International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

Review on Anomaly Based Intrusion Detection System

Vadday Saikiran[1], Indira Reddy[2]
[1]Student, Mtech, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India
[2]Assistant Professor, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India

ABSTRACT

The internet and computer networks are getting new kind of security issues and attacks from intruders. For this the Intrusion detection is an important research area. There are various mechanisms are available for detecting the network intrusion, but that is not enough to identify attacks efficiently. The Intrusion Detection system (IDS) is two types, namely Network based IDS and Host IDS (HIDS). IDS mechanism is very helpful to find the network attacks and anomalies. This paper presents the study of different techniques for intrusion detection system. It is included that how the anomaly based intrusion detection system has been improved with different types of approaches, methods and algorithms to prevent from different kind of intrusion attacks. The efficiency results for false positive rates are also given for customizing the intrusion attacks.

Keywords: Intrusion Detection System, Host Based Detection, Network Based Detection, Signature Based Detection And Anomaly Based Detection, Techniques

I. INTRODUCTION

As internet is growing rapidly security is the vital aspect in the computer networks. IDS are very helpful and act as a safeguard for data integrity, confidentiality and system availability for different kinds of attacks [1]. Firewalls and IDS are primary elements of the security framework. An IDS is one of the framework security foundations that attempts to identify harmful activities, for example, Denial of Service (DOS) attacks and port scans by observing and investigating activities occurring on systems and networks. IDS includes two types Host-based (HIDS) and Network-based (NIDS) approaches [4]. HIDS is the primary sort of IDS, its fundamental capacity is internal observing (inside a computer or machine), yet numerous variations of HIDS have created which can be utilized to monitor network [6]. HIDS decide whether a system has been compromised and caution administrators correspondingly. A NIDS is utilized to control and investigate network traffic activity to protect a framework from network based threats. In any case, there are numerous issues in the conventional IDS, for example, the low identification ability against the unknown network attack, high false alarm rate, and deficient investigation capacity and etc. For the most part, Intrusion discovery techniques are ordered into two strategies, namely Misuse Detection or Signature based recognition and Anomaly Detection. The Misuse identification calculations identify attacks in light of the known attack signatures. They are helpful in identifying known attacks with fewer errors. In any case, misuse detection is can't identify new unclear attacks. To conquer this issue, Anomaly interruption detection can anticipate another attack by identifying any deviation from the client's ordinary profile. A conventional technique of clustering is an unsupervised method, useful for identifying the unknown attacks. Using clustering technique database is divided into dissimilar sets based on it similarities. The particular methods detect the normal and attacked instances in groups [14]. The classification is the supervised data mining technique,

which constructs the classified model, depends on data [15]. This model helps to classify the new data into one predefined classes depends on the attribute values. The class's information can be categorized into different types of classification approaches using some classifier such as Artificial Neural Networks, Decision Trees, evolutionary algorithms, Rule Induction, Bayesian methods, K-Nearest Neighbors, etc.

A. Intrusion Detection System

It is a security service that controls and examines the system activities and challenges to access and identify the system resources as well as unauthorized activities. A IDSs are typically used with the other defensive security techniques namely authentication and access control. Several research works already addressed that IDS is a significant part of whole defense system. First, various conventional systems and applications were developed without security.

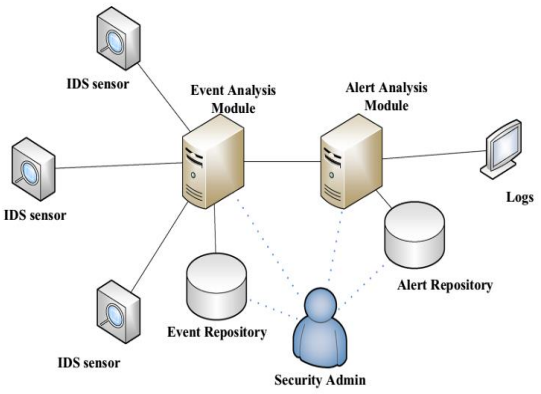

Figure 1. architectural diagram of IDS.

