Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

TREE BASED CLASSIFICATION METHODS FOR INTRUSION DETECTION SYSTEM: A Survey

[1]Rizwan Ullah Siddiqui, [2Ashish] Mishra

[1]*SISTEC, RGPV University, Bhopal (M.P.), India*
[2]*SISTEC, RGPV University, Bhopal (M.P.), India*

Abstract— *Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious or abnormal activity. it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks With the ability to analyze network traffic and recognize incoming and ongoing network attack, majority of network administrator has turn to IDS to help them in detecting anomalies in network traffic In this paper, we focus on different types of attacks on IDS this paper gives a description of different attack on different protocol such as TCP ,UDP,ARP and ICMP. Intrusion detection system is a software which is used to monitor network for any intrusion .There are various types of IDS which are stated as Anomaly based, Host based, Network based and Signature based. In this paper, a review is made on various intrusion detection systems. The review analysis the whole active intrusion detection system. Through the extensive survey we analyzed the whole pose of the active intrusion detection system. We employed the survey towards overall IDS not only for the specific. Since the security threats are in increased level, hence the study and survey about IDS has paid a lot of attentions.*

I. INTRODUCTION

With the increased amount of network technology and throughput characteristic of network the security parameters such as IDS,IPS,firewall,UTM has acquired a lot of attention in study and review the state of the art. Here we are going to discuss about the various IDS proposed by various researchers and research forums. The typical architecture of WSN (Wireless sensor network) IDS and wired IDS has been demonstrated. [1]

Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. There are several reasons that make intrusion detection a necessary part of the entire defense system. First, many traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable when deployed Intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks.

The attack can be launched in term of fast attack or slow attack. Fast attack can be defined as an attack that uses a large amount of packet or connection within a few second [2]. Meanwhile, slow attack can be defined as an attack that takes a few minutes or a few hours to complete [2]. Both of the attack gives a great impact to the network environment due to the security breach decade. As in Fig:-1, Currently IDS is used as one of the defensive tools in strengthens the network security especially in detecting the first two phases of an attack either in form slow or fast attack An intrusion detection system can be divided into two approaches which are behavior based (anomaly) and knowledge based (misuse) [1], [3]. The behavior based approach is also known as anomaly based system while knowledge based approach is known as misuse based system [4], [5].The misuse or signature based IDS is a system which contains a number of attack description or signature that are matched against a stream of audit data looking for evidence of modeled attack [6]. The audit data can be gathered from network traffic or an application log. This method can be used to detect previous known attack and the profile of the attacker has to be manually revised when new attack types are discovered. Hence, unknown attacks in network intrusion pattern and characteristic might not be capture using this technique [7].Meanwhile, the anomaly based system identifies the intrusion by identifying traffic or application which is presumed to be normal activity on the network or host . The anomaly based system builds a model of the normal behavior of the system and then looks for anomalous activity such as activities that do not confirm to the established model. Anything that does not correspond to the system profile is flagged as intrusive. False alarms generated by both systems are major concern and it is identified as a key issues and the cause of delay to further implementation of reactive intrusion detection system [8].

II. INTRUSION DETECTION SYSTEM

Intrusion detection system came into picture around 1980 with the publication of John Anderson's Computer Security Threat Monitoring and Surveillance, which was one of the earliest papers in the field. "An Intrusion Detection Model",

published in 1987, provided a methodological framework that inspired many researchers and laid the groundwork for commercial products [9].

Intrusion Detection System (IDS) are the popular and useful tools for enhancing the security of the system and because of their value; they have now become a very important part of modern network security technology. Intrusion detection (ID) is a type of security management system for various computers as well as networks. An Intrusion Detection System collects all the information from the Host or the networks which include both anomaly and misuse intrusions. Intrusion detection functions include: 1.) Monitoring and analysing both user and system activities, 2.) Analysing system configurations and vulnerabilities, 3.) Assessing system and file integrity. IDS can be categorized in two ways: one is Host based Intrusion Detection System (HIDS) and another one is Network Intrusion Detection System (NIDS).

