniques used.

Neha and Shikha *[18]* presented a decision tree technique that categorizes new data into a number of predefined categories. After the creation of tree the logic can be incorporated from decision tree into many intrusion detection technologies.Yogita and Kalyani*[19]* have shown that by using SVM in IDS can reduce the time required to build a model for classification and can increase the intrusion detection accuracy. Vahid *[20]* has presented a research on new techniques for intrusion detection and evaluate their performance based on the KDD cup 99 intrusion data. Results have shown that hybrid C5.0-SVM outperforms than SVM. It gives 100% accuracy for probe, U2R and R2L attacks. M. Govindarajan et al. *[21]* has been evaluated the performance of new techniques based on NSL-KDD dataset. Authors have proposed a hybrid intrusion detection network system to make optimum use of best performance. The hybrid RBF-SVM has shown higher percentage of classification accuracy and enhances the testing time due to data dimensions reduction. Riti and Manish *[22]* have presented two categories for separating data into two distinct sets i.e. normal data and abnormal data. Results have shown that for classifying normal and abnormal data k-nearest neighbor give better results than SVM but it takes more time for its execution. Deepika and Vineet *[23]* have presented IDS using KNN classification and dempster theory for detecting intrusion behavior with in network. From the observed results it was observed that KNN and dempster can perform better. Phyu and Kyaw *[24]* have presented a comparison of various data techniques. Random forest will process in filtering stage and KNN will use as a classifier because it can get high accuracy and true positive rate in detecting the denial of service attack. Sandhya, Ajith and Johnson*[26]* have presented neural networks, decision tee and SVM for IDS. Neural networks are suitable for misuse and anomaly detection whereas decision tree and SVM are only for misuse detection.

Deepika and Alpha *[27]*have presented the architecture of IDS, features of an ideal IDS and challenges for IDS. According to this paper, neural network and machine learning are used to overcome the challenges of IDS and SVM is used to deal with classifier construction problem. According to *[28]*, performance metrics and quantifiable results have been determined as to two challenging issues in intrusion detection. Also completeness, correctness and performance are the three most important qualities that need to be measured in order to evaluate IDS. Mostaque Md. Morshedur Dassan *[29]* has presented intrusion detection technologies and detection challenges that affect the decision policy of IDS. To reduce the false alarm rate author proposed the new definition of complement of fuzzy sets. Manish et al. *[30]* surveyed trends in multiagent IDS research. In this paper authors have introduced two phases of program execution. The first phase uses a malware profile pattern matching mechanism and second phase uses a program profile matching mechanism.

III. USAGE OF DATA MINING IN INTRUSION DETECTION

Intrusion detection is a passive approach*[8]*. Data mining analyze the observed sets to discover the unknown relationships and summarize the results in order to make the owner of the data to understand*[2]*.

Data mining can help intrusion detection in the following way:

a) Remove normal activity from alarm data to allow analysts to focus on real attacks. Data mining is based on the process of scanning abnormal activity through code variants instead of unique signatures.

b) Identify false alarm generators. In case of false positive, data mining can be used to identify valid network activity that can be filtered out by identifying false alarm generators.

c) Find activity which uncovers a real attack. Data mining help intrusion detection by identify valid network activity so that it can filter it out abnormal activities.
d) Identify long, ongoing patterns. Data mining has the capability to identify or extract data and provide analysts with different views of data to help in their analysis
e) In false negative, those attacks are detected for which there are no known signatures *[10] [7] [2]*.

IV. CLASSIFICATION TECHNIQUES FOR INTRUSION DETECTION

Classification is an automated process of categorizing each instance into one of the predefined categories. It is mainly used for anomaly detection *[2]*.Classification process is divided into two steps: In first step, training set made up of data instances and their associated class labels are used to build a classifier. During the second step, build classifier is used to predict the class for unlabeled data instance*[11]*. Classification techniques which are used to classify the intrusion detection databases are: Bayesian classification, Decision tree, k-Nearest neighbor, Support Vector Machine, Neural Network and Rule Induction Methods*[11][12]*.
Intrusion detection can be considered as a classification problem in which each audit data can be classified into possible set of categories such as normal, abnormal or a particular kind of intrusion. After that classification algorithm is used to build a classifier. This classifier will then use to predict class of new unseen audit data as “normal”, “abnormal” or particular intrusion *[11]*.