The An IDS is a combination of hardware and software, which identify the external and internal user's unauthorized activities from the system. The NIST definition of IDS is theProcess of controlling the activities that are placed in the network or system. These log files helps to recognize the intrusions [20]. On the other hand, in various environments to handle different kinds of works a lot of applications and systems are developed and to improve the system security various protective mechanisms are used. Additionally, the defensive security strategies protect the information systems effectively, but still required in intrusion related information [21]. There are two types of IDS namely,

1. Host Based IDS
2. Network Based IDS

1) Host Based Intrusion Detection system

The objective of the HIDS is the controlling state and dynamic behavior of the computer system. This detection system checks all the activities of inspected packets on a network. HIDS recognize what resources are being utilized and which program gets to those resources. If in the network any alternations or adjustment happens, system administer receive some network alerts. HIDS is progressively becoming essential to ensure the host computer frameworks and its network activities. HIDS with host based information is incorporated into the computer frameworks to identify the intruder abnormal activities, noxious Behavior, application abnormalities and preserve the Information Systems from intruders and report the occasions to the HIDS System Administrator.

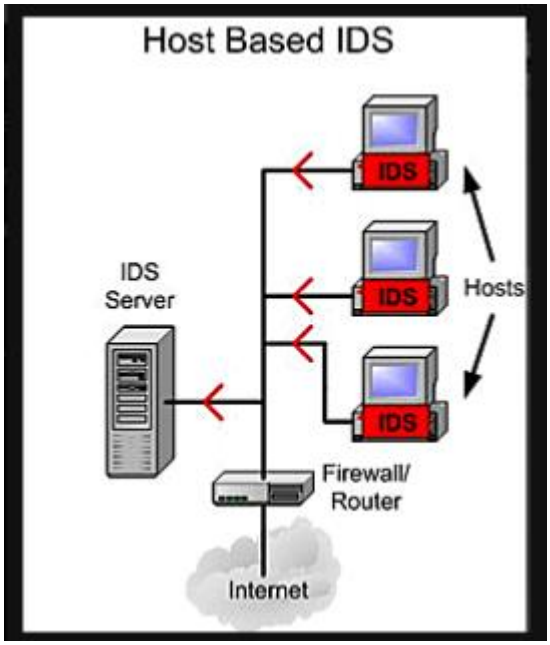

Figure 2. indicates to the HIDS.

A HIDS controls the software and investigate the activities occurring in the systems. After that, HIDS

detect the abnormal activities in the computer systems. In a computer system, security is the significant element. A HIDS provide the Security to the computer system. A lot of security violations in systems happen because of malicious code and unauthorized events are penetrated to the system barriers. The abnormal activities and misuse code affect the system. The HIDS approach avoids the unwanted access in a host system and Provide higher security for the user's information.

2) Network Based Intrusion detection system

NIDS is the attribute function of target system and function modules are observed in network. The investigation of NIDS based on either manually or automatically. The NIDS is significantly used in the security infrastructure of the system. In NIDS to control the incoming and outgoing threads, anti-thread software is installed on the servers.

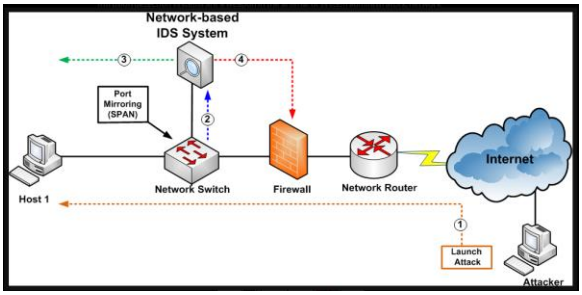

Figure 3. Architecture of Network based IDS

Network intrusion detection systems (NIDS)[5] are most capable way of defending against network-based attacks .Mainly, there are two main types of intrusion detection systems: signature-based (SBS) and anomaly-based (ABS). Signature-based systems rely on pattern identification techniques and they will maintain the record of signatures of earlier known attacks and compare them with analyzed data. An alarm will rise when the signatures are matched. Anomaly-based systems build a statistical model describing the normal network traffic, and any abnormal behavior that deviates from the model is recognized. In this paper mainly focusing on anomaly-based systems.The categories of intrusion detection system are