The two major approaches that are used by IDSs to detect intrusive behavior are called anomaly detection and misuse detection. The anomaly-detection approach is based on the premise that an attack on a computer system (or network) will be noticeably different from normal system (or network) activity, and an intruder (possibly masquerading as a legitimate user) will exhibit a pattern of behavior different from the normal user [10]. So, the IDS attempt to characterize each user's normal behavior, often by maintaining statistical profiles of each user's activities [11,12]. Each profile includes information about the user's computing behavior such as normal login time, duration of login session, CPU usage, disk usage, favorite editor, and so forth. The IDS can then use the profiles to monitor current user activity and compare it with past user activity. Whenever the different between a user's current activity and past activity falls outside some predefined \bounds" (threshold values for each item in the profile), the activity is considered to be anomalous, and hence suspicious. The interested reader is referred to [12] for a thorough discussion of both this topic and the implementation of the IDES anomaly detection component.

In the misuse-detection approach, the IDS watches for indications of \specific, precisely-
representable techniques of computer system abuse" [13]. The IDS includes a collection of intrusion signatures, which are encapsulations of the identifying characteristics of specific intrusion techniques. The IDS detects intrusions by searching for these \tell-tale" intrusion signatures in the records of user activities.

Although there exist only the above two major approaches to intrusion detection, IDSs are nevertheless quite diverse in their designs. Different IDSs employ different algorithms, different criteria for identifying intrusive behavior, and so forth. Also, several IDSs (including several of the example IDSs mentioned in Section 1) use a combination of both detection approaches.

III. TREE BASED CLASSIFICATION

Classification is used to determine the predetermined output. It predicts the target class for each data item. It assigns the data into target classes. For example it is used to identify the credit risk as low, high, medium.

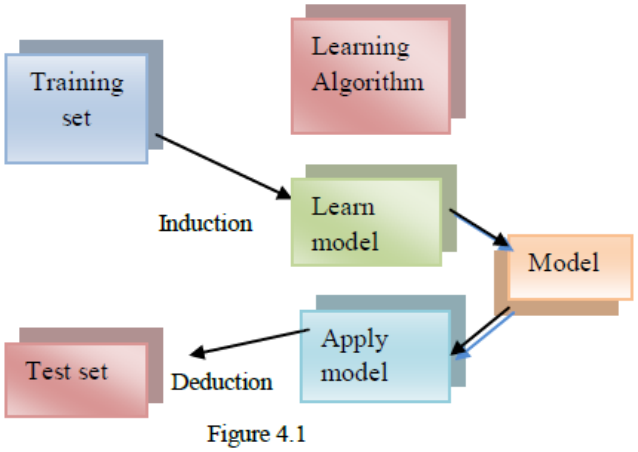

Figure 4.1

Examples of Classification Task

1. Predicting tumor cells as benign or malignant.
2. Classifying credit card transactions as legitimate or fraudulent.
3. Classifying secondary structures of protein as alpha helix, beta sheet, or random coil.
4. Categorizing news stories as finance, weather, entertainment and sports etc.

It is used in statistics, machine learning, and data mining. It is a predictive model which is used to observe the data item and concludes the target output value. Here leaves represent class labels and branches represent conjunctions. It does not describe data or decisions it simply makes the classifications. It generates rules and it is very easy for the humans to understand. It helps to search a record in a database. These rules provide a model transparency. There are two properties of rules. They are support and confidence. It helps us to rank the rules and predict the output.

IV. TREE BASED CLASSIFICATION FOR INTRUSION DETECTION

Decision Tree Techniques

In the decision tree, since there is no need for any type of domain knowledge or the parameter settings to be implemented for the decision tree classifiers, hence it is considered as the most efficient tool for the knowledge discovery process. [14] Within a decision tree, the topmost node is called the root node. This decision trees may manage the data that is having high dimension along with their demonstration of the obtained knowledge in the form of tree which is simple and also easy to resemble with the humans behaviors. The most simple and rapid phases of decision-tree methods are learning and the classification which is having the more accuracy.

