

A Survey: Recent Autonomous Security Techniques for Detection & Avoidance of Network Attacks

Supriya Gupta¹, Ankur Goyal²

¹M.Tech Scholar, Department of Computer Science & Engineering, Y.I.T., Jaipur, Rajasthan, India

²Associate Professor, Department of Computer Science & Engineering, Y.I.T., Jaipur, Rajasthan, India

Abstract: *Over the past several years, uses of networks-based services and users of the Internet have gain tremendous growth to exchange information without any distance barrier. However, such network is most popular for fast and easy process to exchange information over the long distance but the safety and security of long-distance communication remains an issue in the case of confidential data. Day by day with the growth of computer networks, number of attacks has comes in new form to impacting availability, confidentiality, and integrity of critical data that poses a serious problem for their detection and exploits safety vulnerabilities. On the other hand human labeling of the available network audit data instances is usually tedious, time consuming and expensive. Therefore it is essential for a system administrator that he/she use one or more security tools to protect information from passing before curious eyes or, more importantly, from falling into wrong hands. In this paper, we present a current investigation of the network security system, which may help to the researchers to better understand the pitfalls of accessible security systems and to build a more secure data security mechanism.*

Keywords: Attacks, Network Security, Anomaly Detection, Misuse Detection

1. Introduction

Nowadays, Individuals and organizations hardly accomplish their daily tasks without relying on the conveniences provided by computer networks and Internet technologies. Therefore, attackers could have exploited the weaknesses of such technologies to take advantage of the information gained from the individuals as well as organizations. With the deployment of more sophisticated security tools, in order to protect the data and services, the attackers often come up with newer and more advanced methods to defeat the installed security systems [1],[2]. During recent years, number of attacks has dramatically increased. Therefore, it is very important to prevent the system from such types of attacks. The hindrance of such attacks is entirely dependent on their detection that is a key part of any security tool such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Adaptive Security Alliance (ASA), checkpoints and firewalls.

An attack is defined as any set of actions that compromise the integrity, confidentiality or availability of a resource [3], [4]. Mostly attacks are the violation of information security policy. A security system like Intrusion Detection System (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. The first system that was implemented to provide the security against different categories of attacks was host (System) based that located in servers to examine the internal interfaces [5]-[7]. After that with the advancement of the computer networks the focus gradually shifted toward network-based. Network attack prevention system performs packet logging, real-time traffic analysis of IP network, and tries to discover if an attacker is attempting to break into the system [8]-[10]. The system gathers and analyzes information from various areas within a computer or

a network to identify possible security breaches, which include both intrusions and misuse. Today, prevention from different types of attack categories is one of the high priority and challenging tasks for network administrators and security professionals.

However a number of approaches have proposed by several of researchers to reduce the pitfalls of existing security system but most of them have many limitations like time consuming statistical analysis, requiring regular updating, non-adaptive, low accuracy, inflexibility and are tuned specifically to detect known major service level network attacks. The techniques that use to detect and to prevent the system from attacks are identified as the attack detection systems or security techniques. However, the difference between prevention and detection is slowly diminishing as the existing detection systems increasingly focus on real-time attack detection and blocking an attack before it reaches the target. Such systems are better known as the Prevention Systems. Typically two types of errors are important to know in attack detection:

- **False positives:** This type of errors comes when a normal type action detected as an attack types. In general false alarms are known as false positive.
- **False negatives:** it represents a situation in which an attack is not detected by security system and behaves like a normal activity.

2. Attack Detection Systems and Conventional Security Labels

Typically attacks are actions aimed to compromise the confidentiality, integrity, and/or availability of a computer or computer network. Detection of an attack is the process of monitoring and analyzing the events occurring in a computer system in order to detect signs of security problems. The

several dissimilar systems provide unique functions and mechanisms for attack detection with the aim to detect, filter, or prevent system from attack to provide data security and ensure continuity of services provided by a network. Traditional methods for attack detection are based on extensive knowledge of signatures of known attacks. With the rapid advancement in the network technologies including higher bandwidths and ease of connectivity of wireless and mobile devices, the focus of detection system has shifted from simple signature matching approaches to detecting attacks based on analyzing contextual information which may be specific to individual networks and applications. Broadly detection system can be categorized in two categories: (i) Host-based (ii) Network-based detection system [11].