1. SIGNATURE BASED DETECTION:

Signature based detection [1] involves penetrating network traffic for a series of malevolent bytes or packet sequences. The main advantage of this technique is that signatures are very easy to extend and understand if we know what network behavior we are trying to identify. The proceedings generated by signature based IDS can communicate the cause of the alert. The pattern matching can be done more powerfully on modern systems so the amount of power needed to perform this matching is minimal for a rule set.

Limitations of these signature engines are that they only detect attacks whose signatures are previously stored in database; a signature must be created for every attack; and novel attacks cannot be detected. This technique can be easily deceived because they are only based on regular expressions and string matching. Signature based detection does not work well with techniques like nop generators, payload encoder. The efficiency of the signature based systems is very much decreased, as it has to create a new signature for every variation. As the signatures keep on growing, the system engine performance decreases. The difference of speed of creation of the new signatures between the developers and attackers decides the efficiency of the system.

2. ANOMALY BASED DETECTION:

The anomaly based detection is based on defining the network actions. The network behavior is in agreement with the predefined behavior, then it is accepted or else it triggers the event in the anomaly detection. The established network behavior is organized or learned by the specifications of the network administrators.

The major drawback of anomaly detection is defining its rule set. Defining this process is also affected by

various protocols used by different vendors. Rule Apart from these, custom protocols also make rule defining a difficult job. For detection to occur properly, the detailed knowledge about the established network behavior need to be developed by the administrators. After once the rules are defined and protocol is built then an anomaly detection system works.

The major benefit of anomaly based detection over signature-based engines is that a novel attack for which a signature does not exist will be detected if it falls out of the normal traffic patterns. This is observed when the systems are detecting new automated worms. In this when the new systems are containing worms, then it will starts scanning for other vulnerable systems with accelerated rate and filling the network with malicious traffic, thus giving the event of a TCP connection or bandwidth irregularity rule.

The organization of this document is as follows. In Section 2 (Related Work), this gives the brief information about the various techniques used for anomaly based detection. In Section 3 (Conclusion), the conclusion of the reviewed work is explained here and Section 4 shows the References that are referred for this work.

II. RELATED WORK

1. Meng-Kai Tsai proposed a Finite Automata Based Foresight Network intrusion Detection System (FA-FNIDS) to prevent malevolent attacks in advance and further finding novel attacks. Presented three experiments. In this first experimental result showed the advantage of finite automata in efficiency. Then second and third experimental results showed comparison of efficiency between FA-FNIDS and snort. Although the efficiency of FA-FNIDS is slower than snort slightly, got the detection ability of FA - FNIDS is much better. [1]

2. Toru konno given that how to increase the accuracy of anomaly based intrusion detection by Threshold optimization using Taguchi method. Focuses on quality characteristics and noise factors, used the standardized S/N of digital data approach to get optimal conditions. After the results shown that the false detection rate can be more decreased by giving more positive training data. Using this techniques got 0.186% or the less positive rate in real data.[2]

3. Damiano Bolzoni, Sandro Etalle,in this paper present a new approach to Network Intrusion Detection that involves the combination of two different techniques: a self-organizing map and the PAYL architecture and modified the original PAYL to take advantage of the unsupervised classification given by the SOM, which then functions a pre-processing stage. The benchmarked [4] POSEIDON extensively against the PAYL algorithm and data sets showed a higher detection rate and lower false positives rate. The experiments on the DARPA set showed that this approach reduces the number of profiles used by PAYL and results given that PAYL without SOM requires 3 times as many profiles as with the SOM pre-processing.[3]

