# An Intrusion Detection System for Network Security based on an Advanced Honeypots Server

K. Veena [1], K. Meena [2]

[1] Dhanalakshmi College of Engineering
[1, 2] *Department of Computer Science and Engineering*
Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Chennai, India
[1] veenakanagaraj07@gmail.com, [2] meen.nandhu@gmail.com

***Abstract* – The current greatest challenge to Network security is cyber warfare. Every part of computer network security is an essential component. In the existing technologies computer networks and systems are more crucially concerned with network security. The greatest challenge in network is addressing security to the server side. This latest end-to-end research paper recommends to improve the security performance to protect the network from intruders. An advanced honeypot based Intrusion Detection technique is used to detect and analyze threats to ensure security. The Honeypot technique adds a layer to the network security to enhance its performance. A key feature of honeypot is to distract the attacker from the real system to derive important information about hacker activities. To validate whether the clients are authorized or unauthorized and monitor the unauthorized client activities, as a first step we use IP validation together with vulnerability detection of user activities. In the second step we use voice recognition as detectors of malicious attacks. Once IP validation and voice recognition are processed and matched then the client is an authorized client and the packet is transmitted to the server, but if not matched it is an unauthorized client, then the packet transmits it to the honeypot server. Our experiment has demonstrated that this particular approach can successfully identify unknown attacks with greater than 95% detection rate and less than 1% false alarm rate.**

***Keywords - Intrusion Detection System, Honeypot server, Voice Recognition, IP validation.***

## I. INTRODUCTION

The real time application systems are obviously growing very rapidly because of its worldwide usage. Major usage includes the storing and transporting of sensitive data over the Internet [1][2]. This model is more essential and opened up to the day to day secured network and application security protection devices. Security experts usually programmed their database system with a huge number of signatures to help in the detection of known web-based threats [3]. New kinds of various attacks are hidden. Practically, it is not achievable to keep updating the database with the recently identified vulnerabilities.

Network security growing in an enormous way and the huge increase in the applications quantity that rely on it, network security is in advance increasing its importance. Moreover, almost all computer systems are suffering by security vulnerabilities by various kinds of technical difficulties and their increased cost in an enormous way to be solved by the manufacturers. As a result, Intrusion Detection Systems (IDSs) role, is to detect vulnerabilities and find the attacks in a network are more important [4]. Intrusion Detection System (IDS) distinguishes the traffic coming from clients and the traffic originate from the attackers or intruders by using secure technologies on the basis of honeypot. Honeypot provides effective solution to increase the security and reliability of the network [5].

In this research paper, proposed advanced honey pot based Intrusion Detection System techniques those are used to detect and analyze the attack to ensure the performance of the network security performance and shielding the network from intruders. As a result of its performance wise usually, Intrusion Detection System (IDS) is divided into two major types as: IP validation based detection and voice recognition based detection. The overall concept of and process of Intrusion Detection Systems is to achieve the advantage of vulnerabilities detection with high detection rate on recognized intrusions as well as the ability of detectors in detecting malicious attacks.

Honey pot is marvelous because it has the capacity to detect new attacks and improve the security of the network by using the existing intelligence of the security technologies. The way attackers hack and examine their behavior, Honey pot are implemented in such a way to cooperate the new threats and receive the attackers. The two validation techniques are implemented by the proposed techniques. The first category IP validation for vulnerability user activities detecting, which purpose for IP validation process is to validate whether the clients is certified or not and monitor the not certified client activities. The second level of voice recognition to ability

of detectors in detecting malicious attacks, in voice recognition process used to verify if the clients is certified or not certified and monitor the client activities which are not certified.

Depending on the result of IP validation and voice recognition done on the client, a certified client packet is transmitted to server, or the packet is transmitted to the honey pot server (if clients are not certified). The approach has successfully identified unknown attacks with greater than a 95% detection rate and less than a 1% fake alarm rate by executing this experiment.

This paper is structured as follows. In section 2, a brief explanation of the previous author work is given, section 3 presents the proposed intrusion detection systems classification and the aspects of different stages, in section 4, our investigational outcome are shown, finally, Section 5 concludes this research study and proposes future research work.