A. Naïve Bayes

Naïve Bayes is a probabilistic classifier mainly used to predict the likelihood of group members. It is an advancement of Bayes theorem and it assumes conditional independence of class*[13]*.Naïve Bayes Intrusion Detection Algorithm first finds out prior probability and then class conditional probability for the given intrusion data set. Next step is to find the highest class probability after which the detection rate and false positive rate is calculated*[14]*. Figure 1 shows the framework for a naïve bayesian model to perform intrusion detection*[15]*.

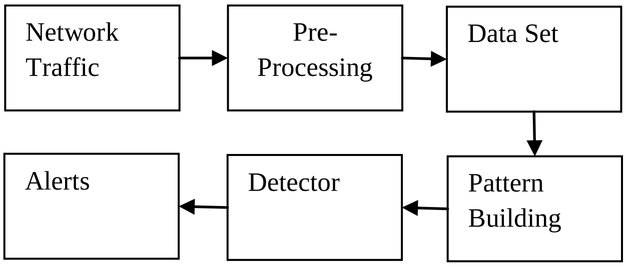

Fig. 1 The framework of intrusion2w detection model

The naïve bayes classifier operates on a strong independence assumption i.e. probability of one attribute does not affect the probability of other. It makes 2n! independent assumptions by a series of n attributes. Figure1 shows the framework for a Naïve Bayesian model to perform intrusion detection*[15]*.
The naïve bayes classifier can easily handle missing attribute values by simply omitting the probability when calculating the likelihoods of membership in each class*[16]*.

B. Decision Tree

Decision trees can learn a model based on the training data and can predict the future data as one of the attack type. Due to this they can be used as misuse intrusion detection *[17]*. Two prerequisites for the analysis are data collection (i.e. identifying and collecting data) and tool acquisition and selection (i.e. identifying and deploying data mining tools). Figure 2 shows the process to implement decision tree for intrusion detection *[18]*.

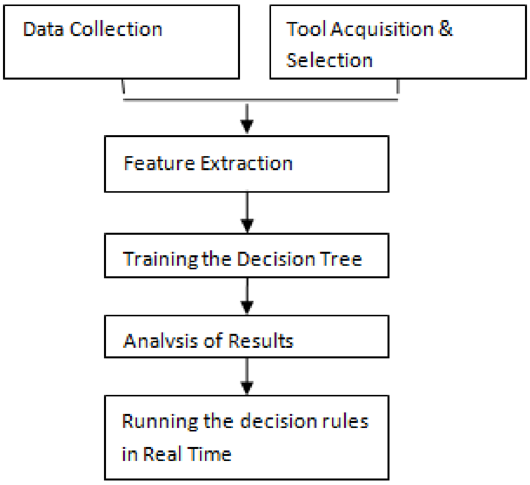
Data Collection
Tool Acquisition & Selection
Feature Extraction
Training the Decision Tree
Analysis of Results
Running the decision rules in Real Time

Fig.2Process to implement decision tree for intrusion detection

To classify a new instance, start at the root node and follow the branch indicated by the outcome of each test until a leaf node is reached. Leaf node label represents the result of classification *[13]*. They are useful in real time intrusion detection because of their high performance. Due to generalization accuracy of decision tree, they are able to detect new intrusions *[14]*.

C. Support Vector Machine

In IDS we have to construct a SVM model for classification. SVM aims to produce a model that produces the target value of a data instance*[19] [20]*. Various kernel functions are used to achieve this aim. Three major SVM kernel functions are: Gaussian Kernel, Polynomial Kernel, and Sigmoid Kernel. In classification phase, SVM training model is build and to generate classification results SVM functions are used*[19]*. The basic formulation can be extended to the nonlinear case by using nonlinear kernels that maps the input space to a higher dimensional feature space *[21] [20]*.