Decision tree is one of the recursive approach and having the tree like architecture for representing the classification-rules. This is applied divide-and-conquer approach for dividing the data based on the attribute-values. And the classification of data move towards leaf node from the root node, in which every node has represented the attribute along with their value and every leaf-node is represented the class-label of the data. The Tree-based classifier may have the highest rate of performance within the huge data-set. And separate decision-tree approaches are also mentioned here:

J48 Algorithm

In order to generate pruned and the un-pruned type of C4.5 Decision-tree by applying the J48 algorithm. And the decision-tree that is made by using the J48 created the group of the training data through using the information entropy concept. This J48 may also be implemented for the purpose of classification. It utilized the concept of every attribute from data may be utilized to prepare the decision through dividing the data into some tiny sub-sets. This algorithm determines the normalized information which is obtained from the dividing the data. Then prepare the leaf node for informing to select that class. So the J48 generated a decision node which is at top in the tree by using some class expected value. It is based over the ID3 approach. Within the WEKA tool, the C4.5 decision-tree approach is also called as the J48 approach. This method creates a decision-tree by the use of information and the attribute that may have the high rate of information-gain which is selected in order to build the decision. Major demerit of this type of approach is it may needs more values of CPU time and the memory for execution purpose. The other types of tree based classifier are described here [15].

AD Tree

AD Tree is referred as the alternating-decision-tree which is applied for the classification purposed. The AD Tree may have the prediction node in the way it is having leaf-node and the root-node both.

ID3 algorithm

ID3 algorithm is one of the famous types of decision-tree algorithm that is introduced by the Quinlan. The ID3 algorithm is generally an attribute which is an algorithm used to create a decision-tree based on the training data-set. And the attribute that may have the highest rate of information-gain which is applied as the tree root.

NBTree

This NB-Tree Algorithm for decision-tree is the cross in between the two approaches one is Naïve-Bayes classifier and another one is the classification. The NB-Tree represents the optimal one that is represented as the decision-tree along with the nodes and the branches and leaf-nodes of Bayesian-classification. Since, along with the other types of tree based approaches of Classification, the NB-Tree is having the branches and the nodes. This is provided A which is the group of instances for algorithm developing node which is practiced for every type of division for the property. And if the highest value of the property is apparently better as compare to the practices instance hence this is dependent over the recent node, and this will be portioned into the property. And if it is not divided then here provides a significant approach which is providing better efficiency of the naïve-Bayesian-classifier in order to prepare the recent node.

Random Forest

The approach of Random Forest is given by [16] that is ensemble the classification approach that may includes the two or more type of decision-trees. Within the Random-Forest approach each tree is created through selecting the data randomly from the data-set. Through the use of Random-Forest approach it enhances the prediction power and the accuracy since it is less reactive to the data [17].

Table 2.1: Pros and Cons of Tree Based Classification in Intrusion Detection

ALGORITHM	PROS	CONS
Best First Tree	For few datasets prepare easy and simpler tree	For the sub-set of the decision tree, some new approaches have been introduced
C4.5 Tree	The data get classified by the help of missing values	Slower as compare to the other approaches
ID3	Used in various applications by testing and applying	Discrete and continuous variable are not handled by this
Navie Bayes	This approach target at particular attack also prepare decision tree dependent on the features of attack	Its results are based on previous probabilities assumed.
NB Tree (ISA)	This increases the detection rate by lowering the false positive rate through investigating the huge dataset	Not applied on real time data
NB Tree	This approach generate branches and nodes, and determine "utility" of the split attribute	Time complexity is high

V. DATA MINING

Data mining is the process of finding the unknown pattern from given set of patterns [18], [19]. In case of intrusion detection system, the use the concept of data mining the will find out the pattern which will track all users' activity to find out the intruders. In existing system are focusing on knowledge engineering processes in which the decisions are taken on the basis of some fixed rule. Basically the intrusion-detection-system is split in two broad categories such as intrusion-detection-system by the use of association-rule-mining and the intrusion-detection-system by the use of event-correlation data-mining.