2.1 Host-based Attack Detection System

Host-based attacks target a machine and try to gain access to privileged services or resources on that machine. Host-based detection usually uses routines that obtain system call data from an audit process, which tracks all system calls made on behalf of each user.

2.2 Network-based Attack Detection System

Network-based attacks make it difficult for legitimate users to access various network services by deliberately occupying or sabotaging network resources and services. This can be done by sending large amounts of network traffic, exploiting well-known faults in networking services, and overloading network hosts.

According to the detection principle, the attack detection technology may divide into Misuse / Signature-based Detection and Anomaly Detection [12], [13].

2.3 Misuse / Anomaly Attack Detection System

Misuse / Signature-based Detection technique looks for patterns and signatures of already known attacks in the network traffic. A constantly updated database is usually used to store the signatures of known attacks. The way this technique deals with intrusion detection resembles the way that anti-virus software operates. Misuse detection catches intrusions in terms of the characteristics of known attacks or system vulnerabilities; any action that conforms to the pattern of a known attack or vulnerability is considered.

2.4 Active / Passive Attack Detection System

Active attacks configured automatically, block suspected attacks without any intervention required by an operator. It has the advantage of providing real-time corrective action in response to an attack. Passive system only alerts the operator against attacks and potential vulnerabilities. The operator of the system takes responsive action on the base of information. This type of attack detection system is not capable of performing any protective or corrective functions on its own. The major advantages of these type of systems are that the systems can be easily and rapidly deployed and are not normally susceptible to attack themselves. Usually the security approaches can be labeled into the following areas.

- **Attack Deterrence** – it refers to influence an assailant not

to initiate an attack by increasing the perceived risk of negative consequences for the attacker. However, it covers a fairly permissible system to help attack anticipation but requires strong evidence against the attacker in case an attack was launched.

- **Attack Prevention** – As like the name it aims to prevent the system from attacks by blocking. To block an attack it is must for a system that system has a complete knowledge of all possible attacks in advance, which is always not possible because of frequent generation of new types of attacks. Firewall is a best example of attack prevention system.
- **Attack Avoidance** – it aims to make the source not viable by an attacker even though the attacker is able to illegally access that resource. An example of security mechanism for attack avoidance is the use of cryptography. Encrypting data renders the data useless to the attacker, thus, avoiding possible threat.
- **Attack Detection** – same as its name it refers to sense an attack while the attack is still in growth or to detect an attack which has already occurred in the past. Detecting an attack is important for two causes; first the system must recover from the damage caused by the attack and second, it allows the system to take measures to prevent similar attacks in future. Research in this area focuses on building intrusion detection systems.
- **Attack Reaction and Recovery** – Once an attack is detected, the system must react to an attack and perform the recovery mechanisms as defined in the security policy.

3. Challenges and Requirements for Fine Attack Detection System

The attack detection system is most important tool to provide security for computer and networks. The different approaches are proposed and implemented to accomplish the desirable elements of a detection system but they all require the exacting and suitable recognition of the attack.

A single attack can cause a heavy loss in a computer network or the consistency of network became insecure. To reduce the effect of attacks in the system or network it is good to detect at an early stage as it entered. For building a high-quality detection system the major challenges and requirements are:

- The system must be able to detect attacks reliably without giving false alarms. It is very important that the false alarm rate is low as in a live network with large amount of traffic, the number of false alarms may exceed the total number of attacks detected correctly thereby decreasing the confidence in the attack detection capability of the system. Ideally, the system must detect all attacks with no false alarms. The challenge is to build a system which has broad attack detection coverage, i.e. it can detect a wide variety of attacks and at the same time which results in very few false alarms.
- The system must be able to handle large amount of data without affecting performance and without dropping data, i.e. the rate at which the audit patterns are processed and decision is made must be greater than or equal to the rate of arrival of new audit patterns. Hence the speed of operation is critical for systems deployed in high speed

networks. In addition, the system must be capable of operating in real-time by initiating a response mechanism once an attack is detected. The challenge is to prevent an attack rather than simply detecting it.

