iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

A Feasible Study for Virtual Intrusion Detection System (VIDS) using VMware and SNORT IDS

Preeti Gupta[1], Aditya Priyadarshi Sudhansu[2], Harsh Rastogi[3]
[1, 2, 3]*Department of Computer Science and Engineering, Inderprastha Engineering College, Ghaziabad, Uttar Pradesh, India*

Abstract: ***Nowadays, the majorly signature based Intrusion Detection System(IDS) are used to detect intrusions in their intranet. We have used the concept of virtualization to develop an Intrusion Detection System which will use Honeypots/Honey Clients to detect and trap the attackers. With the increasing popularity of cloud networks, serious issues around security for ubiquitous hosts will need to be addressed. In this project we focus on a virtual intrusion detection system (V-IDS). We present an architecture that uses basic principles of computer networking, virtualization, and Cyber security and apply them to intrusion detection systems, in order to protect networks characterized by a constantly changing underlying infrastructure and physical topology. Our goal is to define a process and a novel architecture that minimizes the security risk in networks, implementing the principle that network security and reliability is not a "product," but a well-defined "process." On the basis of the defined architecture we have implemented a prototype Virtual IDS.***

Keywords: Virtualization, Intrusion detection system, cloud networks, honeypots

I. INTRODUCTION

The use of the internet has increased considerably in the last few years, and so there has been an increase in the number of cyber-crimes ranging from data theft to identity theft. Many Intrusion Detection Systems have been designed in the past which were - Host Intrusion Detection System (HIDS), Network Intrusion Detection System (NIDS), Port Intrusion Detection System (PIDS). The latest addition to this has been the Virtual Intrusion Detection System (VIDS) which is still under development phase.

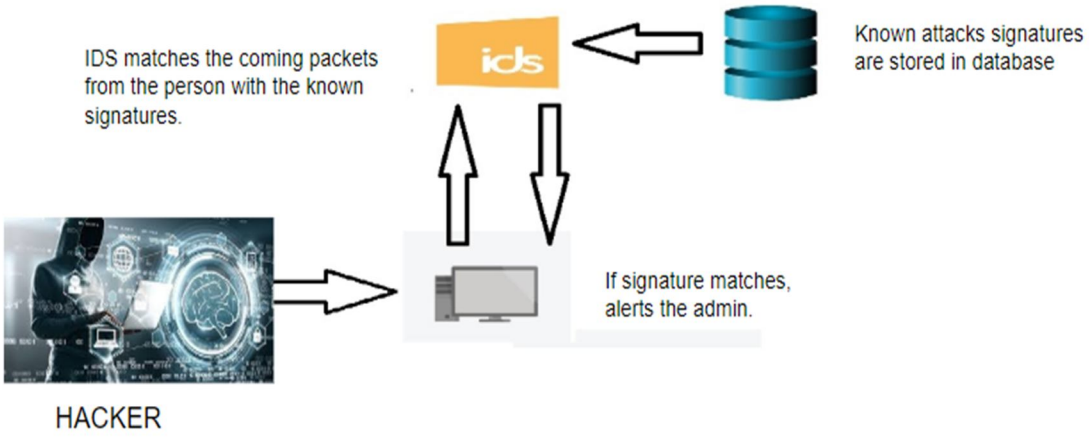


Fig1.1: Basic IDS architecture

Figure 1.1 shows basic IDS architecture which is incorporated in traditional systems. It shows a set of actions taken once an attacker or hacker tries to gain unauthorised access to the network. As soon as an attempt for intrusion is made, IDS matches the pattern of the invasion with rules present in its database and if the signature of the attack matches with any previous pattern, the administrator is alerted at once.

An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Many IDS tools also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control.

Following are the functions of an Intrusion Detection System:

A. Monitoring and analyzing both user and system activities
B. Analyzing system configurations and vulnerabilities
C. Assessing system and file integrity
D. Ability to acknowledge the existence of patterns of typical attacks
E. Analysis of anomalous activity patterns
F. Tracking user policy violations