The two main reasons for using SVM for intrusion detection are speed and accuracy *[11]*.The implementation of SVM intrusion detection system has two phases: training and testing. Whenever a new pattern is detected during classification it updates the training pattern dynamically. It provides high accuracy rates *[10]*.

D. K-Nearest Neighbor

If the prior knowledge of data is unavailable or discriminate analysis is to be performed when reliable parametric of probability density are unknown or difficult to determine then K-NN classification is applied *[22]*. In K-Nearest Neighbor (k-NN) objects are classified based on closest training example in the feature space. It is a type of lazy learning*[23]* because functions are approximated locally and all the computations are delayed until classification*[17]*. Figure 3 shows the method for deciding the nearest neighbor.

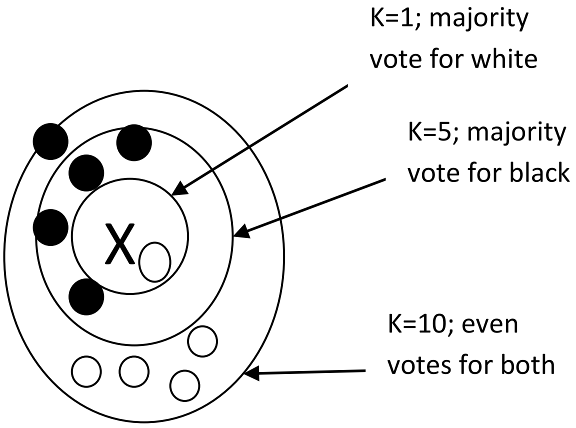
K=1; majority vote for white
K=5; majority vote for black
X
K=10; even votes for both

Fig. 3 Majority voting scheme

The 1-Nearest Neighbor (1NN) classifier id based on representative points. In the 1NN algorithm, whole train samples are taken as representative points and the distance from the test samples to each representative point are computed. Test samples assigned same class label as the representative point nearest to them. The k-NN is an extension of 1NN in which test samples are determined by finding the k nearest neighbors *[24]*.Mostly it is used with statistical schemes for intrusion detection*[17]*.

E. Artificial Neutral Networks

Neural networks have been used both in anomaly intrusion detection and in misuse intrusion detection. In case of anomaly IDS, neural networks identify the variations from user’s established behavior while in case of misuse IDS, neural networks have been designed to receive the data from network and analyze it for any occurrence of misuse*[25]*. In case of anomaly detection, the system learns to predict the next command based on the sequence of previous commands. In this case, a shifting window of w recent commands is used *[17]*.

For misuse detection, neural networkscan be implemented in two ways. The first method filters the incoming data to detect any suspicious event and forward it to expert system. The second method implements neural network as a standalone misuse detection where data is received from a network stream and then analyzed for any misuse intrusion *[26]*.

Neural network would be capable of analyzing the data from network, even if the data is incomplete or distorted *[25]*.

V. POTENTIAL ISSUES FOR INTRUSION DETECTION SYSTEMS

a) Feature Extraction: If the features are improperly selected then the performance of system will be influenced a lot.

b) Classifier construction: Classifier constriction is another technical issue that affects the performance of IDS. It is difficult to find the new intrusion based on the small training set.

c) Sequential pattern prediction: Because of intrinsic temporal relationships between a single short sequence of system calls so it difficult to detect it as normal or abnormal *[27]*.

d) Human Intervention: After lot of enhancements IDS still require human intervention for some tasks. Expert rule set must be constructed by a human domain expert. IDS technology recommends some automation such as reporting the administrator in case of malicious activity, avoiding the malicious connection for a configurable period of time, etc. But security administrator must investigate the attack once it is detected and reported, to determine how it is occurred, correct the problem and take necessary action to prevent the occurrence of the same attack in the future*[28][29]*.