4. Damiano Bolzoni presents a comparison between different anomaly-based network intrusion detection systems, focusing in particular on the data analyzed by the detection engine to discover possible malicious activities.Presented two payload-based anomaly-based NIDSs:PAYL and POSEIDON[3].Given Payload-based vs header-based approaches ,argued that header-based systems are more suitable to detect attacks directed at vulnerabilities of the network and transport layers.[4]

5. Paulo M. Mafra presents the development of an anomaly based intelligent intrusion detection model named Octopus-IIDS that makes use of artificial neural network and support vector machines to

recognize malicious activity through the analysis of network traffic, dropping the false positive rate and improving the detection rate..Given two artificial intelligence techniques Kohonen neural network (KNN) and support vector machine (SVM) are applied to detect anomalies. These techniques are used in sequence to improve the system accuracy, identifying known attacks and new attacks, in real time. [5]

6. Veselina G. Jecheva, given a new approach to anomaly based detection using the Hidden Markov Models and the BCJR decoding algorithm for decoding problem in intrusion recognition. In this describe the system model and applied the ML criterion to maximize the probability of a given sequence of observations .Given simulation experiments to compare the values of LLR's corresponding to the same observations with different values of T. [6]

7. Benoit Morel, In this paper given that Anomaly based intrusion detection suffering from the uncontrollability of the rate of false alarms (false positive).Describes the majority rule gates for simulation and in which there will be a lot of correlation in the probability of false positive and false negative of the different detectors. In this also given the Performance of the detection system in the presence of correlations to analyze the "real data" by exposing the different detectors to different samples of the data stream to check the effect and to reduce the frequency of false positive. Results got that for early malware detection,it constitutes less than 10-4 of the total traffic, an IDS with a false positive of 1%,will report a false alert 99% of the time. [7]

8. Sho Ohtahara presents an anomaly based detection system which shares normal behavior data between multiple machines and the normal behavior data obtained on each machine is accumulated in a server and the integrated data is distributed to each machine for improving the detection accuracy .Given a ADCOIN that collects normal behavior data from different machines and creates a high-accuracy normal behavior model. Uses Integration Algorithm for getting the false positive rates and Evaluated three algorithms for integrating multiple databases. In the future, would like to demonstrate the usefulness of the proposed system. [8]

9. Luis Miguel Torres, In this paper introduced functional intrusion detection system that combines them in order to offer resilient detection of the most common attacks in 802.11.Describes wireless intrusion detection systems and the state of the art in anomaly detection techniques for wireless intrusion.Discussed the 802.11 standards and addressed some security issues with privacy systems like WPA2 networks and given the need by introducing a wireless intrusion detection system called S2WIDS.[9]

10. Hadeel Amjed Saeed, in this paper developed an anomaly based intrusion detection system which can rapidly detect and classify different attacks. Given ANNs and KDD9's for implementing IDS .The proposed system for anomaly-based intrusion detection is composed of four main stages are monitoring, detection, classification, and alerting. Then Detection Rate (DR) and False Positive rate (FP) are calculated for different scenarios. Then got obtained results of training with 41 features are better than those with training with 22 features. Finally, given that the results of testing with normalization are better than the results of testing without normalizing.[10]

11. Hae-Duck J. Jeong given an anomaly teletraffic intrusion detection systems based on the open-source software platform hadoop for early detection of anomaly teletraffic on Hadoop platforms. Describes the Hadoop Distributed File System, Map Reduce, anomaly teletraffic intrusion detection system [2]. Given AT-IDS to detect anomaly teletraffic using the Map Reduce framework. Discussed the problems and technical solutions for AT-IDS.[11]

12.Deepak Kumar Singh, In this paper, given the designed and implementing real time Intrusion detection system with the help of integration of Snort