There were many limitations of a signature-based Intrusion Detection System because of which VIDS is preferred. It detects the strikes, only if it matches a pattern preloaded in the database to detect new attacks, it has to be updated. If the network is in traffic, the Signature based IDS can have a difficult time inspecting every single packet and forces it to be dropped.
Server Virtualization deals with consolidation of server-based applications running on different physical servers on a single host machine using a virtual machine (VM). Virtual Machines can run different operating systems and consider that they own and have complete control over hardware dedicated to them. In reality physical host hardware is shared by virtual machines running on host and this resource allocation and sharing is monitored and managed by another layer called Virtual Machine Monitor (VMM).
Figure 1.2 shows the structure of a virtual machine when deployed on a hardware for server virtualization[1]. The server virtualization is composed of hardware virtualization and operating system virtualization where physical servers provide the hardware required. The operating system deployed on top of a physical server serves the purpose of operating system virtualization and provides a method to access virtual machines. The datastore shown below uses a storage space to store all kinds of files which are used and functions in a similar way to that of physical storage devices. The only difference is that it is a virtual memory space created for virtual machines for storage and access. On the virtual disks, the configurations for virtual machines are done based on the requirements of the user. The thick configuration can be used when the user does not want the system to automatically manage resources allocated to it at run time. However, thin configuration allows the system to manage usage of resources based on the latest requirement of the system. VMWare is a level which acts as an interface between hardware and operating system to allow creation of virtual machines. It serves as software required for server virtualization and also used for accessing virtual machines. On top of this layer we have virtual machines which are used for accessing physical hardware on top of which entire architecture is built upon. Since multiple virtual machines are created, utilization and efficiency of underlying hardware is evolved.

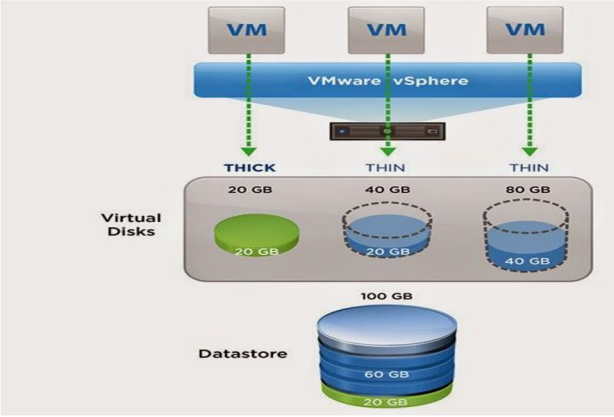


Fig1.2: Basic structure for a virtual machine (VMWare)

The suggested system of VIDS will use the concept of honeypots to detect intrusions and assert logs which can be further used by admin of the network to prepare for new invasions and methodology used by hackers. While honeypots have been around for some time, they are passive collectors, sitting on some random network on the Internet, waiting for a hacker to connect to and leave evidence. Typically, they consist of a Web server and a stripped-down operating system with tracking software that registers when a hacker tries to compromise the system. While they are great at documenting exploits, they have one of greatest demerits.
The primary objective is to reduce hardware usage by performing routing and switching virtually and maintaining a network with minimal usage of hardware. At the same time security of the network should be developed using honeypots and IDS which will keep track of all suspicious activities in the network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

II. LITERATURE REVIEW

A feasible approach to intrusion detection in virtual network layer of Cloud Computing by Chirag Modi et al [2] discusses the security issues in cloud computing and how they can be addressed using creation of virtual machines. Deploying IDS on each host machine allows monitoring the host machine's activity, underlying hypervisor's activity and anything travelling between the VMs on that hypervisor.

This helps monitor virtual networks (networks established within the host itself). However large amounts of data communication (between VMs) reduces performance of IDS and may cause packet dropping at IDS. Therefore, IDS should be fast, if it is deployed on a host machine to monitor multiple VMs. IDS can be deployed in a traditional network (external network of Cloud) that is an entry point of Cloud system.

This is how VMs allow detection of external attacks to Cloud[10-12]. It also narrates the various challenges of cloud IDS. In the virtual environment of Cloud, switch is virtualized (on each host system) to allow communication between VMs, and therefore, there is a need of monitoring network traffic that flows through virtual switches. In Cloud, VMs are dynamically added (or removed). In addition, security requirements for each VM may be different. Therefore, signature

database (or behaviour database) should be dynamic and relevant to each VM. As different attacks, their complexity and unpredictability increase in current network technology.

Julien Corsini [3], in this paper authors have used an anomaly detection based on multi model has offered intelligent detection algorithms. A novel multi model-based anomaly intrusion detection system with embedded intelligence and resilient coordination for the field control system in industrial process automation is designed. In this system, an anomaly detection based on a multi model has been suggested, and the corresponding intelligent detection algorithms are designed. Furthermore, to overcome issues of anomaly detection, a classifier based on an intelligent hidden Markov model, designed to differentiate the actual raids from faults.