e) Historical analysis: Monitoring the logs on the daily basis is required to analyze the type of malicious activities detected by IDS over a period of time. Today's IDS still require a manual activity for historical analysis of intrusive activities detected over a period of time.

f) False positive and false negative alarms rate: IDS should be implemented in such a way that it raises minimum false positive and negative alarms. False positive takes place when the IDS erroneously identify a problem. False negative means detecting an attack for which there are no known signatures and IDS does not generate an alarm when an intrusion is actually takes place. Both create problems for security administrators and demands that malicious attacks are detected correctly.

g) Signature database: To detect attacks IDS is to remember signatures of known attacks. The signature database needs to be update whenever a new attack is detected *[29] [30]*.

Table 1 shows comparison of various data mining tools according to their capability, learnability, interoperability and flexibility. Using equal weights for each category and equal spacing between scale intervals, the best tools within each group are: S-plus for decision tree, DataMind for Rule induction, PRW for Neural networks, and ModelQuest Expert and NeuroShell2 for Polynomial Networks. Overall, the network methods (Polynomial and Neural) are more accurate than the portioning methods (Tree and Rules).

Table 1: Capability, Learnability, Interoperability, Flexibility

		Capability					Learnability				Interoperability			Flexibility			
Technology	Data Mining Tools	Handles Missing Data	Allows data transformations	Quality of testing options	Provides useful output reports	visualization	Tutorials	Wizards	User's manual	Online help	Importing data	Exporting data	Links to other applications	Model adjustment flexibility	Customizable work environment	Ability to write or change code	Overall (average groups)*
Tree	CART	+	+	+	+	+	√	None	+	+	-	-	-	+	√	+	√
	Scenario	+	√	--	√	+	+	+	+	+	++	+	+	--	√	-	√
	See5	+	-	√	+	-	√	None	NE	+	√	+	√	+	--	-	√
	S-Plus	+	++	+	++	+	√	None	+	+	++	++	++	+	+	++	+
	Tree Average*	+	+	√	+	+	√	--	+	+	+	+	+	√	√	√	√+
Rule	WizWhy	+	-	√	+	√	+	-	√	√	+	-	√	√	√	--	√
	DataMind	++	√	+	++	++	++	++	+	+	++	+	+	√	√	--	√+
	DMSK	--	++	√	-	--	None	None	--	-	-	√	√	√	--	--	-
	Rule Average*	√	√	√	+	√	√	-	√	√	+	√	√	√	-	--	√
Neural	NeuroShell 2		--	-	√	-	+	√	None	+	√	--	--	-	-	--	-
	PcOLPARS	--	√	√	√	++	√	None	√	-	--	√	--	++	-	--	-
	PRW	√	++	++	√	+	+	√	+	+	++	++	++	++	-	-	+
	Neural Avg.*	-	√	√	√	+	+	-	-	√	√	√	-	+	-	--	√-
Poly Net	MQ Expert	+	+	+	+	+	√	√	√	√	√	√	√	+	√	√	√+
	Neuroshell 2	++	+	-	-	-	-	-	√	√	√	√	√	-	+	√	√
	Gnosis	√	--	√	-	-	√	-	+	√	-	--	--	-	-	√	-
	K'Miner	--	--	√	-	√	√	--	None	-	-	--	√	√	√	--	-
	PolyNet Avg. *	√	√	√	√	√	√	-	√	√	-	√	√	√	√	√	√-
	Overall Avg.*	√	√	√	√	√	√	-	√	√	√	√	√	√	√	-	√

Legend: ++=Excellent, +=Good, √=Average, -=Needs Improvement, --=Poor, None=Does not Exist, NE=Exists, but Not Evaluated

VI. CONCLUSION

Intrusion has become a bottleneck in networks and host-based systems. A powerful Intrusion Detection System is therefore required to overcome these problems. Data mining techniques can be used in this field for better decisions and to detect any occurrence of intrusion. Various classification algorithms are available for this problem and can be used on the basis of their time and space complexity.