(Signature based system and Anomaly based system) for detecting anomalies. Describes the Snort for detecting variety of attacks and improves the efficiency of IDS by using Bayesian classification method to get better detection rate and less false positives in detecting the intrusions. By using this techniques got the detection accuracy of ≈84 % is achieved using the Bayesian method with the false positive rate of 4.6.and Hotellings statistical method given a hit rate of 81% at 6.2% false positive rate. [12]

13. Nilanjan Sen, in this paper proposed an efficient BPNN architecture for the developing the anomaly based IDS with high accuracy and detection rate and uses KDD'99 [2] dataset to train the architecture. Describes the Intrusion Detection System (IDS)[1], Back Propagation Neural Network (BPNN) [2]and KDD '99 Data set for the proposed work. He compared the performance of the proposed model with other models' and achieved the results superior to the available results. [13]

14. Alka Chaudhary, In this paper developed an anomaly based fuzzy intrusion detection system to detect the packet dropping attack from mobile ad hoc networks(MANETs).The author discussed the MANETs security issues and defined the scenarios and simulation parameters by Qualnet simulator. In given simulation results the author proved that proposed system is more capable to detect the packet dropping attack with high positive rate and low false positive under each level (low, medium and high) of speed of mobile nodes. In future, the author wants to develop a new intrusion detection system which can classify the suspicious and normal activities in the MANETs. [14]

15. Dipika Narsingyani, In this paper mainly focuses on Genetic algorithm (GA) based anomaly detection technique for optimization specifically focusing on false positive rate .Given a study on various kind of machine learning techniques have been used for detecting different types of intrusion that are exist in KDDcup99 dataset. Discussed Selection, Evaluation, Cross-over, Mutation steps in GENETIC ALGORITHM[2] and GA BASED[3] IDS modules.The results given False Positive alarm rate can be reduced and Data rate can be increased using appropriate feature selection with KDD 99 data set.[15]

16. Evgeniya Nikolova, in this paper presents a fuzzy clustering approach to anomaly host based intrusion detection and discussed the fuzzy clustering by local approximation of memberships (flame) and used Fuzzy clustering techniques for Intrusion Detection System to divide the current activity patterns into two clusters one for the normal and one for anomalous data. Given CLUSTERING VALIDATE to achieve better classification as well as the cluster compactness and done PERFORMANCE ANALYSIS for clustering quality evaluations. The result from a fuzzy clustering into the intrusion detection process was proved that efficient for enhancing the system's results. [16]

17. Naila Belhadj Aissa proposes a clustering-based detection technique using a genetic algorithm named Genetic Clustering for Anomaly-based Detection (GC-AD) and presents a two-stage fitness function. The accuracy of the technique is tested on different subset from KDD99 dataset. Evaluated the performance of the scheme using different subsets of KDD99. The simulation results given high detection rates between 75% and 98%, and low false positive rates between 1.3% and 0.12%.The results proved that CG-AD is more efficient compared to kmeans. Also wants to analyze and reduce the rejected instances for future improvements to this work. [17]

18. M.Anandapriya ,In this paper mainly focuses on Anomaly based HIDS and reducing the problem of false alarm rate, using semantic based system call patterns. Proposed semantic approach is applied on the system call patterns for detecting the intrusion on the host system using ADFA-LD dataset and Extreme Learning Machine is used as Decision Engine (DE) for performing classification. [18]

19. Abdelaziz Amara korba, in this paper proposes a new protection mechanism to secure routing in ad hoc networks. Describes the wormhole & rushing attacks[1] and proposed protection mechanism consider a mobile ad hoc network routed by AODV protocol, Anomaly-based detection[1].The Attack detection and prevention for attacks in adhoc network. Based on nodes route selection rate, malicious nodes are detected as traffic concentration points due to their high capacity of competition in route discovery process. As a result the proposed mechanism exhibits high detection rate without affecting network performances.[19]