- A system which can link an alert generated by the intrusion detector to the actual security incident is desirable. Such a system would help in quick analysis of the attack and may also provide effective response to intrusion as opposed to a system which offers no after attack analysis. Hence, it is not only necessary to detect an attack, but it is also important to identify the type of attack.
- It is desirable to develop a system which is resistant to attacks since, a system that can be exploited during an attack may not be able to detect attacks reliably.
- Every network and application is different. The challenge is to build a system which is scalable and which can be easily customized as per the specific requirements of the environment where it is deployed.

4. Related Work

Since the born of first attack detection technique, several of approaches have been proposed by the researchers to provide more security to the single host and/or to network system. In current scenario, several of attack detection technologies are exist but each type of techniques has it owns advantages and disadvantage in detection, configuration, and cost. On the other hand day by day attacks are comes in new flavor that pose a challenging state to the accessible system to detect the intrusive activity on a network or a device.

The concept of attack detection was firstly introduce [14] in 1980, the author launch a risk arrangement model that build up a security observing surveillance system based on detecting anomalies in user behavior. The lead was then taken by [15] at the SRI International and the first model of detection has been introduces [16]. The system was rule based for monitoring traffic on network and achieve high precision rate. The rule based methods extract features from various audit streams, and detect attacks by comparing the feature values to a set of attack signatures provided by human experts. The signature database has to be manually revised for each new type of attack that is discovered. If the network is small and signatures are kept up to date, the human analyst solution to intrusion detection works well. But when organizations have a large, complex network the human analysts quickly become overwhelmed by the number of alarms they need to review. Therefore, the process of encoding rules is expensive and slow.

However, numerous approaches have been proposed to overcome the limitations of the rule-based systems [17],[18]. These techniques have been used to mine normal patterns from audit data and concentrate on analyzing the properties of the audit patterns rather than identifying the process which generated them [19]. Different approaches like classification, clustering, association rule, and outlier detection are frequently used to analyze network data to gain attacks related knowledge. The Audit Data Analysis and Mining (ADAM) [19] used tcpdump to build profiles of rules for classifications. In [20], k-means clustering algorithm applied

for detection. The clustering technique has limitation that it cannot be easily used with symbol features, the observation must be numeric. It considers the features independently and unable to capture the relationship between different features of a single record, which degrades attack detection accuracy.

A concurrent attack detection system proposed in [21] for large-scale of attacks by using fuzzy association rules. The technique selected the 16 attributes from release network environment and passes each packet through the selected attributes. Then, each record will be sent to another computer in order to update new rule. However this technique does not show the detection rate and is able to detect only DoS attack. In same context one another neural network based approach has been proposed in [22], proposed approach in this paper introduces real-time network attack detection; they collected the network traffic by using an open source attack detection system (Bro IDS). This technique is able to detect unknown attack in real time. However, it can classify only 2 classes attack and normal.

In [23],[24] authors use neural network for NIDS. Like some of other algorithms neural network show efficient performance with noisy data but for training it required huge amount of data that often is not easy to select the best possible architecture for the neural network. In [25], approach includes neural networks and fuzzy logic with network profiling that uses simple data mining techniques to process the network data. The model —Intelligent Attack Detection Systeml combines anomaly, misuse and host based detection. Simple Fuzzy rules allow constructing if-then rules that reflect common ways of describing security attacks.