REFERENCES

[1] Peyman Kabiri and Ali A. Ghorabani, “Research on Intrusion Detection and Response: A Survey”, International Journal of Network Security, Vol. 1, Issue 2, Sep. 2005, Pp. 84-102.

[2] Mitchell D’silva, Deepali Vora, “Comparative Study of Data Mining Techniques to Enhance Intrusion Detection”, International Journal of Engineering Research and Applications, Vol. 3, Issue 1, ISSN: 2248-9622, Jan-Feb 2013, Pp. 1267-1275.

[3] Tripti Sharma, Khomlal Sinha, “Intrusion Detection Systems Technology”, International Journal of Engineering and Advanced Technology, Vol. 1, Issue 2, ISSN: 2249-8958, December 2011, Pp. 28-33.

[4] V. Jaiganesh, S. Mangayarkarasi, Dr. P. Sumathi, “Intrusion Detection Systems: A Survey and Analysis of Classification Techniques”, International Journal of Advanced Research in Computer Engineering, Vol. 2, Issue 4, ISSN: 2319-5940, April 2013, Pp. 1629-1635.

[5] Manoranjan Pradhan, Sateesh Kumar Pradhan, Sudhir Kumar Sahu, “Anomaly Detection Using Artificial Neural Network”, International Journal of Engineering Sciences & Emerging Technologies, Vol. 2, Issue 1, ISSN: 2231-6604, April 2012, Pp. 29-36.

[6] Amanpreet Chauhan, Gaurav Mishra, Gulshan Kumar, “Survey on Data Mining Techniques in Intrusion Detection”, International Journal of Scientific & Engineering Research, ISSN: 2229-5518, Vol. 2, Issue 7, July 2011, Pp. 1-4.

[7] Sneha Kumari, Maneesh Shrivastava, “A Study Paper on IDS Attack Classification Using Various Data Mining Techniques”, International Journal of Advanced Computer Research, Vol. 2, No. 3, Issue 5, ISSN: 2249-7277, September 2012, Pp. 195-200.

[8] S. Neelima, N. Satyanarayana and P. Krishna Murthy, “Data Mining Techniques in Intrusion detection”, International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol. 4, Issue 2, Feb 2014, Pp. 631-634.

[9] Kamini Maheshwer and Divakar Singh, “A Review of Data Mining based Intrusion Detection Techniques”, International Journal of Application or Innovation in Engineering & Management, ISSN: 2319-4847, Vol. 2, Issue 2, Feb. 2013, Pp. 134-142.

[10] Ajayiadebowale, Idown S.A, AnyehieAmarachi A, “Comparative Study of Selected Data Mining Algorithms Used For Intrusion Detection”, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Vol. 3, Issue 3, July 2013, Pp.237-241.

[11] P. Amudha, S. Karthik, S. Sivakumari, “Classification Techniques for Intrusion Detection – An Overview”, International Journal of Computer Applications (0975-8887), Vol. 76, No. 16, August 2013, Pp.33-40.

[12] Abhaya, Kaushal Kumar, Ranjeeta Jha, Sumaiya Afroz, “Data Mining Techniques for Intrusion Detection: A Review”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 6, ISSN: 2319-5940, June 2014, Pp. 6938-6942.

[13] Patel Hemant, Bharat Sarkhedi, Hiren Vaghamshi, “Intrusion Detection in Data Mining With Classification Algorithm”, International journal of Advance Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2320-3765, Vol. 2, Issue 7, July 2013, Pp.3063-3070.

[14] Shyara Taruna R., Mrs. Saroj Hiranwal, “Enhanced Naïve Bayes Algorithm for Intrusion Detection in Data Mining”, International Journal of Computer Science and Information Technologies, ISSN: 0975-9646, Vol. 4, Issue 6, 2013, Pp.960-962.