The approach of data-mining is referred as the process of the non-trivial derivation of the automatic, existing unknown and extremely necessary information among the data. This is the most comfortable method of deriving of patterns that may show the mining process which automatically record within the huge data-sets and focuses on issues relating to their feasibility, usefulness, effectiveness and scalability. It can be viewed as an essential step in the process of knowledge data discovery. There is huge traffic of network and information is obtained from the various sources such that the data-set for the intrusion-detection-system has becomes so large. Therefore, this is extremely complicated for observing the data within the situation of the huge data-set. Recently, data-mining approaches [20], perform a significant function within the recognition of normal and the abnormal patterns, as it may extract the hidden details also it works with the huge data-set. And this part of the paper explains various data-mining approaches like the classification and the clustering approaches in order to achieve the information regarding the susceptibility through checking out the data of network. The process of data-mining may investigate the analyzed sets in order to generate the unknown-relation then merge it with the results of the analysis of data in order to make data to be understandable by its owner. Therefore the issues of data-mining are treated as the data analysis issue. And the data-mining architecture implicitly find out the patterns within the data-set then apply these types of patterns in order to detect the set of the malignant binaries. that is the Data-mining approach may find out the patterns within the huge volume of data, like the byte-code and then apply these types of patterns in order to find out the future instances within the same type of data. Within the intrusion-detection-system, the information comes from various sources like host data, network log data, alarm messages etc.

VI. LITERATURE REVIEW

Web servers are ubiquitous, remotely accessible, and often misconfigured. In addition, custom web-based applications may introduce vulnerabilities that are overlooked even by the most security-conscious server administrators. Consequently, web servers are a popular target for hackers. To mitigate the security exposure associated with web servers, intrusion detection systems are deployed to analyze and screen incoming requests. The goal is to perform early detection of malicious activity and possibly prevent more serious damage to the protected site. Even though intrusion detection is critical for the security of web servers, the intrusion detection systems available today only perform very simple analyses and are often vulnerable to simple evasion techniques. In addition, most systems do not provide sophisticated attack languages that allow a system administrator to specify custom, complex attack scenarios to be detected. This paper presents WebSTAT, an intrusion detection system that analyzes web requests looking for evidence of malicious behavior. The system is novel in several ways. First of all, it provides a sophisticated language to describe multistep attacks in terms of states and transitions. In addition, the modular nature of the system supports the integrated analysis of network traffic sent to the server host, operating system-level audit data produced by the server host, and the

access logs produced by the web server. By correlating different streams of events, it is possible to achieve more effective detection of web-based attacks.

[21] Shailendra Sahu and B M Mehtre, "Network Intrusion Detection System Using J48 Decision Tree", suggested the use of data-set called as Kyoto 2006+ which is prepared on the basis of real traffic data of over three years. In this suggested paper the approach of J48 decision tree have been used for the network intrusion detection purpose and also obtained the accuracy at nearly 97.23 percent. This approach is implemented by the use of WEKA 3.6.10 tool, here also prepared the decision-tree in order to find out the intrusion with n the given data-set that have received higher rate of true positive approx. 99 percent for the normal and the attack packets. By the analysis of the generated result, the tree may have correctly classified nearly 130931 instances among the 134665 instances that are 97.23percent approx. And the results of simulation have presented that this model is now capable to find out the unknown attacks also.

[22] Miss Meghana Solanki and Mrs. Vidya Dhamdhere, "Intrusion Detection System by using K-Means clustering, C 4.5, FNN, SVM classifier", describes various recent intrusion detection methods generate high false positives and negatives Network Anomaly detection systems are designed based on availability of data instances. Many intrusion detection techniques have been specifically developed for certain application domains, while others are more generic. In this paper present a cascaded algorithm using K– Means and C4.5. In this paper performance analysis is measured by using five measures, Precision, detection accuracy or True Positive Rate, Total Accuracy, False Positive Rate, and F–Measures. The proposed algorithm gives impressive detection accuracy in the experiment results.

[23] Mr. Vilas S. Gaikwad and Dr. Prakash J. Kulkarni, "One Versus All classification in Network Intrusion detection using Decision Tree", have represents a learning algorithm for the anomaly-based NIDS by the use of decision-tree, based on one versus all criteria which adjusts the weights of dataset based on probabilities and split the dataset into sub-dataset until all the sub-dataset belongs to the same class. In this paper developed the performance of intrusion-detection-system by the use of decision tree. In conventional decision tree algorithm weights of every example is set to equal value which contradicts general intuition, but in our approach weights of every example change based on probability. The experimental results on KDD99 benchmark data-set suggested an algorithm that is obtained through the high rate of detection over various kinds of attacks on network. The future part of this work will focus on parallelism of one versus all problems.