Another approach shows that Naïve bayes classifier has an advantage over neural network classifier in terms of detection rates and false positives [26]. The two phases feature selection method discussed in [27]. The algorithm at first stage eliminates the worthless information from the original high dimensional database and at the next step design a method to solve the problems of uncertainty caused by limited and ambiguous information. In [28],[29] use data mining technique association rules together with fuzzy logic use to proposes a model for detection systems, anomaly detection based on fuzzy association rules which use genetic programming. The data mining and network behavior analysis approaches for network intrusion detection discuss in [30], recommended that a combination of both approaches has the potential to detect intrusions in networks more effectively. A Length-Decreasing Support to detect attacks based on data mining proposed in [31], which is an improved Apriori algorithm. In [32], Author presents a novel approach for learning from imbalanced data sets, based on a combination of the SMOTE algorithm and the boosting procedure. Unlike standard boosting where all misclassified examples are given equal weights, SMOTEBoost creates synthetic examples from the rare or minority class, thus indirectly changing the updating weights and compensating for skewed distributions.

In same way two new approaches has been proposed by [33] for anomalous network packet detection based on the data stream mining paradigm. In first way the author modified

DenStream algorithm for stream clustering specifically tailored to evaluate network traffic. In this algorithm, individual packets are treated as points and are flagged as normal or abnormal based on their belonging to either normal or outlier clusters. The second algorithm utilizes a histogram to create a model of the evolving network traffic to which incoming traffic can be compared using Pearson correlation. This approach achieve reasonably high detection rates with moderately low false positive percentages for different types of attacks but required more parameters than the clustering-based algorithm. A hybrid system proposed in [34], which combine the anomaly and misuse detection.

To improve the detection rate of attacks a novel attack detection model has been proposed [35]. The proposed model performs well for all the classes of attack. In this framework authors use four tiers architecture to enhance the adaptability of the cyber attack detection. The data collection and preprocessing of the proposed model is included in first tier of proposed model. The Second tier is meant for the feature extraction technique, third tier is dedicated to classification of cyber attacks and fourth tier is dedicated to user interface for reporting the events. The Second tier is meant for the feature extraction technique, third tier is dedicated to classification of cyber attacks and fourth tier is dedicated to user interface for reporting the events.

Several of researchers proposed layered approaches [2],[36],[37] for improving the quality of detection system. In [2], [36] authors addressed the dual problem of accuracy and efficiency for building robust and efficient detection systems. They used CRFs for improving the attack detection rate and decreasing the FAR. Having a low FAR is very important for any intrusion detection system. Further, feature selection and implement the layered approach significantly to reduce the time required to train and test the model. The proposed system achieved high gain in attack detection accuracy, particularly, for the U2R attacks (34.8 percent improvement) and the R2L attacks (34.5 percent improvement). A combinational model is designed in [37] for attack detection mechanism. The meta-modeling applied in this for gaining better classification performance than any individual classifier. To test the results used NSL-KDD datasets; and also applied PCA for feature reduction that results in a significant improvement on learning algorithms.

A novel framework [38], [39] proposed to satisfy the core purpose of attack detection system, and allows detecting the attacks as quickly as possible with available data using mobile agents. This framework was mainly designed to provide security for the network using mobile agent mechanisms to add mobility features to monitor the user processes from different computational systems. The experimental results have shown that the system can detect anomalous user activity effectively.

In [40], intelligent detection and prevention system proposed to monitors a single host system from three different coating. A multifaceted approach files analyzer, system resource and connection layers used in which each layer connects both aspects of existing approach, signature and anomaly approaches, to achieve a better detection and prevention

capabilities. The First layer, File-analyzer direct monitoring the files and folders on a host server that could be of interest to any attacker and this is determined to a large extent by the administrator. The administrator decides on the important files or directories to monitor so that the detection system does not monitor all the files and folders on the machine as this would cause a large overhead on the system resources.