[15] Mrutyunjaya Panda, Manas Ranjan Patra, “Network Intrusion Detection Using Naïve Bayes”, International Journal of Computer Science and Network Security, Vol. 7, No. 12, December 2007, Pp. 258-263.

[16] Dewan Md. Farid, Mohammad Zahidur Rahman, Chowdhary Mofizur Rahman, “Adaptive Intrusion Detection based on Boosting and Naïve Bayesian Classifier”, International Journal of Computer applications, Vol. 24, No. 3, ISSN: 0975-8887, June 2011, Pp. 12-19.

[17] Reema Patel, Amit Thakkar, Amit Ganatra, “A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems”, International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Vol. 2, Issue 1, March 2012, Pp.265-271.

[18] Neha Jain, Shikha Sharma, “The Role of Decision Tree Technique for Automating Intrusion Detection System”, International Journal of Computational Engineering Research, Vol. 2, Issue 4, ISSN: 2250-3005, August 2012, Pp. 1076-1078.

[19] Yogita B. Bhavsar. Kalyani C. Waghmare, “Intrusion Detection Systems Using Data Mining Technique: Support Vector Machine”, International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol. 3, Issue 3, March 2013, Pp.581-586.

[20] Vahid Golmah, “An Efficient Hybrid Intrusion Detection system based on C5.0 and SVM”, International Journal of Database Theory and Application, Vol. 7, No. 2, ISSN: 2005-4270, Pp. 59-70.

[21] M. Govindarajan, RM. Chandrasekaran, “Intrusion Detection using an Ensemble of Classification Methods”, Proceedings of World Congress on Engineering and Computer Science 2012.1, ISSN: 2078-0958, 2012.

[22] Riti Lath, Manish Shrivastava, “Analytical Study of Different Classification Technique for KDD Cup Data’99”, International Journal of Applied Information Systems, ISSN: 2249-0868, Vol. 3, Issue 6, July 2012, Pp. 5-9.

[23] Deepika Dave, Prof. Vineet Richhariya, “Intrusion Detection with KNN Classification and DS- Theory”, International Journal of Computer Science and Information Technology & Security, ISSN: 2249-9555, Vol. 2, Issue 2, April 2012, Pp. 274-281.

[24] Phyu Thi Htun and Kyaw Khaing, “Detection Model for Daniel-of-Service Attacks using Random Forest and k-Nearest Neighbors ”, International Journal of Advanced Research in Computer Engineering & Technology, ISSN: 2278-1323, Vol. 2, Issue 5, May 2013, Pp.1855-1860.

[25] E. Kesavulu Reddy, “Neural Network for Intrusion Detection and Its Applications”, Proceedings of the World Congress on Engineering 2013, Vol. 2, ISSN: 2078-0958, July 2013.

[26] Sandhya Peddabachigari, Ajith Abraham, Juhnson Thomas, “Intrusion Detection Systems Using Decision Trees and Support Vector Machines” International Journal of Applied Science and Computations, USA, 2003.

[27] Deepika P Vinchurkar, Alpa Reshamwala, “A Review of Intrusion Detection Systems Using Network and Machine Learning Technique”, International Journal of Engineering Science and Innovative Technology, ISSN: 2319-5967, Vol. 1, Issue 2, Nov. 2012, Pp.54-63.

[28] Douglas J. Brown, Bill Suckow, Tianqiu Wang, “A Survey of Intrusion Detection System”,

[29] Mostaque Md. Morshedur Hassan, “Current Studies on Intrusion Detection Systems, Genetic Algorithm and Fuzzy Logic”, International Journal of Distributed and Parallel Systems, Vol. 4, Issue 2, March 2013, Pp.35-47.

[30] Manish Kumar, Dr. M. Hanumanthappa, Dr. T. V. Suresh Kumar, “Intrusion Detection Systems Challenges for Wireless Network”, International Journal of engineering Research and Applications, Vol. 2, Issue 1, ISSN: 2248- 9622, Jan-Feb 2012, Pp. 274-280.