[24] A. Mitrokotsa and C. Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", have determined how to use the classification approaches properly within the intrusion-detection for the MANETs. For obtaining this here determined five types of supervised classification approaches for the intrusion-detection over a various metrics. Here also evaluate the performance over the data-set that is mentioned within this paper that may contain different types of traffic situations and the mobility signatures for various types of attacks. The major objective is to analyze how the performance of classification is based over the problem-cost-matrix. And relatively, here also determine the use of the uniform cost matrices versus the weighted-cost-matrices influenced the performance of classifier. And another objective is to determine the approaches for making the classifiers if the unknown-attack of sub-types has anticipated while testing. And if the classifiers have got tuned by the use of cross-validation approach, then the data among the similar kinds of attacks have been provided within the all folds. This approach is different from the real-world application in which the unknown attacks are also presented.

[25] Tetsuji Nakagawa and Kentaro Inuiand Sadao Kurohashi, "Dependency Tree-based Sentiment Classification using CRFs with Hidden Variables", have been represented the dependency tree-based approach for the sentiment type of classification by the use of random fields that are conditional along with the variables that are hidden. Within this approach, contradiction of every type of dependency sub-tree of the subjective-sentence is described through the hidden-variable. And the values of hidden-variables get estimated within the regards of the interactions in between the variables whose nodes have head-modifier relation in the dependency tree. The value of the hidden variable of the root node is identified with the polarity of the whole sentence. Experimental results showed that the proposed method performs better for Japanese and English data than the baseline methods which represents subjective sentences as bag-of-features.

[26] Mohammed E. El-Telbany and Mahmoud Warda, "An Empirical Comparison of Tree-Based Learning Algorithms: An Egyptian Rice Diseases Classification Case Study", have suggested the data-mining approach within the agriculture that is a very interesting research topic and can be used in many applications such as yields prediction, disease detection, optimizing the pesticide usage and so on. There are many algorithms that have been presented for classification in diagnosing the Egyptian rice diseases data set. However, in this selected four algorithms the J48 decision tree, Bayes net, random trees and random forest that belongs to the Tree-based category which are easy to interpret and understand. Here conduct many experiments to evaluate the four classifiers for Egyptian rice diseases. The above analysis shows that for the J48 decision tree achieves highest sensitivity, specificity and accuracy and lowest RMS error, than Bayes net, random trees and random forest. J4.8 gave the best results due to the pruning process which simplify the tree and remove un-relevant branches. Moreover, the random forest superior over random trees due to boosting process.

[27] Purushottam R. Patil, Yogesh Sharma, and Manali Kshirasagar, "Performance Analysis of Intrusion Detection Systems Implemented using Hybrid Machine Learning Techniques", may describes various research articles on the Intrusion-detection-Systems have been implemented by the use of clustering and classification hybrid techniques are analyzed. The Dataset used by all researchers is DARPA KDD‟99. The detection rate of attack classes like Normal, U2R, Probe, R2L, ranges from 66 percent to 100 percent and the False-Alarm rate is minimized up to 0.102. Number of attributes selection for processing also effect conduct of the system, lower the numbers of attributes better the conduct. In future hybrid of such machine learning approaches will achieve 100 percent detection rate, False alarm rate to 0 percent hence more adaptive and efficient systems can be designed.

[28] P. Amudha, S. Karthik, and S. Sivakumari, "Classification Techniques for Intrusion Detection – An Overview", have suggested the data-mining approaches have been suggested that are attracted by the researchers in the intrusion detection domain recently and they aim to reduce the great burden of analyzing huge volumes of audit data. There is an imbalance among the classes in the KDD Cup'99 data set that has been recognized as an issue in intrusion detection that may cause poor detection of minor classes and is a major issue to the data-mining approach. Obtaining the high detection-rate and reducing false alarm rates are the significant challenges in designing an intrusion detection system.

Using different classification techniques, it could be possible to improve the detection rate and reduce false alarm rate and need to be studied. In this paper, various classification techniques used by the researchers in evaluating the performance of intrusion detection model are reviewed. From the empirical study performed, this work identified that different researchers propose different algorithms for the intrusion detection domain in different categories, but still, it has to be explored.