The Second layer in system is designed to periodically scan through the system log for latest entries and compare with the threshold value that must have been defined by the user. This enables the system resources layer to detect attacks on system resources. The next connection layer monitors all of connections made to a host machine. The design of attack detection system consist of three basic components; the iExecutive which is an agent that runs in the background, iBaseline which is a database that stores the signatures of intrusions and the iManager which is a user Interface that serves as an intermediary between the detection system and the user. The standalone techniques face several of problems in detecting the unforeseen attacks because of different techniques often expose different pros and cons;. Therefore, the use of multiple classifier systems (also called communal systems) to avoids the risk of mistake in choosing a poor or inappropriate classifier as the target attack detection model. Multi classifier approaches have brought many remarkable contributions to the detection domain. There are many types of ensemble proposed in the machine learning literature.

Two classifier algorithm selection models [41] proposed, after evaluating the performance of a comprehensive set of classifier algorithms using KDD99 dataset. The multiple classifier system based approach [42] proposed to handle unlabeled network anomaly attacks detection. The various modules use by proposed model in which each module specifically designed to model a particular group of similar protocols or network services. The DT and SVM combine in [43] to propose a novel hybrid attack detection system, in which for generating leaf node information training set is passed through the DT classifier and after that SVM classifier trained to provide effective output from the model.

A fresh method has been proposed in [44], to secure the system against the novel cyber attacks. The approach performs well to detect the attacks of almost all of attack categories. The proposed system use the concepts of layering in which at first level the system collect the data and have done the d preprocessing work. After that at second level smallest feature set has select for each type of attacks detection. The classification work has done at the third layer of the proposed system and the forth or last layer of the proposed system was dedicated to user interface for reporting the events. In same context another authors has proposed a innovative learning algorithm [45], the proposed approach use decision tree to prevent the system from anomaly attacks. A improved Support Vector Machine (iSVM) has been proposed in [46]. The proposed method improved the performance of the classical SVM and increases the attack detection power especially for Denial of Service (DOS) classes and comparable to false alarm rate. To increases the detection ration proposed approach modify Gaussian kernel to enlarge the spatial resolution around the margin by a conformal mapping. It is based on the Riemannian

geometrical structure induced by the kernel function. To improve the attack detection the approach present in [47] has combine the clustering and naïve based approach, in which approach firstly applied the dimension reduction technique and after that on reduced data set fuzzification of feature values is done to get simpler range. The approach performs well in terms of detecting attacks faster and with reasonable reduction in false alarm rate.

Adaboost algorithm for network attack detection system with combination of multiple weak classifiers is proposed in [48]. The classifiers such as Bayes Net, Naive Bayes and Decision Tree have been used as weak classifiers. A benchmark dataset is used in these experiments to demonstrate that boosting algorithm can greatly improve the classification accuracy of weak classification algorithms. The approach achieves higher detection rate with low false alarm rates and is scalable for large datasets, resulting in an effective detection system. In same context a new detection approach, especially for network attack detection, based on improved genetic algorithm (GA) and multi-ANN classifiers has proposed in [49]. The improved GA used energy entropy to select individuals, optimize the training procedure of the BPNN, RBF, PNN and Fuzzy-NN. Then, the satisfactory ANN models with proper structure parameters were attained. In addition, to alleviate the complexity of the input vector, the principal component analysis (PCA) has been employed to eliminate redundant features of the original disturbance data. The efficiency of the proposed method was evaluated with the practical data, and the experiment results show that the proposed approach offers a good detection rate, and performs better than the standard GA-ANN method.

5. Problems in Current Attack Detection Approaches

Traditional methods for network attack detection are based on extensive knowledge of signatures of known attacks. Monitored events are matched against the signatures to detect attacks. These methods extract features from various audit streams, and detect attack by comparing the feature values to a set of attack signatures provided by human experts. The signature database has to be manually revised for each new type of attacks that is discovered. If the network is small and signatures are kept up to date, the human analyst solution to attack detection works well. But when organizations have a large, complex network the human analysts quickly become overwhelmed by the number of alarms they need to review.