## II. RELATED WORK

Shahid Anwaretal [6], proposed the increase in attacks on network communication devices has ended in reduced network operation, output and performance. As a means to identify and reduce these network attacks, Intrusion Detection Systems (IDSs) having automatic response feature were developed. In fact, the auto-response system is regarded as the most vital part of IDS as the Intrusion Detectors may not operate appropriately in counteracting different attacks during real-life applications. To reciprocate properly, the Detection System must choose the ideal response option according to the kind of network attack. This research study offers a comprehensive close examination of both IDSs and Intrusion Response Systems (IRSs) based on thorough interpretation of the response options available for various network attack types. Understanding of the path of data transfer from IDS to IRS can help network administrators/ staffs to get an idea of how to deal with various types of network attacks using the latest technologies. A Feature Selection (FS) algorithm is then implemented to make the most significant features recognition and controllable data dimensionality reduction. Finally, several monitoring techniques are assessed to declare whether the network traffic is harmful, to assign it under familiar malware "families" and to recognize new risks. A relative empirical study based on real-time network traffic from different environments shows that the system under study operates more efficiently when compared to the already existing latest rule-based IDSs like Snort and Suricata. In specific, sequential assessments of various monitoring techniques reveal that several unfamiliar malware events could be identified at least a month before introducing the static rules to the open-source rules-based Snort or Suricata IDs [7].

Modi et al. [8] reveals various network intrusions that has an impact on accessibility, privacy and data integrity of cloud resources and cloud computing services. Some of the prevailing proposals such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) available for cloud networking are discussed. Several commercial cloud networking service provider have developed already, and each company offers distinct cloud framework and infrastructure, Application Programming Interfaces (APIs) and Application Description document formats to acquire the network cloud resources and assist for Service Level Agreements (SLAs) which are commitment between the cloud networking companies and the clients or end users. As a consequence, vendor/ proprietary/ customer lock-in has earnestly limited the pliability of clients, who would prefer to distribute applications over several infrastructures in various positions on the earth, or to move a cloud service from one company to another. Different kinds of attacks ranging from network level attacks like DDoS (Distributed denial of service) attacks to application-level attacks like SQL (Structured Query Language) injection are analyzed. The commonly identified types of attacks ranging from network to application levels include Brute-force, DNS reflection, ICMP flood, Malicious Web activity (TDS), Port scan, SQL injection, Spam, TCP SYN flood, and UDP flood. Cloud computing, an IT paradigm comprising private, public and hybrid models, features "pay-as-you-go" models, offers cost-effective and "pay-as-you-go" features. A set of cloud computing services can energetically duplicate virtual machines rapidly. That is, they can duplicate a gigabyte level server within a minute [9].

The importance of system security is becoming popular, and hence many network devices are designed with required protection features. Network Intrusion Detection Systems (NIDS) are the frequently used protection systems [5]. Since new more dreadful risks are possible beside the commonly known network attacks, several expert and active plans are needed. These infrastructure completes the allocated work of internet traffic node profiling, and then uses this profile to continuously monitor the system operation for detecting any threats. When the framework identifies any fault, threat or inconsistent variation in the network traffic properties or qualities, it makes some essential steps, such as, giving out an alarm or alert. In this work, many prevalent NIDS (Network Intrusion Detection System) frameworks used to detect and tackle network security hazards are discussed [10] [11].

Bro IDS, more effective network analysis framework different from that of the common IDS, is anomaly-based intrusion detection normally used in conjunction with free lightweight open-source intrusion detection and prevention system called Snort. Bro IDS and Snort

complement each other effectively. Bro is actually a domain-specific language (DSL) network analysis framework used in computer network applications using Bro IDS. The technology is highly powerful for traffic analysis, forensics, and associated applications. This policy engine, a network science platform that facilitates an organization to form, observe and execute rules regarding accessing of network resources and the organization's data, implements own language. Bro IDS includes the following essential components like Event Engine, libpcap library, and Policy Script Interpreter [12]. The system capture data from the network interfaces utilizing libpcap library. Libpcap captures all the network traffic and then filters out the unwanted elements. The filtered data packet is then transferred to the Event engine. OpenWIPS-ng is an open source and modular Wireless IPS (Intrusion Prevention System) with three parts that includes Sensors, Server and Interface. The OpenWIPS-ngsensor captures wireless traffic and transmits the captured data to the server. The server analyzes, detects and recognizes both common and hidden network attacks and intrusions [13], and reacts to or alerts an attack. The interface controls the server machine and displays information regarding the network attack. Latest studies have also suggested Pattern based IDS that mainly deals with the IDS configuration that will facilitate for intrusion/ threat detection based on an important network component. For example, Pattern based IDS implements the intrusion/ threat detection method based on protecting certain protocols. It includes three parts. OSSEC (Open Source HIDS Security) is an ascendible open source Host-based Intrusion Detection System (HIDS) that can run on many types of computer platforms. It stores only intrusion warning data and not all the traffic data [14], and hence minimizes the storage overhead. It has an efficient correlation and analysis engine that automatically performs both profile and signature based analysis of the sensed data. It performs combined log analysis, file integrity checking, Windows registry or policy monitoring, root-kit detection, centralized network policy enforcement, active response, and time-based warning. OSSEC can detect Denial-of-Service (DOS) attack which results in shutting down of the network. The OSSEC has the following benefits: It is simple and uncomplicated to install or establish, and easy to customize. It supports multi-platform, and hence runs on different platforms of computer systems.