[29] Kajal Rai, M. Syamala Devi, and Ajay Guleria, "Decision Tree Based Algorithm for Intrusion Detection", have suggested an Intrusion-Detection-System which is one of the defense approach which governs the activities of network and informs about the malignant activities immediately with system-administrator. The intruders have performed various efforts in order to obtain the access over the network also they have attempts to damage the data of organization. Hence security is one of the major aspects for the organization. Because of these causes the intrusion-detection approach has now been one of the major issues for research. An intrusion-detection-system may be widely categorized as the Signature-based intrusion-detection-system and the Anomaly-based-intrusion-detection-system. In this suggested work, the decision-tree approach have been introduced which is dependent on the C4.5 decision-tree algorithm. And the feature-selection may divide the value that is significant problem for creating the decision-tree. In this the experimentation is made over the NSL-KDD data-set which is dependent on various properties. And the time utilized through the classifier in order to create the design and the obtained accuracy has got analyzed.

[30] Patel Hemant, Bharat Sarkhedi and Hiren Vaghamshi, "Intrusion Detection in Data Mining With Classification Algorithm", now proposed the analysis over various algorithm such as the Decision-Tree, Naïve-Bayes, and NB-Tree for the intrusion-detection. In this also observed the merits and demerits for these approaches. The Naïve-Bayes approach refers to create a decision-tree which is dependent on the particular feature of the attacks whereas on the contrary the performance of Bayesian approach is based on the previous probabilities. In the NB-Tree (ISA) approach observed the huge amount of data of network that are considered as the complicated features of the attack pattern in which on the contrary this is not applied within the real time network also within the NB-Tree it provides branches and the nodes.

[31] Tanmayee S. Sawant, and Prof. Dr. S.A. Itkar, "Intrusion Detection System using Adaboost based approach and Fuzzy genetic algorithm", have been suggested the network-intrusion-detection-systems is having the completely developed infrastructures regarding to the security. Inadequately the recent architectures of network are not able to detect the unknown-attacks properly. In this paper also explained the data-mining process which is the method of extracting the information from large volume of noisy, incomplete, fuzzy data. Being the basic reason of this issue is to transmit the classification approaches implementation of the data-mining methodology that may be used in the network in order to find out several attacks. Within this paper also introduced one of the intrusion-detection-system for extending the rate of detection of the R2L and the U2R attacks also analyzed the available systems of different domains like intrusion-detection-systems or commercial systems. Some of the standard data-sets and some information extraction approaches have become significant more as it was expected. And the basic data-mining approach have also been analyzed here which was applied. So this paper is concluded with the issues analysis made in this paper along with the further research on their solution.

VII. CONCLUSION

Network based Intrusion detection system can detect small attacks or stepping stone of big attack. Signature based IDS play important role in NBIDS but With Time New Malicious data with New Pattern may exist, Update of the signature pattern is very important and difficult otherwise it cannot able to detect new attacks. Different algorithms are used for ID but fast and take less space in matching is good algorithm. SNORT and SAX2 are mainly signature based IDS. AX2 is faster, GUI, and packet dropping is lass. [12]