The traditional model of detection has established inefficient and the cost of research is so much. Additionally, with more and more data becoming available in digital format and more applications being developed to access data, the data and applications are also a victim of attackers who exploit these applications to gain access to data. With the deployment of more sophisticated security tools, in order to protect the data and services, the attackers often come up with newer and more advanced methods to defeat the installed security systems. A significant limitation of existing intrusion detection methods is that they cannot detect emerging cyber threats, since by their very nature these threats are launched using previously unknown attacks. In addition, even if a new

attack is discovered and its signature developed, often there is a substantial latency in deployment across networks. These limitations represent the problem with the currently existing attack detection system, and have led to an increasing interest in attack detection techniques.

6. Conclusion

This paper presents the some basics of network attack detection system with the details of security labels. Furthermore, the challenges and requirements for fine attack detection system with the problems in current attack detection approaches are also discussed, which may help to the researchers to better understand the network attack detection system. The presented shortcoming of current security approaches may help to the researchers in building a more secure network security system.

References

- [1] Overview of Attack Trends, 2002. Last accessed: November 30, 2008. http://www.cert.org/archive/pdf/attack_trends.pdf.
- [2] Kapil Kumar Gupta, Baikunth Nath, Kotagiri Ramamohanarao, and Ashraf Kazi. Attacking Confidentiality: An Agent Based Approach. In Proceedings of IEEE International Conference on Intelligence and Security Informatics, pages 285–296. Lecture Notes in Computer Science, Springer Verlag, Vol (3975), 2006.
- [3] Jian Pei Shambhu J. Upadhyaya Faisal Farooq Venugopal Govindaraju. Proceedings of the 20th International Conference on Data Engineering (ICDE'04) 1063-6382/04 \$ 20.00 © 2004 IEEE
- [4] Debar, H., Dacier, M., and Wespi, A., A Revised taxonomy for intrusion detection systems, *Annales des Telecommunications*, Vol. 55, No. 7–8, 361–378, 2000.
- [5] Jackson, T., Levine, J., Grizzard, J., Owen, and H., "An investigation of a compromised host on a honeynet being used to increase the security of a large enterprise network," IEEE workshop on Information Assurance and Security, IEEE, 2004.
- [6] D. Y. Yeung, and Y. X. Ding, "Host-based intrusion detection using dynamic and static behavioral models," *Pattern Recognition*, 36, 2003, pp. 229-243.
- [7] X. Xu, and T. Xie, "A reinforcement learning approach for host-based intrusion detection using sequences of system calls," In Proc. of International Conference on Intelligent Computing, Lecture Notes in Computer Science, LNCS 3644, 2005, pp. 995-1003.
- [8] Krasser, S., Grizzard, J., Owen, H., and Levine. J., "The use of honeynets to increase computer network security and user awareness," *Journal of Security Education*, vol. 1, 2005, pp. 23-37.
- [9] Shon T., Seo J., and Moon J., "SVM approach with a genetic algorithm for network intrusion detection," in Proc. of 20th International Symposium on Computer and Information Sciences (ISCIS 2005), Berlin: Springer-Verlag, 2005, pp. 224-233.
- [10] X. Xu, X.N. Wang, "Adaptive network intrusion detection method based on PCA and support vector