20. Veselina Jecheva, in this paper presents the adaptive approach of data mining techniques and string metrics in anomaly based intrusion detection systems. Given the methodology for creating anomaly detection approach, based on the concept of minimization of the distance between the received sequence and the normal activity patterns and done Simulations and Comparisons of the Obtained Results. In this discussed the whole approach [5] and conclude the proposed approach was result as a system working as an alert device in the event of attacks directed towards the protected system.[20]

21. Radoglou-Grammatikis presents an intrusion detection system (IDS) for detecting the anomaly behaviors in Android mobile devices. Discussed the related intrusion detection technologies for mobile devices. Describes the architecture and the design of the proposed IDS. The experimental results gives the accuracy and the detection rate of the proposed system reaches 85, 02% and 81,39% respectively. In the future, improving the accuracy and the detection rate of the IDS, by taking into account more critical traffic features such as user's touch patterns and behaviors.[21]

22. Pratik Satam presents the two architectures to develop an anomaly based intrusion detection system for single access point and distributed Wi-Fi networks. The proposed approach monitors illegal exploitations of existing vulnerabilities in the IEEE 802.11 protocol. Describes the IEEE 802.11 Behavior Analysis module and Tracking module architecture for APn.Given enhancing the performance and scalability of the Wi-Fi IDS algorithms. The current Wi-Fi location accuracy is at 81 % and our goal is to improve it up to upper 90%. [22]

23. Chau Tran proposes a heterogeneous anomaly–based intrusion detection system (HA-IDS) built on the integration of two platforms (FPGA and GPU) to utilize their strength .Introduces Compute Unified Device Architecture (CUDA) and FPGA based Future construction to handle large-scale data while CM is deployed on GPU using Back-propagation Neuron Network to utilize the parallel computing for improving the system performance. Employed the proposed system on GPU –GIGABYTE GeForce GTX 1080 and FPGA – Xilinx Virtex-5 XC5VTX240T chip. The training outcome on GPU is faster than that on CPU by up to 12*x* and testing system throughput in real-time is 200Mbps with more than 80% in Accuracy Rate.[23]

24. Imtiaz Ullah introduces a filter-based feature selection model for anomaly-based intrusion detection systems and used ISCX and NSL-KDD datasets to evaluate the proposed model. The proposed model gives the features based on information gain by considering consistency, dependency, information, and distance of each feature. After the analysis the author getting the accuracy of the proposed model was measured as 99.70 % and 99.90% for the ISCX and NSL-KDD datasets.[24]

25. Fakhroddin Noorbehbahani proposes a novel network anomaly detection framework to improve efficiency in classifying data in an online fashion to overcome the streaming nature of data in computer networks. The proposed method is compared to the incremental naive Bayesian classifier using the NSL-

KDD standard dataset. After Implementation results revealed that the proposed method outperforms the naive Bayesian approach in terms of both accuracy and Kappa. Given some recommendations in detecting network anomalies which can be addressed in future studies.[25]

26. Zhigang Zhang presents a control flow anomaly detection algorithm CFCPM based on the control flow of the business programs.Given the CFCSC and RSCFC the control flow analysis algorithms implementation in software use are basic blocks as one research unit, such as CFCSC and RSCFC Proved that the algorithm can detect most of the control flow and greatly reduce the control flow anomaly detection.[26]

27. Mohammad Teshnehlab, In this paper proposed a method based on the deep neural network as feature learning method and isolation forest as a classifier and compared this method with the methods does not include feature extraction models on CSIC 2010 data set.Also implemented n-gram model for the construction of features and SAE algorithm for feature extraction and isolation forest to detect malicious requests. The Results showed that deep models have the various performances with different structures of SAE. [27]

28. Thaksen. J. Parvat introduced an unique way of deducing the call traces for raw system and its results were improved by using a true semantic interpretation.Uses extreme learning machine (ELM) a decision engine used for detecting intrusions and for checking the performance of the new semantic algorithm the KDDCup99 [18] and the ADFA Linux datasets are used for evaluation. The Public data sets are utilized for assessment of the proposed algorithm to compare with the present method. [28]