Snort is free, lightweight and open-source network intrusion detection and prevention system (NIDPS) software invented by Martin Roesch in the year in 1998[15]. Snort acts in three modes as follows: Packet sniffer, Packet logger, and Network intrusion detection and prevention system [NIDS, NIPS]. During the Packet sniffer mode, Snort software will study the network data packets and exhibit them on the monitor screen. During the Packet logger mode, it will perform packet logging. During the Network intrusion detection and prevention system mode, the Snort software will perform real-time network traffic monitoring and analysis. It will perform network traffic analysis based on user-defined set of rules. Snort, categorized under network IDS, has been invented for Linux and Windows based computer systems to identify emerging network attacks or threats. SNORT has the potentiality to perform existing real-time traffic analysis and packet logging functions on Internet Protocol (IP) communication networks.

The standard intrusion detection system (IDS) is not versatile in providing secure cloud computing because of the distributed cloud computing structure. This paper focuses on the intrusion detection and prevention procedures and techniques in Host as well as system Based Intrusion Detection system [17][18][19]. It explains about DDoS (Distributed Denial of Service) attacks in Cloud computing. Uncommon Intrusion Detection methods like anomaly based and signature based intrusion detection techniques described. It further researches about uncommon methods of intrusion Prevention system. Intrusion Detection Systems (IDS) have been widely utilized to detect adverse operations in communication systems and hosts. It is explained as a PC system to collect data based on many important points, and analyze the data to detect any disturbance in the system security arrangement or any signs of attack [16].

Intrusion Detection is the method of identifying undesirable traffic or access on a network. It acts as the important concept in the entire network as well as computer security design. Intrusion Detection System (IDS) is software/ physical device installed to observe network resources and traffic and detect undesired actions like unauthorized and destructive traffic, network resource abuse, etc. Deep Packet Inspection (DPI) is broadly implemented in IDS [20]. DPI examines all the information in the packet and utilizes regular expression matching. The complicated string patterns like attack signatures are represented as regular or definite expression. In this paper, the following things related to IDS and DPI are discussed: IDS basics, IDS components, IDS types, Different types of network attacks, Packet inspection levels, implementation of DPI, Different techniques of DPI, Characteristics of regular expression and the operating procedure of regular expression with respect to DPI. Hence, the IDS using DPI for regular expression matching extensively increases the intrusion detection speed and aids for satisfactory network performance [21].

Finsterbush et al. [22] concentrated primarily on protocol decoding technique to distinguish traffic classification. It is actually a lightweight pattern matching which identifies protocols based on the protocol header features like magic numbers and session identifiers, and the protocol behavior. Omprakash Chandrakar, et. Al. [23] explains about the basic abstract idea of network

intrusion detection system, as well as the components and classifications of network attacks. The IDS comprises three different types of components which includes the data source, the analysis engine, and the response manager. This paper summarizes genetic algorithm. In genetic algorithm, the input (chromosome) is chosen randomly and the fitness value is computed for each chromosome using iteration method. The iteration method includes different operations such as sorting process, selection process, crossover process, mutation process and then fitness value calculation.

R. Jakhale, et. Al [24] gives paper which explains an anomaly detection system and two stages of the detection system. The two stages include the training and testing phases. The clustering and sliding window is employed in observing the network traffic by extracting the frequent patterns utilizing certain algorithms. The frequent multi-pattern capturing algorithms are very efficient, applicable for real time monitoring, and has outrageous detection rate. Finally, the detection rate and false alarm rate percentages are determined. The paper described by R. Venkatesan, et al., [25] also explains an anomaly detection system which monitors the network traffic using sliding window and clustering techniques using frequent multi-pattern capturing algorithm. Here also, the algorithm proved highly effective with excellent detection rate. The detection rate and false alarm rate percentages are also determined. In the paper given by Abhilasha Sayar, et.al.,[26], the authors speaks about the classification, merits and demerits, and kinds of intrusion detection system. In this paper, the IDS implements neural network, artificial intelligence and fuzzy logic methods to identify or detect the intrusions in image data.

## III. PROPOSED SYSTEM

### *A. Overview*

Especially the server side security issues are an important aspects in network security. Every kind of computer network security is an essential component. In the current technologies computer networks and systems are more fundamental and concerns more on network security. In present days the significant issue is securing the data on the file server is the major concern. Several organizations hold various kinds of sensitive data and those are used to develop the market competitive products. These days intruder tries different kinds of hacking methods resides in the file server in many targeted organization to fetch the data of their significance. Intrusion Detection System (IDS) is a security system act as a secure layer for the communications and also monitor the network and find if any harmful operations are experience. So the present research works largely paying attention on providing the security into the server. The proposed systems have two validation techniques. First one is IP address validation and second one is voice recognition [27]. IP address verification is a normal validation that is mainly based on key generation in the networks. Voice reorganization is an authenticated validation that is mainly based testing the user voice. Figure1 shows the overall proposed system architecture.

### *B. Intrusion Detection System*

Intrusion Detection system monitors the flow of regular network traffic for suspicious activity and alert the issues immediately when such an activity is discovered. To monitor the malicious events and to identify the malicious activities in operating system or network IDS is appropriate. To identify the probable incidents, monitoring information about intruders, tries to stop them, and reporting them to security administrators IDS is apt. In addition, the IDS is classifying the troubles in the security policies and prevent individuals from violating security policies. The proposed advanced honeypot based intrusion detection system techniques examine the two validation n techniques below as: IP Address verification and Voice Recognition

### *C. IP Validation*

An Internet Protocol address is a logical address that is uniquely used to identify each and every system has own IP address in the network. To identify a valid entity on the network, majority of operating systems and networks are using each computer's IP address. Usually user first registers their details similar to user name, password and mobile number. After that the user login into that network system then it will generate the individual IP address for every user.

### *D. Key Generation*

A key generator (keygen) is a cryptographic tool that generates the validate keys for every users that validate key is accurate then only user allowed to enter into the respective network system. To provide security environment that validate the entered user is vulnerable to unauthorized disclosure or hidden change during transmission or while in storage using this key generation.

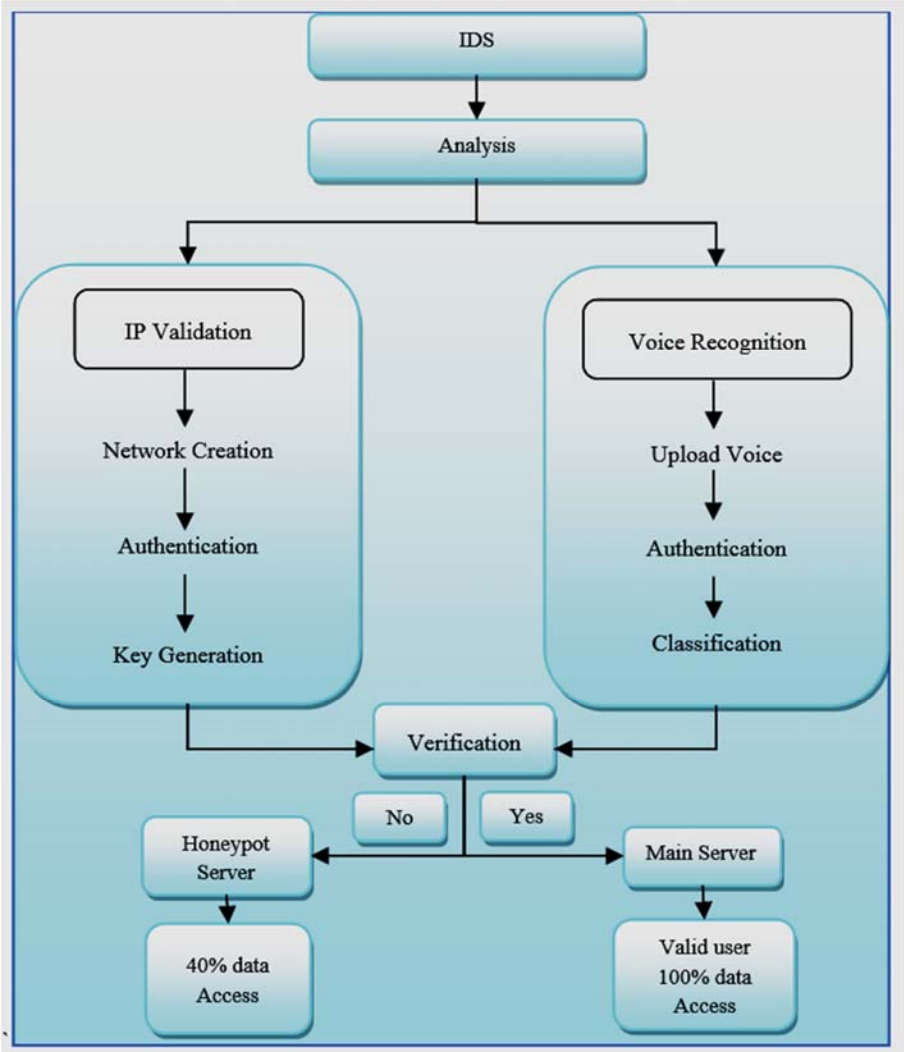


Figure 1. System Architecture.

*E. Voice Authentication*

Voice authentication is the technique of determining whether the user voice is authorized voice or unauthorized voice. Authorization is the method of providing permission to user to access or to process something. Usually, the new user speak about the own voice and the user voice slag is uploaded into the network system.

*F. Classification*

Voice classification is a significant to identifying vocal identity. Normally, the user already had given a voice through by segregation process. During the segregation moment, the voice process is transformed into threshold value and then the threshold value is stored in our database for security process. When the user tries to login into the system, the voice authenticated process checked by threshold values. If the threshold value is matched that particular user is authorized, if unmatched that particular user is an unauthorized users.

*G. Verification*

Verification testing is a technique of is used to examining and providing the support that the design output meets the desired input specifications. An essential process during validate the present user is approved user or unapproved user. IDS process verifies the process of the IP address verification and voice reorganization.

*H. Main Server*

The Main server processes the request and reply messages are used in the security system and also provide the functionality for the more complex operations. The

client details are not stored in the back-end server. Instead assigning permissions to each accessed objects or queries. Then comparing the assigned permissions to the client to test whether the client can legally access the desired information or not. The masquerading router is the connection between the client and the back-end server is kept confidential, so that the back-end server is more protected from corruption by the malicious user. The network traffic generating from clients and authentication server monitor the traffic generated from the attackers. Honey-pot is the process of forwarding requests that detect traffic as an attack on the server directed to an alternative server. But the attacker has no knowledge about the present honey-pot (i.e.) the hacker who will be unaware that they are not using a "real" server. After the authentication process is completed or not.

*I. Honeypot Server*

Honeypot is the process to implement fake services like real server to enhance the better security to server data. Honeypot is a intermediate fake server that provide emulated services similar to the real services running on the actual server side. So whenever attacker tries to attack actual server, attacker is redirected towards the fake server that is honeypot and eventually gets trapped in the honeypot. Honeypot offer the valuable information regarding the intruders. This information can be used to block the attacker and it can be used to take the legal actions against them. In this process, once the IP address verification and voice authentication process is mismatched then the honey pot server provides present user is only fewer and restricted portion of data will be accessed. Therefore, detecting the customer is unauthorized users.

*J. Advantages*

Lower entry cost.
Easier to deploy.
Near real time detection and response.
Does not require additional hardware.
Detect network based attacks.
Retaining evidence.
Real Time detection and quick response.

## IV. RESULT AND DISCUSSION

Three main performance metrics were used in this experiment to estimate our proposed methods False Alarm Rate (FAR). To count the amount of benign traffic detected as malicious traffic. (Detection Rate (DR)). The proportion of detected attacks among all attack data.(c)Accuracy (ACC). The study provides contributions through a new set of techniques using 2-stage detection which aims to improve the outlier detection rate and minimize the false alarm rate in IDS environments:

$$\text{False alarm Rate (FAR)} = \frac{(FP)}{(FP)+(TN)}, \quad (1)$$

$$\text{Detecting Rate (DR)} = \frac{(TP)}{(TP)+(FN)}, \quad (2)$$

$$\text{Accuracy (ACC)} = \frac{(TP)+(TN)}{(TP)+\{TN)+(FP)+(FN)} \quad (3)$$

TABLE 1: COMPARISON OF IDS

| Algorithms | Model built (sec.) | Detection time (sec.) | False alarm rate (%) | Detection rate (%) | Accuracy (%) |
|---|---|---|---|---|---|
| Naïve Bayes (NB) | 0.53 | 0.42 | 0.15 | 85.06 | 98.18 |
| Support Vector Machine (SVM) | 158 | 142 | 0.22 | 82.78 | 97.86 |
| Multilayer Perceptron (MLP) | 135 | 1.2 | 0.083 | 89.29 | 98.72 |
| Decision Table (DT) | 0.85 | 0.61 | 0.15 | 33.85 | 92.39 |
| Decision Tree (J48) | 0.97 | 0.67 | 0.05 | 85.84 | 98.35 |
| Random Forest (RF) | 1.6 | 1.13 | 0.17 | 87.1 | 98.39 |
| Adaboost + Random Forest (RF) | 3.41 | 1.83 | 0.13 | 88.85 | 98.62 |
| Unified Intrusion Anomaly Detection (2017) | 4.23 | 2.21 | 0.13 | 95.84 | 99.41 |
| Advance honeypot based IDS | 5.2 | 2.1 | 0.34 | 92 | 97.45 |

Table 1, display a comparison of performance metrics between our proposed approach and seven other data mining algorithms previously used by researchers in IDSs, including Naïve Baye's , Support Vector Machine, Multilayer Perception, Decision Table, Decision Tree, Random Forest, Adaboost Unified Intrusion Anomaly Detection (2017),Advance honeypot based IDS. To choose a better combination for the Advance honeypot based IDS classifier from a set of single classifiers in terms of accuracy, detection rates, and false alarm rates, Detection time, Model built classifiers are evaluated individually as illustrated.

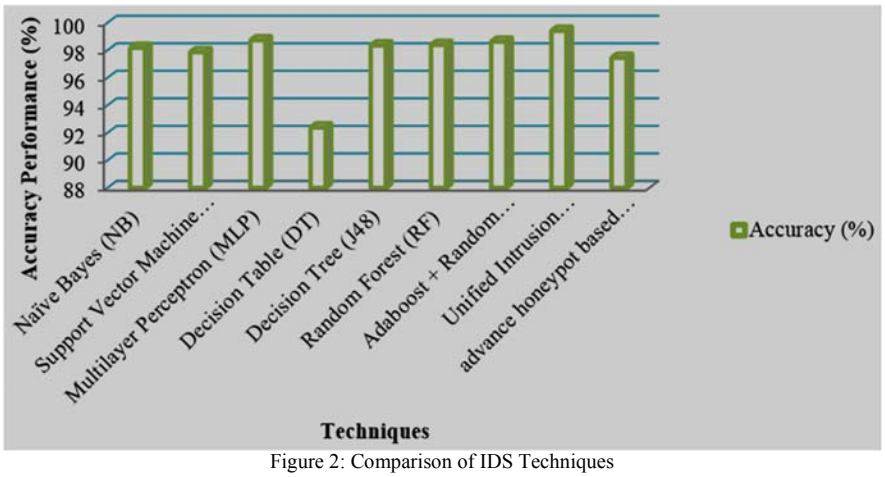


Figure 2: Comparison of IDS Techniques

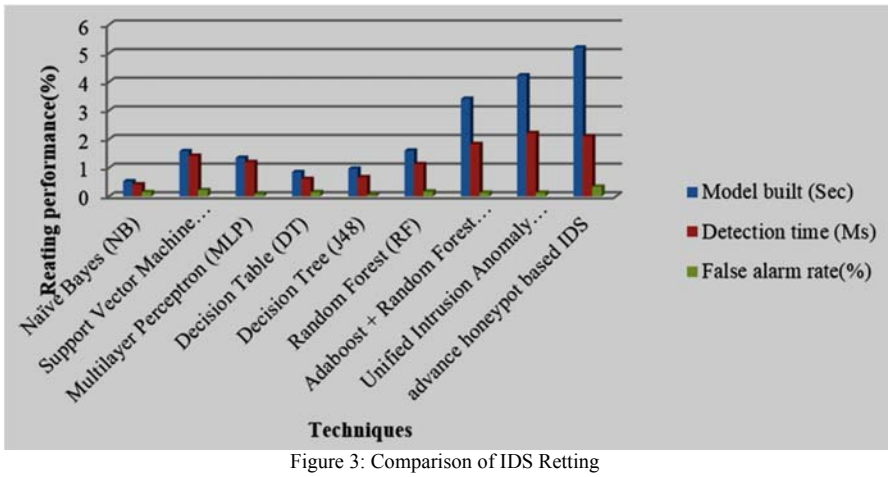


Figure 3: Comparison of IDS Retting

Figure 2 and 3 shows the comparative performance of Intrusion detection system by using techniques of Naïve Bayes , Support Vector Machine, Multilayer Perceptron, Decision Table, Decision Tree, Random Forest, Adaboost Unified Intrusion Anomaly Detection (2017) and Advance honeypot based IDS based on the attributes of Model built, Detection time and False alarm rate. The evaluated results show the better output for Advance honeypot based IDS than existing techniques.

## V. CONCLUSION

We introduced an advanced honeypot based IDS that provides comparable detection accuracy rate with a low failure notification rate, this is the majority crucial property of IDSs in practice. The major challenge is to achieve a low failure notification rate with high attack recognition capabilities for hidden attacks. In this paper we presented a novel advanced honeypot based Intrusion Detection System (IDS) and demonstrated its success through experimental results. The experiments synthesize both statistical and Network security approaches to achieve better and enhanced results to ensure various security methods.

## REFERENCES

[1] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, 2013. View at Publisher · View at Google Scholar.

[2] S. V. Thakare and D. V. Gore, "Comparative study of CIA and revised-CIA algorithm," in Proceedings of the 2014 4th International Conference on Communication Systems and Network Technologies, CSNT 2014, pp. 713–718, April 2014.

[3] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, "Intrusion detection based on K-means clustering and OneR classification," in Proceedings of the 2011 7th International Conference on Information Assurance and Security, IAS 2011, pp. 192–197, December 2011. View at Publisher · View at Google Scholar · View at Scopus

[4] C.-M. Ou, "Host-based intrusion detection systems adapted from agent-based artificial immune systems," Neurocomputing, vol. 88, pp. 78–86, 2012. View at Publisher · View at Google Scholar · View at Scopus

[5] K. L. I. Iii, "Anomaly Detection for HTTP Intrusion Detection," in Algorithm Comparisons and the Effect of Generalization on Accuracy, p. 196, Anomaly Detection for HTTP Intrusion

Detection, Algorithm Comparisons and the Effect of Generalization on Accuracy, 2007. View at Google Scholar

[6] Shahid Anwar, Jasni Mohamad Zain , Mohamad FadliZolkipli, Zakira Inayat, Suleman Khan , Bokolo Anthony and Victor Chang ," From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions", www.mdpi.com/journal/algorithms., Algorithms 2017, 10, 39; doi:10.3390/a10020039.

[7] Dmitri Bekerman, Bracha Shapira, LiorRokach, Ariel Bar," Unknown Malware Detection Using Network Traffic Classification", 2015 IEEE Conference on Communications and Network Security (CNS)

[8] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, and MuttukrishnanRajarajan. A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1):42–57, 2013.

[9] Chunyi Peng, Minkyong Kim, Zhe Zhang, and Hui Lei. Vdn: Virtual machine image distribution network for cloud data centers. In: Proceedings of INFOCOM, IEEE, Orlando, FL, USA, pp. 181–189, 2012.

[10] Shui Yu, Yonghong Tian, Song Guo &Dapeng Oliver Wu, "Can We Beat DDoS Attacks in Clouds?", in IEEE Transactions on Parallel and Distributed Systems, Vol: 25, Issue: 9, PP: 2245 – 2254, 2014.

[11] Ankit Punia, Vedang Ratan Vatsa," Current Trends and Approaches of Network Intrusion Detection System", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.6, June- 2017, pg. 266-270

[12] Zhiyuan Tan, ArunaJamdagni, Xiangjian He, Priyadarsi Nanda & Ren Ping Liu, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", in IEEE transactions on Parallel and Distributed Systems, Vol: 25, Issue: 2, PP: 447 – 456, 2014.

[13] Mehra, Pritika. A brief study and comparison of snort and bro open source network intrusion detection systems. International Journal of Advanced Research in Computer and Communication Engineering. 2012;1(6): 383-386.

[14] Open WIPS-ng. Available: http://www.openwipsng. org/. Last accessed 10th Sep 2015.

[15] OSSEC website, http://www.ossec.net/, 30 Oct 2013.

[16] Fu T. An Analysis of Packet Fragmentation Attacks vs. Snort Intrusion Detection System. International Journal of Computer Engineering Science (IJCES), May 2012.

[17] Ragupathi et al., "Brief Survey of Intrusion Detection and Prevention Systems in Cloud Computing Environment "International Journal of Advanced Research in Computer Science and Software Engineering 7(3), March- 2017, pp. 326-332

[18] Daniel Sun, Min Fu, Liming Zhu, Guoqiang Li &Qinghua Lu, "Non-Intrusive Anomaly Detection With Streaming Performance Metrics and Logs for DevOps in Public Clouds: A Case Study in AWS", in IEEE transactions on Emerging Topics in Computing, Vol: 4, Issue: 2, PP: 278 – 289, 2016.

[19] Ajay Kumara M. A &Jaidhar C. D, "Hypervisor and virtual machine dependent Intrusion Detection and Prevention System for virtualized cloud environment", in 1st International Conference on Telematics and Future Generation Networks (TAFGEN), PP: 28 – 33, 2014.

[20] Zhiyuan Tan, Upasana T. Nagar, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu, Song Wang &Jiankun Hu, "Enhancing Big Data Security with Collaborative Intrusion Detection", in IEEE transaction on Cloud Computing, Vol: 1, Issue: 3, PP: 27 – 33, 2014.

[21] S.Prithi, S.Sumathi, C.Amuthavalli," A Survey on Intrusion Detection System using Deep Packet Inspection for Regular Expression Matching", International Journal of Electronics, Electrical and Computational System IJEECS ISSN 2348-117X Volume 6, Issue 1 January 2017

[22] Jayesh Surana et al," A Survey On Intrusion Detection System", International Journal of Engineering Development and Research (www.ijedr.org) 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939.

[23] M. Finsterbusch, C. Richter, E. Rocha, J.-A. Muller, and K. Hanssgen, "A survey of payload-based traffic classification approaches," IEEE Commun. Surveys Tuts. , vol. 16, no. 2, pp. 1135–1156, 2nd Quart. 2014.

[24] Omprakash Chandrakar, Rekha Singh, Dr. LalBihariBarik, "Application of Genetic Algorithm in Intrusion Detection System", International Institute for Science, Technology and Education, Vol. 4, No. 1, 2014, ISSN. 2224-5774.

[25] A.R. Jakhale, G.A. Patil, "Anomaly Detection System by Mining Frequent Pattern using Data Mining Algorithm from Network Flow", International Journal of Engineering Research and Technology, Vol. 3, No.1, January 2014, ISSN. 2278-0181.

[26] R. Venkatesan, Dr. R. Ganesan, Dr. A. Arul Lawrence Selvakumar., "A Survey on Intrusion Detection using Data Mining Techniques", International Journal of Computers and Distributed Systems, Vol. 2, No. 1, December 2012, ISSN. 2278-5183.

[27] Abhilasha A Sayar, Sunil. N. Pawar, Vrushali Mane., "A Review of Intrusion Detection System in Computer Network", International Journal of Computer Science and Mobile Computing, Vol. 3, No. 2, February 2014, pp. 700 - 703.

## BIOGRAPHY

K.Veena is a Research Scholar in Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai. She received her M.E.,(I.T) degree from Vinayaka Missions University, Salem, Tamilnadu in 2007 and B.E., degree from B.V.Bhoomraddi College of Engineering and Technology, Karnatak University, Karnataka. At present she is a full time Assistant Professor at Dhanalakshmi College of Engineering. Her main interest is in Security issues regarding the safety of women.

Dr K. Meena received her Ph.D Degree in Computer Science and Engineering Department from Manonmaniam Sundaranar University, India in the year 2014. She received the B.E. (Electronics and Communication Engineering) and M.E. (Computer Science and Engineering) Degrees from Manonmaniam Sundaranar University in 2002 and 2009. She is working as Associate Professor in Computer Science & Engineering Department, Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai. Her research interests include Machine Learning, Pattern Recognition, Image Processing, Biometrics and Cyber security. She has published 30 papers in international journals, 7 papers in international conferences and 11 papers in national conferences.