- machines,” Lecture Notes in Artificial Intelligence (ADMA 2005), LNAI 3584, 2005, pp. 696-703.
- [11] Asmaa Shaker Ashoor, Prof. Sharad Gore —Importance of Intrusion Detection System (IDS) International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011
 - [12] Marchette, D., A statistical method for profiling network traffic, First {USENIX} Workshop on Intrusion Detection and Network Monitoring, Santa Clara, CA, 1999, pp. 119–128.
 - [13] McCanne, S., Leres, C., and Jacobson, V., libcap, available via anonymous ftp at ftp://ftp.ee.lbl.gov/, 1989.
 - [14] James P. Anderson, “Computer security threat monitoring and surveillance,” Technical Report 98-17, James P. Anderson Co., Fort Washington, Pennsylvania, USA, April 1980.
 - [15] Dorothy E. Denning, and P.G. Neumann “Requirement and model for IDes- A real-time intrusion detection system,” Computer Science Laboratory, SRI International, Menlo Park, CA 94025-3493, Technical Report # 83F83-01-00, 1985.
 - [16] H. S. Javitz and A. Valdes. The SRI IDes Statistical Anomaly Detector. In Proceedings of the IEEE Symposium on Security and Privacy, pages 316–326. IEEE, 1991.
 - [17] Barbarà, D., Couto, J., Jajodia, S., Popyack, L., and Wu, N., ADAM: A Testbed for Exploring the Use of Data Mining in Intrusion Detection, ACM SIGMOD Record, 30(4), 2001, pp. 15-24.
 - [18] Wenke Lee and Salvatore J. Stolfo, —A Framework for Constructing Features and Models for Intrusion Detection Systems, ACM Transactions on Information and System Security (TISSEC), Volume 3, Issue 4, November 2000.
 - [19] Animesh Patcha and Jung-Min Park. An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends. Computer Networks, 51(12):3448– 3470, 2007.
 - [20] L. Portnoy, E. Eskin, and S. Stolfo, —Intrusion Detection with Unlabeled Data Using Clustering, Proc. ACM Workshop Data Mining Applied to Security (DMSA), 2001.
 - [21] M-Y. Su, et al., “A real-time network intrusion detection system for Large-scale attacks based on an incremental mining approach,” Computers and Security 28 (5), pp. 301-309.
 - [22] P. Kachurka, V. Golovko., “Neural network approach to real-time Network intrusion detection and recognition,” The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS'2011, Art.No. 6072781 , pp. 393-397.
 - [23] Anup K. Ghosh, James Wanken, and Frank Charron. Detecting Anomalous and Unknown Intrusions Against Programs. In Proceedings of the 14th Annual Computer Security Applications Conference, pages 259–267. IEEE, 1998.
 - [24] Zheng Zhang, Jun Li, C.N. Manikopoulos, Jay Jorgenson, and Jose Ucles. HIDE: a Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification. In Proceedings of the IEEE Workshop on Information Assurance and Security United States Military Academy, pages 85–90. IEEE, 2001.
 - [25] Anup K. Ghosh, Aaron Schwartzbard, and Michael Schatz. Learning Program Behavior Profiles for Intrusion Detection. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring, pages 51–62. USENIX Association, 1999.
 - [26] M. Panda, and M. R. Patra, —Network intrusion detection using naïve Bayes, International Journal of Computer Science and Network Security (IJCSNS), Vol. 7, No. 12, December 2007, pp. 258-263
 - [27] T. S. Chou, K. K. Yen, and J. Luo —Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms. International Journal of Computational Intelligence 4;3 2008
 - [28] G.V.S.N.R.V.Prasad, Y.Dhanalakshmi, Dr.V.Vijaya Kumar Dr I.Ramesh Modeling An Intrusion Detection System Using Data Mining and Genetic Algorithms Based On Fuzzy Logic, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008
 - [29] Y.Dhanalakshmi, Dr.I. Ramesh Babu —Intrusion Detection Using Data Mining Along Fuzzy Logic and Genetic Algorithms IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008
 - [30] Ahmed Youssef And Ahmed Emam —Network Intrusion Detection Using Data Mining And Network Behaviour Analysis International Journal of Computer Science & Information Technology (Ijcsit) Vol 3, No 6, Dec 2011
 - [31] Lei Li, De-Zhang Yang, Fang-Cheng Shen —A Novel Rule-based Intrusion Detection System Using Data Mining 978-1-4244-5539-3/10/\$26.00 ©2010 IEEE
 - [32] Ms.Nivedita Naidu, Dr.R.V.Dharaskar —An effective approach to network intrusion detection system using genetic algorithm, International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 2, 2010.
 - [33] Zachary Miller, William Deitrick, Wei Hu* —Anomalous Network Packet Detection Using Data Stream Mining Journal of Information Security, 2011, 2, 158-168 doi:10.4236/jis.2011.24016 Published Online October 201 (http://www.SciRP.org/journal/jis)
 - [34] Rasha G. Mohammed, Awad M. Awadelkarim —Design and Implementation of a Data Mining-Based Network Intrusion Detection Scheme Asian Journal of Information Technology, Year: 2011 | Volume: 10 | Issue: 4 | Page No.: 136-141
 - [35] Shailendra Singh, Sanjay Silakari “An Ensemble Approach for Cyber Attack Detection System: A Generic Framework” 14th ACIS, IEEE 2013. Pp 79-85.
 - [36] Mr.C.Saravanan, Mr.M.V.Shivsankar, Prof.P.Tamije Selvy, Mr.S.Anto —An Optimized Feature Selection for Intrusion Detection using Layered Conditional Random Fields with MAFS International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol.2, No.3, June 2012
 - [37] Ankita Gaur, Vineet Richariya —A Layered Approach for Intrusion Detection Using Meta-modeling with Classification Techniques International Journal of