In the paper Intrusion Detection System by Mohit Tiwari et al[4] describes the basic understanding of Intrusion Detection System, its needs in the contemporaneous era where a huge number of cyber attacks are recorded and observed on a regular basis. It explains phases of business on the internet and how it brings in outstanding potential to business in terms of reaching the users and at the same time it also brings a lot of risk to business.

There are both harmless and harmful users on the Internet. Whereas an organization makes its information system accessible to harmless Internet users.

Malicious users or hackers can also get access to the organization's internal systems for various reasons. It also mentions various types of intrusion detection systems which are popularly present in the market for use. The algorithms that are used in these IDS, methods of deployment, and pros and cons of those when used inside the network is properly expressed.

We have suggested a new system in order to reduce the drawbacks of the systems already present. Instead of using various data mining and warehousing techniques[7-9] and methods to teach the network about intrusions we shift to using a mechanism which can simply trap the hacker in a honeypot and gain significant information about him. This information or unique signature of the attacker can be shared with other workstations to alert them. The concept of virtualization allows us to easily access the server and create honeypots to lure attackers and store their signature. The IDS plays a significant role in detecting intrusions and is also used to update rules based on intrusion attempts on the network.

IDS should be trained to detect new attacks with assistance of previously observed events. This improves its detection capability with minimum false alerts. In addition, there is a need to maintain the performance and efficiency of the system.

III. IMPLEMENTATION

A. Based on requirements VMWare ESXi 6.5[5] is used for setting up the virtual environment for creating the Windows server. Accordingly Windows 7 virtual machines are created in order to access servers, and run the required applications.

B. The Windows virtual machines also serve the purpose of honeypots inside the network as decoys to trap attackers from gaining access to any sensitive information. The entire system requires an active internet connection to communicate with each other.

C. The Snort IDS is used as a third party application in Windows virtual machines to detect intrusions and thus enhance security. The internal routing and switching is provided by VMWare suite.

D. Also BASE is used as a graphic user interface for SNORT. The rules are added to the IDS using BASE so that intrusions are reported to users. The firewall for the individual systems needs to be configured to allow connections and filter out the traffic by enhancing the security of the overall system.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

IV. METHODOLOGY

A. *System Requirement For The Proposed System*

1) VMWare ESXi is a Virtual Machine Manager(VMM) for maintaining servers remotely. The host system on which the server is running must have a minimum of 8GB RAM to successfully allow functioning of the virtual machines. Here each virtual machine is allocated a minimum physical memory of 2 GB.

2) The Windows 7 64-bit Operating system is used for creation of virtual machines on VMWare Esxi and a minimum of 1 TB of hard disk storage is required to create and store virtual machines on the server. Thus , each virtual machine will have sufficient storage memory to store and execute files and applications. At Least 20 GB of hard disk space is allocated to each of the virtual machines.

3) The server must have a processor configured with at least- i3 octa core- sixth generation- 2.30 GHz processor. This makes it easy for applications such as SNORT IDS[6]- an Intrusion Detection Tool which is to be installed on each of systems to detect any and all malicious activities.

4) The basic computer hardware and peripherals such as mouse, keyboard and a monitor must be available at the data center where the server is placed. Also, sufficient power backups must be available to ensure continuous availability of data and security. Corresponding cooling systems must be present at the site in order to deal with overheating of the server and other networking devices. Also physical security of the data center should be assured so that sensitive information is always secured from human intervention or natural calamities.

B. *System Flow For The Proposed Work*

Since the start of communication in the network, data packets are flooded. This acts as the perfect opportunity for the attacker to get into the network and gain access to sensitive information and make use of it. This is where honeypots[21-27] come into play. The honeypots are systems which can be easily compromised and can be used to trick an attacker into believing that he has gained access to the actual system. The below mentioned Figure 1.3 outlines the steps taken by the new system to respond when an intrusion[13-20] is detected. As soon as the invader gains access to the honeypot, the IDS installed in the system gets activated and sends alerts to other systems present in the network to defend against any attacks in future by the same intruder. The signature of the infiltrator is shared with the rest of the network as soon as incursion takes place.