29.Hassan Dao discussed a hybrid approach to network IDS to minimize the malicious traffic in the network by using machine learning. Mainly focuses on Anomaly-based NIDS and used machine learning to improve the False Positive, Accuracy and Detection Rate. [29]

30. Youssif Al-Nashif introduces a rule based anomaly detection framework to protect a building automation network (BACS) and BACNETANOMALY DETECTION FRAMEWORK protocol targeted attacks are demonstrated. The framework continuously monitors the network behavior based on frame header and payload contents as well as network flow information. Discussed the framework modules Monitoring module, Training module, Attack Classification module, and Action Handler module[2][3]. Given a Anomaly detection framework architecture [2] and data mining algorithm was used to achieve the high detection rates.[30]

III. CONCLUSIONS

Now a day, the security is the crucial element in the computer networks. In computer network security, to identify the intrusion attacks is a big issue. The IDS was classified into two techniques namely signature and anomaly detection .The methods of anomaly detection include predictive pattern generation, neural network, sequence matching, and statistics and supervising. In this paper, we have study the foundations of the main anomaly based network intrusion detection technologies. The most significant open issues regarding Anomaly based Network Intrusion Detection systems are identified. The presented information constitutes important points for detecting anomaly based attacks. We find that the majority of surveyed works do not meet these requirements. For improving the anomaly detection method, an efficient automated hybrid technique is suggested to achieve accurate detection rate.

IV. REFERENCES

[1]. Meng-Kai Tsai, Shun-Chieh Lin, Shian-ShyongTseng ,"Protocol Based Foresight Anomaly Intrusion Detection System" National Chiao Tung University,2003.

[2]. Toru konno , Masamichi Tateoka,"Accuracy Improvement of Anomaly-based intrusion Detection System using Taguchi Method" ,Advanced Technology Department ,Japan,2005.

[3]. Damiano Bolzoni, Sandro Etalle, Pieter Hartel," POSEIDON: a 2-tier Anomaly-based Network Intrusion Detection System", University of Twente,Distributed and Embedded System Group,2006.

[4]. Damiano Bolzoni,Sandro Etalle," Approaches in anomaly-based intrusion detection systems", University of Twente,2005.

[5]. Paulo MMafra, Vinicius Moll, Joni da Silva Fraga, Altair Olivo Santin," Octopus-IIDS: An Anomaly Based Intelligent Intrusion Detection System", IEEE, 2010.

[6]. Veselina GJecheva, Evgeniya PNikolova,"An Application of Learning Problem in Anomaly-based Intrusion Detection Systems", Burgas Free University, 2007.

[7]. Benoit Morel," Anomaly-based Intrusion Detection using Distributed intelligent systems", Third International Conference on Risks and Security of Internet and Systems,2008.

[8]. Sho Ohtahara ,Takayuki Kamiyama, Yoshihiro Oyama," Anomaly-based Intrusion Detection System Sharing Normal Behavior Databases among Different Machines", Department of Computer Science, IEEE Ninth International Conference on Computer and Information Technology,2009.

[9]. Luis Miguel Torres, Eduardo Magana, Mikel Izal and Daniel Morat´o , Guzm´an Santaf´e,"An anomaly-based intrusion detection system for IEEE 802.11 networks", Departamento de Autom´atica y Computaci´on, Universidad P´ublica de Navarra,spain,2010.

[10]. Sufyan TFaraj Al-Janabi and Hadeel Amjed Saeed," A Neural Network Based Anomaly Intrusion Detection System", Developments in E-systems Engineering, 2011.

[11]. Hae-Duck JJeong, WooSeok Hyun, Jiyoung Lim, and Isun You," Anomaly Teletraffic Intrusion Detection Systems on Hadoop-based Platforms:A Survey of Some Problems and Solutions",15th International Conference on Network-Based Information Systems,2012.

[12]. Deepak Kumar Singh , MrJitendra Kumar Gupta,"An approach for Anomaly based Intrusion detection System using SNORT", International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September,2013.