Computer Technology and Electronics Engineering
(IJCTEE) Volume 1 , Issue 2

- [38] N.Jaisankar¹ and R.Saravanan² K. Durai Swamy —intelligent intrusion detection System framework using mobile Agents|| International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009
- [39] B.Bhanu Chander*, K. Radhika, D. Jamuna — An Approach On Layered Framework For Intrusion Detection System|| Asian Journal of Computer Science And Information Technology 2: 8 (2012) 230 – 233.
- [40] Oludele Awodele, Sunday Idowu, Omotola Anjorin, and Vincent J. Joshua —A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS)|| Issues in Informing Science and Information Technology Volume 6, 2009
- [41] Y. Ma, D. Choi, and S. Ata (Eds.) —Application of Data Mining to Network Intrusion Detection: Classifier Selection Model|| APNOMS 2008, LNCS 5297, pp. 399–408, 2008. © Springer-Verlag Berlin Heidelberg 2008
- [42] G. Giacinto, R. Perdisci, M.D. Rio, F. Roli: Intrusion detection in computer networks by a modular ensemble of one class classifiers. In Information Fusion, 9, 69-82 (2008)
- [43] S. Peddabachigari, A. Abraham, C. Grosan, J. Thomas: Modeling intrusion detection system using hybrid intelligent systems . In Journal of Network and Computer Applications, 30, 114-132 (2007)
- [44] Shailendra Singh, Sanjay Silakari “An Ensemble Approach for Cyber Attack Detection System: A Generic Framework” 14th ACIS, IEEE 2013. Pp 79-85.
- [45] Dewan Md. Farid, Nouria Harbi, Emna Bahri, Mohammad Zahidur Rahman, Chowdhury Mofizur Rahman “Attacks Classification in Adaptive Intrusion Detection using Decision Tree” World Academy of Science, Engineering and Technology, 2009. Pp 86-91.
- [46] Shailendra Singh, Sanjay Agrawal, Murtaza, A. Rizvi and Ramjeevan Singh Thakur “ Improved Support Vector Machine for Cyber Attack Detection” WCECS IEEE 2011. Pp 1-6.
- [47] Vineet Richhariya , Dr. J.L.Rana ,Dr. R.C.Jain ,Dr. R.K.Pandey” Design of Trust Model For Efficient Cyber Attack Detection on Fuzzified Large Data using Data Mining techniques” IJRCCT Vol 2, Issue 3, 2013. Pp 126-132.
- [48] P. Natesan, P. Balasubramanie, G. Gowrison —Improving Attack Detection Rate in Network Intrusion Detection Using Adaboost Algorithm with Multiple Weak Classifiers|| Journal of Information & Computational Science 9: 8 (2012) 2239–2251 Available at <http://www.joics.com>
- [49] Yuesheng Gu, Yongchang Shi, Jianping Wang —Efficient Intrusion Detection Based on Multiple Neural Network Classifiers with Improved Genetic Algorithm|| JOURNAL OF SOFTWARE, VOL. 7, NO. 7, JULY 2012