In case the trespasser tries to gain access to the system with actual information (system which is not a honeypot), IDS installed can be used to identify an attack and take necessary actions as required by the user. The trespasser can simply be shut away from accessing the network or the administrator can monitor activities of the attacker to gain more information about them to take action. The 50 % possibility is dependent on the degree to which the patterns are matched in the database. It is the criteria that decides whether the administrator needs to be alerted or not. Also, time taken by IDS to alert the other systems in the network gets reduced as the entire network is virtualized along with the individual systems.

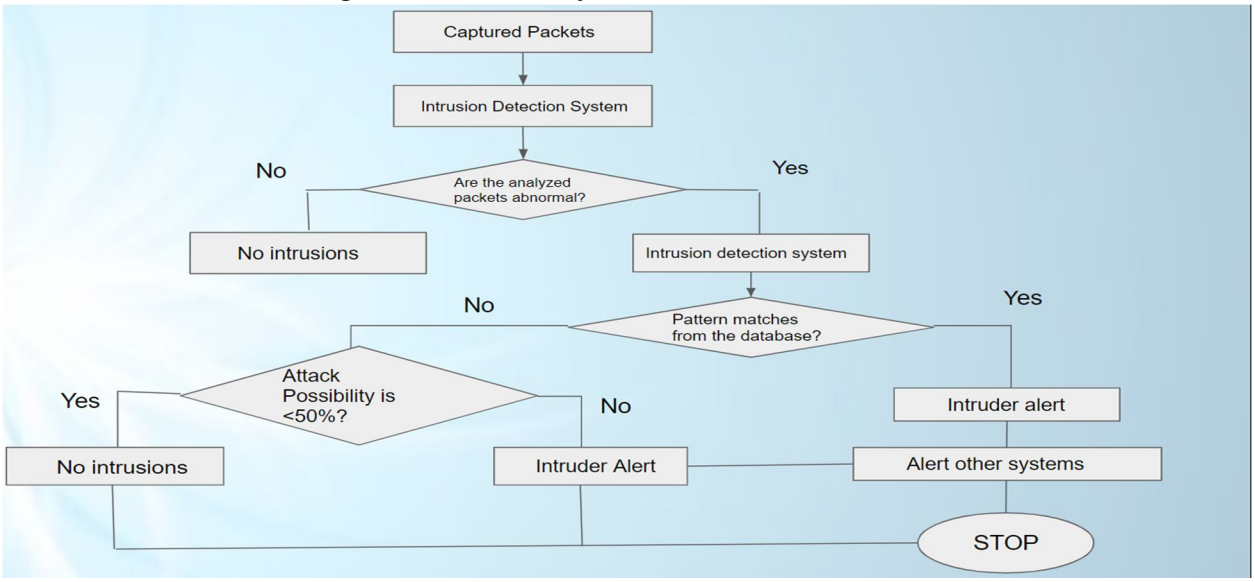


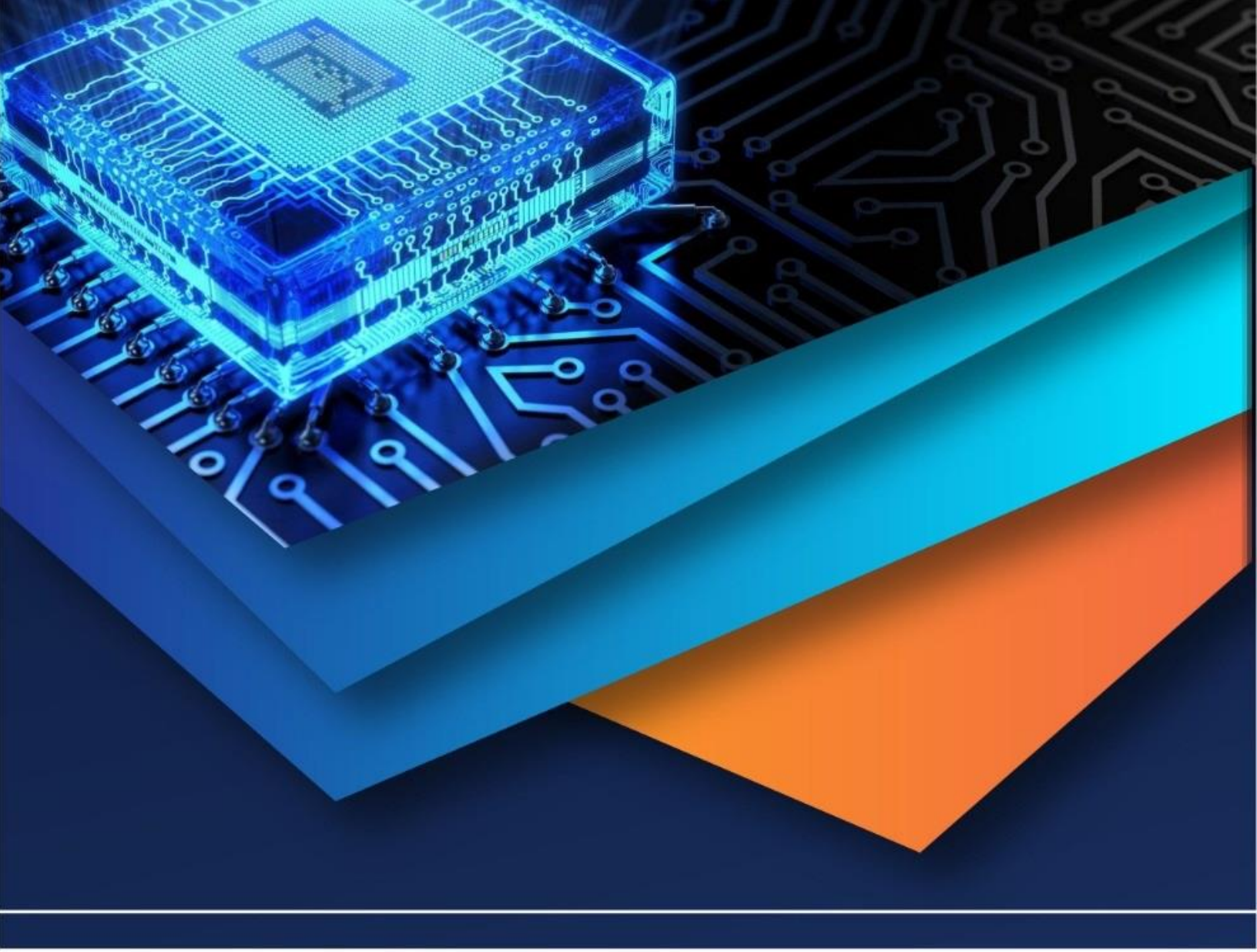
Fig 1.3 Flow diagram for proposed system

V. CONCLUSIONS

Earlier latest hardware and software were developed that improved security however increased the overall cost as well. The maintenance of these devices is expensive and upgrades of software and hardware needs to be done on a uniform basis to assert quality of the entire system. Now, new software/hardware are not required because of the suggested system. Maximum efficiency can be achieved with the available resources as compared to current systems. After the implementation of our proffered model in future we can say that it will enhance security of the extant systems and it will also aid to create more secure systems at the industry level. It will also facilitate the intelligence agencies to create one more layer of protection against cyber attacks on their networks. In the offered system we have reduced hardware cost by simply shifting all work to the virtual environment using the concept of virtual machines and reduction in hardware also leads to the reduction in physical space required. Even the electronic waste generated by industries is reduced leading to positive environmental contribution. Furthermore, the propound system is open to all possible techniques which can be used to further improve the performance and competency of the network. Evolution of the network can be achieved by various methods including mechanisms to detect the physical location of strike, and catch the intruder red handed. This can prevent any future strikes by the hacker. Patches corresponding to exploited vulnerability can be installed frequently by detecting the incursion patterns using reverse engineering. The installation of patches can be monitored by the administrator to ensure authenticity of updates.