[13]. Nilanjan Sen, Rinku Sen , Manojit Chattopadhyay," An Effective Back Propagation Neural Network Architecture for the development of An Efficient Anomaly Based Intrusion Detection Systems", Sixth International Conference on Computational Intelligence and Communication Networks,2014.

[14]. Alka Chaudhary, V.NTiwari, Anil Kumar," Design an Anomaly Based Fuzzy Intrusion Detection System for Packet Dropping Attack in Mobile Ad Hoc Networks", IEEE International Advance Computing Conference (IACC),2014.

[15]. Dipika Narsingyani, Ompriya Kale," Optimizing False Positive In Anomaly based Intrusion Detection using Genetic Algorithm", IEEE 3rd International Conference on MOOCs, Innovation and Technology in Education (MITE),2015.

[16]. Evgeniya Nikolova, Veselina Jecheva," Applications of Clustering Methods to Anomaly-Based Intrusion Detection Systems", 8th International Conference on Database Theory and Application, 2015.

[17]. Naila Belhadj Aissa, Mohamed Guerroumi,"A Genetic Clustering Technique for Anomaly-

Based Intrusion Detection Systems", IEEE SNPD Takamatsu, Japan, 2015.

[18]. M.Anandapriya, Mr.B.Lakshmanan,"Anomaly Based Host Intrusion Detection System Using Semantic Based System Call Patterns", IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO), 2015.

[19]. Abdelaziz Amara korba, Mehdi Nafaa, and Yacine Ghamri-Doudane," Anomaly-Based Intrusion Detection System for Ad hoc Networks", IEEE, 2016.

[20]. Evgeniya Nikolova, Veselina Jecheva," Anomaly Based Intrusion Detection Using Data Mining and String Metrics", International Conference on Communications and Mobile Computing, 2009.

[21]. Panagiotis IRadoglou-Grammatikis, Panagiotis GSarigiannidis," Flow Anomaly Based Intrusion Detection System for Android Mobile Devices", 6th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2017.

[22]. Pratik Satam," Anomaly Based Wi-Fi Intrusion Detection System",IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS*W),2017.

[23]. Chau Tran, Tran Nguyen Vo, Tran Ngoc Thinh." HA-IDS: A Heterogeneous Anomaly-based Intrusion Detection System", 4th NAFOSTED Conference on Information and Computer Science, 2017.

[24]. Imtiaz Ullah, Qusay HMahmoud," A Filter-based Feature Selection Model for Anomaly-based Intrusion Detection Systems", IEEE International Conference on Big Data (BIGDATA),2017.

[25]. Parisa Alaei,Fakhroddin Noorbehbahani," Incremental Anomaly-based Intrusion Detection System Using Limited Labeled Data", 3th International Conference on Web Research (ICWR), 2017.

[26]. Dayu Yang, Alexander Usynin, and JWesley Hines," Anomaly-Based Intrusion Detection for SCADA Systems", Department of Nuclear Engineering University of Tennessee Knoxville.

[27]. Ali Moradi Vartouni, Saeed Sedighian Kashi, Mohammad Teshnehlab,"An Anomaly Detection Method to Detect Web Attacks Using Stacked Auto-Encoder", 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), 2018.

[28]. Sandeep Ankush Maske, ThaksenJParvat,"Advanced Anomaly Intrusion Detection Technique For Host Based System Using System Call Patterns", IEEE, 2016.

[29]. Mohd Raffie Z.A, Megat FZuhairi, Shadil AkimiZ,A, Hassan Dao,"Anomaly-Based NIDS: A Review of Machine Learning Methods on Malware Detection", International Conference on Information and Communication Technology (ICICTM), 16th - 17th May 2016.

[30]. Zhiwen Pan, Salim Hariri, Youssif Al-Nashif,"Anomaly Based Intrusion Detection for Building Automation and Control Networks", IEEE, 2014.