References

[1] Cuppen, F. & Miege, A. (2002). Alert Correlation in a Cooperative Intrusion Detection Framewok. In Proceeding of the 2002 IEEE Symposium on Security and Privacy. IEEE, 2002]
[2] Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.
[3] Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.
[4] Yeophantong, T, Pakdeepinit, P., Moemeng, P & Daengdej, J. (2005).Network Traffic Classification Using Dynamic State Classifier. In Proceeding of IEEE Conference
[5] Farah J., Mantaceur Z. & Mohamed BA. (2007). A Framework for an Adaptive Intrusion Detection System using Bayesion Network. Proceeding of the Intelligence and Security Informatics, IEEE, 2007.
[6] Vaishali Kosamkar, and Sangita S Chaudhari, "Improved Intrusion Detection System using C4.5 Decision Tree and Support Vector Machine", International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1463-1467.
[7] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S. (2002). Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference.
[8] Karl Levitt. (2002). Intrusion Detection: Current Capabilities and Future Direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE, 2002.
[9] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012, "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols".
[10] D. E. Denning, An Intrusion-Detection Model," IEEE Transactions onSoftware Engineering, vol. SE-13, no. 2, pp. 222-232, February 1987.
[11] T. F. Lunt et al., \A Real-Time Intrusion Detection Expert System (IDES)," Interim Progress Report, Project 6784, SRI International, May 1990.
[12] H. S. Javitz and A. Valdes, The SRI IDES Statistical Anomaly Detector," Proc.,IEEE Symposium on Research in Security and Privacy, Oakland, CA, pp. 316-376,May 1991.
[13] S. Kumar and E. H. Spa_ord, A Software Architecture to Support Misuse IntrusionDetection," Technical Report CSD-TR-95-009, Purdue University, March 17, 1995.
[14] Deepthy K Denatious and Anita John. "Survey on data mining techniques to enhance intrusion detection". In Computer Communication and Informatics (ICCCI), 2012 International Conference on Digital Object Identifier, p. 1–5.IEEE, 2012.
[15] A.M. Chandrasekhar, "Intrusion Detection Technique By Using K-Means, Fuzzy Neural And Svm Classifier", International Conference on Computer Communication and Informatics, Jan 04-06, 2013 Coimbatore, India.
[16] Sandeep Kuma, and Prof. Satbir Jain, "Intrusion Detection and Classification Using Improved ID3 Algorithm of Data Mining", International Journal of Advanced Research in Computer Engineering &Technology Volume 1, Issue 5, July 2012.
[17] Ammar Boulaiche, "A Quantitative Approach For Intrusions Detection And Prevention Based On Statistical N-Gram Models ", Proceeding a Computer Science 10 (2012) 450 – 457.
[18] M. Zaki and W. Meira, Data mining and analysis: foundations and algorithms, Cambridge University Press, 2014.
[19] A. Alazab, M. Hobbs, J.Abawajy, and M. Alazab, "Using Feature Selection for Intrusion Detection System", International Symposium on Communications and Information Technologies, 2012.
[20] Deepthy K Denatious and Anita John. "Survey on data mining techniques to enhance intrusion detection". In Computer Communication and Informatics (ICCCI), 2012 International Conference on Digital Object Identifier, p. 1–5.IEEE, 2012.
[21] Shailendra Sahu, B M Mehtre, "Network Intrusion Detection System Using J48 Decision Tree", 978-1-4799-8792-4/15/ 2015 IEEE
[22]Miss Meghana Solanki, and Mrs. Vidya Dhamdhere, "Intrusion Detection System by using K-Means clustering, C 4.5, FNN, SVM classifier", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 6, November-December 2014.
[23] Mr. Vilas S. Gaikwad, and Dr. Prakash J. Kulkarni, "One Versus All classification in Network Intrusion detection using Decision Tree", International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 1 ISSN 2250-3153.
[24] A. Mitrokotsa, and C. Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", Ad Hoc Netw. (2012),
[25] Tetsuji Nakagawa, and Kentaro Inuiand SadaoKurohashi, "Dependency Tree-based Sentiment Classification using CRFs with Hidden Variables", Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the ACL, pages 786–794,.

[26] Mohammed E. El-Telbany, and Mahmoud Warda, "An Empirical Comparison of Tree-Based Learning Algorithms: An Egyptian Rice Diseases Classification Case Study", International Journal of Advanced Research in Artificial Intelligence, Vol. 5, No.1, 2016.
[27] Purushottam R. Patil, Yogesh Sharma, and Manali Kshirasagar, "Performance Analysis of Intrusion Detection Systems Implemented using Hybrid Machine Learning Techniques", International Journal of Computer Applications (0975 – 8887) Volume 133 – No.8, January 2016.
[28] P. Amudha, S. Karthik, and S. Sivakumari, "Classification Techniques for Intrusion Detection – An Overview", International Journal of Computer Applications (0975 – 8887) Volume 76– No.16, August 2013.
[29] Kajal Rai, M. Syamala Devi, and Ajay Guleria, "Decision Tree Based Algorithm for Intrusion Detection", Int. J. Advanced Networking and Applications Volume: 07 Issue: 04 Pages: 2828-2834 (2016) ISSN: 0975-0290.
[30] Patel Hemant, Bharat Sarkhedi, and Hiren Vaghamshi, "Intrusion Detection in Data Mining With Classification Algorithm", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, July 2013.
[31] Tanmayee S. Sawant, and Prof. Dr. S.A. Itkar, "Intrusion Detection System using Adaboost based approach and Fuzzy genetic algorithm", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 2, February 2016.