REFERENCES

[1] VMWare ESXi 6.5 Networking, Copyright © 2009–2017 VMware Inc., https://www.vmware.com/
[2] Chirag Modi and Dhiren Patel, “A feasible approach to intrusion detection in virtual network layer of Cloud Computing”, 22nd June 2018, https://doi.org/10.1007/s12046-018-0910-2
[3] Julien Corsini, Analysis and evaluation of network intrusion detection methods to uncover data theft, M.S. thesis, School of Computing, 2009.
[4] International Journal of Technical Research and Applications 5(2):2320-8163 · April 2017
[5] VMware Infrastructure Architecture Overview [White Paper], https://www.vmware.com/
[6] Snort 2014 Snort-home page. Snort Tool, https://www.snort.org/
[7] Modi C N, Patel D R, Patel A and Rajarajan M 2012 Bayesian classifier and Snort based network intrusion detection system in cloud computing. In: Proceedings of the 2012 Third International Conference on Computing Communication Networking Technologies (ICCCNT), pp. 1–7
[8] Modi C N, Patel D R, Patel A and Rajarajan M 2012 Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing. In: Proceedings of the 2nd International Conference on Communication, Computing & Security [ICCCS-2012], pp. 905–912
[9] Kayacik N and Heywood M 2005 Selecting features for intrusion detection: a feature relevance analysis on KDD 99 intrusion detection datasets. In: Proceedings of the The 3rd Annual Conference on Privacy, Security and Trust (PST)
[10] Ram S 2012 Secure Cloud computing based on mutual intrusion detection system. International Journal of Computer Application 2(1): 57–67
[11] Modi C, Patel, D, Borisaniya B, Patel A and Muttukrishnan R 2012 A novel framework for intrusion detection in Cloud. In: Proceedings of the Fifth International Conference on Security of Information and Networks, pp. 67–74
[12] NVD 2009 Vulnerability summary for CVE-2009-1542. National Vulnerability Database, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1542.
[13] Popovic K and Hocenski Z 2010 Cloud computing security issues and challenges. In: Proceedings of the 33rd International Convention MIPRO, pp. 344–349
[14] Gens F 2008 IT Cloud services user survey, pt.2: top benefits and challenges. International Data Corporation, http://blogs.idc.com/ie/?p=210
[15] Idrees F, Rajarajan M and Memon A Y 2013 Framework for distributed and self-healing hybrid intrusion detection and prevention system. In: Proceedings of the International Conference on ICT Convergence (ICTC), pp. 277–282
[16] Roschke S, Feng C and Meinel C 2009 An extensible and virtualization-compatible IDS management architecture. In: Proceedings of the Fifth International Conference on Information Assurance and Security, pp. 130–134
[17] Gupta S, Kumar P and Abraham A 2013, A profile based network intrusion detection and prevention system for securing Cloud environment. International Journal of Distributed Sensor Networks 9(3): 1–12
[18] Chan A P F, Ng W W Y, Yeung D S and Tsang E C C 2005 Comparison of different fusion approaches for network intrusion detection using ensemble of RBFNN. In: Proceedings of the 2005 International Conference on Machine Learning and Cybernetics, pp. 3846–3851
[19] Hubballi N, Biswas S and Nandi S 2013 Towards reducing false alarms in network intrusion detection systems with data summarization technique. Security and Communication Networks 6(3): 275–285.
[20] Lo C C, Huang C C and Ku J 2010 A cooperative intrusion detection system framework for Cloud computing networks. In: Proceedings of the 39th International Conference on Parallel Processing Workshops (ICPPW), pp. 280–284.
[21] Aaditya Jain, Dr. BalaBuksh, ”ADVANCE TRENDS IN NETWORK SECURITY WITH HONEYPOT AND ITS COMPARATIVE STUDY WITH OTHER TECHNIQUES”, M.tech(CS&E), Professor(CS&E) R.N. Modi Engineering College, Kota,Rajasthan,India, (IJETT) – Volume 29 - No. 26 (Nov 2015).
[22] DenizAkkaya – Fabien Thalgott, “HONEYPOTS IN NETWORK SECURITY”,Linnaeus University, 29th Feb 2010.
[23] Aye AyeThu, ” INTEGRATED INTRUSION DETECTION AND PREVENTION SYSTEM WITH HONEYPOT ON CLOUD COMPUTING ENVIRONMENT”,University of Computer Studies (Yangon), Myanmar, (IJCA)- Volume 67– No.4,(April 2013).
[24] Dacier Marc, Pouget Fabien and Debar EurecomHervé, ―Honeypots: Practical Means to Validate Malicious Fault Assumptions‖, In the proceedings of the 10th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC‘2004), February 2004
[25] Kreibich Christian and Crowcroft Jon, ―Honeycomb – Creating Intrusion Detection Signatures Using Honeypots‖, In the proceedings of the 2nd Workshop on Hot Topics in Networks (Hotnets II), Boston, November, 2003.
[26] Sink Michael, ―The Use of Honeypots and Packet Sniffers for Intrusion Detection‖, SANS Institute , As part of GIAC practical repository 2000 - 2002.
[27] Spitzner Lance, ―Honeypots, definitions and value of Honeypots‖ http://www.spitzner.net/Honeypots.html, May 2003.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY