

Intruder Detection System: -An innovative approach for Host Machines in cloud computing

Divya Mahajan,

Research Scholar, CS Department Bhagwant University, Ajmer, Email:
divyamahajan41@yahoo.com

Dr. Kalpana Sharma

Assistant Professor Department of Computer Science Bhagwant University, Ajmer
kalpanasharma56@gmail.com

Abstract— There may be very big position of Virtualization in cloud computing. “*Virtualization*” that refers to the process of making a “virtual version” of something like hardware or software- virtual servers, infrastructure, devices and computing resources. For example, creating a virtual machine that serves as a real-life computer.

The physical hardware in the cloud computing are living with the host machine and the virtualization software runs on it. The virtualization lets in digital machines to exist. The host device shares its bodily additives together with reminiscence, storage, and processor ultimately to handle the desires of the digital machines. If an attacker effectively compromises one VM, it is able to outbreak others at the equal host on the community over lengthy durations of time. Virtualized Intrusion Detection System is deal with the community get right of entry to visitors and guard the data and applications in cloud from malicious attack and vulnerabilities. IDS Model having characteristics of virtualization to offer higher safety in cloud surroundings. This is an step by step extra famous method for go-virtual-gadget assaults, on the grounds that site visitors among VMs cannot be tested through general IDS/IPS software program programs. As we recognize that the cloud environment is distributed in nature and subsequently extra at risk of various kinds of intrusion attacks which consist of installing malicious software program and generating backdoors. In a cloud environment, where groups have hosted essential and important statistics, the safety of underlying technologies turns into vital. To alleviate the chance to cloud environments, Intrusion Detection Systems (IDS) are a cowl of defense. In this paper, we are offering an innovative version for Intrusion Detection System for securing Host machines in cloud infrastructure. This very proposed IDS has two critical features: (1) signature based totally and (2) prompt alert gadget.

Keywords—Cloud computing, Virtual machine, Intruder detection system, IDS, attack, Host Machine, alerts, prevention, Signature, Anomaly.

I. INTRODUCTION

The demanding situations throughout covid-19 for every kind organizations either academic, marketing, enterprise industry, and so forth put a pressure to the IT & Telecommunication enterprise to provide the everyday IT services and to expand other modern verbal exchange and paintings platforms. Cloud computing is such an efficient computing environment that percentage each sort of computing assets in line with the requirement of clients on pay-per-use basis as a carrier either computing Infrastructure as a Service, computing Platform as a Service, Software as a Service, Security as a Service, and so forth. These all the offerings are accessed in the cloud computing from a Data Centre, each Data Centre might also have more than one Host Machines, and each host machine have a variety of computing sources in sufficient number. These resources are shared with more than one clients the usage of the virtualization techniques. Virtual Machine Monitor or Hypervisors are used on the Host Machines for coping with the consumer’s sources requirements and the real bodily resources.

The position of broking must be discussed right here because consumer put up their requirements through the broker and dealer provides the satisfactory answers by way of taking the information from the CIS [Cloud Information Server]. The dealer than submit the requirement to the Data Centre and resources are allocated by using the Host Machines to the patron. The customer get entry to those assets and execute its procedures using virtual Fmachines.

The Host Machine is the bodily hardware in cloud computing, wherein the client information resides, processed or done, saved, etc., and it really runs the virtualization software program that allow virtual machines to exist. Its physical components including reminiscence, garage, and processors in the end take care of the desires of the virtual machines.

Intruders are continually a trouble no longer most effective for the cloud computing based structures however in nearly all of the machine. These Intruders are both outsiders or valid customers of the device. But they've malicious intentions, they try to paintings out of doors their profile or function in the system and any how they need to get right of entry to the continuing tactics records or completed processes info. They provide such records to the attacker, or an attacker may use such intruders to get entry to the continued techniques statistics or completed initiatives information. So, that it is able to use such facts for their malicious purposes.

In case of cloud computing, the service providers or clients are the use of maximum of the computing sources by means of hiring them from the third birthday celebration. So, their information resides or strategies are done, at the third party cloud servers or statistics centers. So, the security of the continuing methods or data resides on the third party cloud servers ought to be secured from the intruders. This is the principle motivation for penning this paper.

II. IDS, ITS TYPES AND ROLES

There are a few security measures like firewalls taken via many networks for preventing the attacks. These security features are simplest powerful for outside attacks but are insufficient for inner attacks. The inner assaults are accomplished via the valid users or by way of the complicated external assaults e.G. DOS and DDoS. Such assaults cannot be tackled by using firewalls like mechanism but IDS systems will play an important role in these cases.

Intruder Detection System is the very much required at present for all type of computer networks. Its requirement is more in cloud computing because cloud computing provides an open architecture and shared computing resources environment. In cloud computing, Data Centers share its resources that are physically with the Host Machines to their clients. Clients access these resources using virtualization through virtual machines.

These intruders basically target Host Machines of the Data centers, because all the client's processes are executed concurrently on Host Machines and client's data will also be stored on the Host Machines. So, there is very much requirement of such an efficient intruder detection system that will identify and block such intruders before they enter in the Host Machines. If any how they enter in the Host Machine, they will not be allowed to do malfunction with the internal configuration of the network, its permissions to different client or processes, data, or other important files of the Host Machine.

Intruder Detection System are of two types: (i) Network Intruder Detection System [NIDS] and (ii) Host Intruder Detection System [HIDS].

NIDS helps to observe the network traffic and can also be deliberated as a packet sniffer. Principally, it observes each and every data packet of the network in depth to get if there are any nasty payloads. Another advantages of using NIDS are protocol analysis and content searching. It can detect multiple harmful attacks like port scans, buffer overflow, etc. It examines the network traffic or packets on the basis of provided set of rules and then send prompt alert message to the administration for any distrustful activity. As it work for securing the whole network, so it is divided into various components and these components work together to perceive the intrusion.

HIDS observe the system for detecting and reporting for any unapproved variations to the files and directories. Once a baseline is formed, it observes and detects the changes in the file system like file addition, file alteration, who has done these changes, and also records time stamps. If the changes are authentic, it can update the system's database to accept these changes.

The Intruder Detection System [IDS] or Intruder Detection & Prevention System [IDPS] layer is used as additional prevention layer of security used by the cloud Host Server. It will detect the many known as well as some unknown attacks and gives alerts to the administrator.

The intruder identification process is a strategic issue for an IDS and this process depends on two major things: (i) the service model, and (ii) Security mechanism. Here we are discussing the IDS implementation for the cloud computing and the cloud computing has three service models: (i) SaaS, (ii) PaaS, and (iii) IaaS.

The design of an Intruder Detection System should consider the factors like Malware Detection, Log Management, Change Detection, Security Configuration Assessment, Policy Management, Vulnerability Assessment, Asset Discovery, etc. as shown in figure 1.

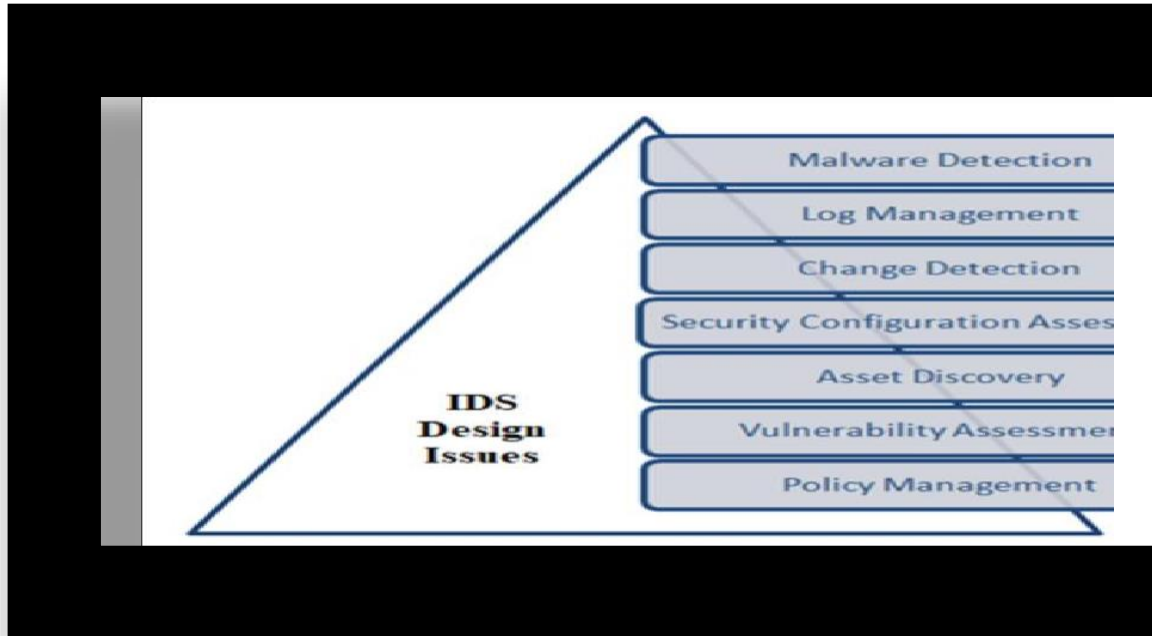
An efficient IDS works on more than one stages and the Log Management, Policy Management and Vulnerability Assessment or mapping at the Host Machine or on the cloud community are the primary goals. As on this paper, we're operating extra specifically for the HIDS. Log Management is an important trouble for the IDS device because Cloud Computing are utilized by more than one clients, and those clients produce big quantity of logs. So, the machine administrators must need to determine the order of those logs for analysis.

These logs of information are to be had at the Host Machine and the IDS will put together a database of all of the log documents. Besides this may it additionally put together a log of the transactions achieved on the Host Machine for destiny use and observe the customer's behaviour.

Malware Detection is any other vital factor for IDS. There are diverse malware detection processes that may be used to locate a malware. Signature-based totally and heuristic based totally detection techniques are the two main processes to malware detection. The outcomes show that these processes are correct for detecting regarded malware detection but those approaches can not stumble on the new and unknown malware attacks.

Network intrusion detection structures (NIDS) are placed at a strategic factor or points within the community to display visitors to and from all devices on the community. [8]It plays an evaluation of passing visitors on the whole subnet, and fits the traffic that is handed at the subnets to the library of regarded assaults. Once an assault is identified, or unusual behavior is sensed, the alert can be sent to the administrator. An instance of an NIDS could be putting in it at the subnet in which firewalls are placed on the way to see if a person is attempting to break into the firewall. Ideally one could experiment all inbound and outbound site visitors, but doing so might create a bottleneck that could impair the overall velocity of the network.

Figure 1: IDS Design Issues different malfunctioning purposes. Hence, there is very much need of an efficient and effective Intruder Detection



mixture analysis, artificial neural networks and integration of geographical information system and remote sensing data. Each change detection technique have its some merits and hence no single technique is ideal and appropriate to all cases. The change detection techniques are often compared to find the best results for a specific application.

Security Configuration Assessment (SCA) helps to expand your current vulnerability management program and automates configuration assessment and reporting of IT assets in a continuous way. SCA is an add-on option to VM to complete your vulnerability management program. SCA is very important for the implementation of an effective Intruder Detection System because all the VMs executes physically at the Host Machine.

A good IDS policy should be different and innovative and may integrate other policies as well, like firewalls, routers, and other related inputs. To create a new policy, one should analyze the available information and then determine the best strategies according to the standards, guidelines, procedures, and other basic rules.

III. PROPOSED INTRUDER DETECTION SYSTEM

As the cloud computing provides a distributed and open architecture to its users. Attackers are taking the advantage of its architecture and easily enter in the cloud network to target host machines for the available data or processes for

Another important IDS technique is the Change detection. System to protect the data and processes from such attacks. It will observe and identify the differences in the state of the objects or phenomenon. There are multiple change detection In the last one year, the growth in the online attacks on techniques are proposed like Image differencing, principal cloud networks and on the other online services is notice component analysis and postclassification comparison. As more. These are now more detrimental than before. In this attackers are continuously changing their attacking paper we are proposing an innovative intruder detection strategies, so for countering such attacking strategies some innovative technique are proposed for example spectral system HITS [Host based Intruder Tracing System] and the model is presented in the figure 2 below.

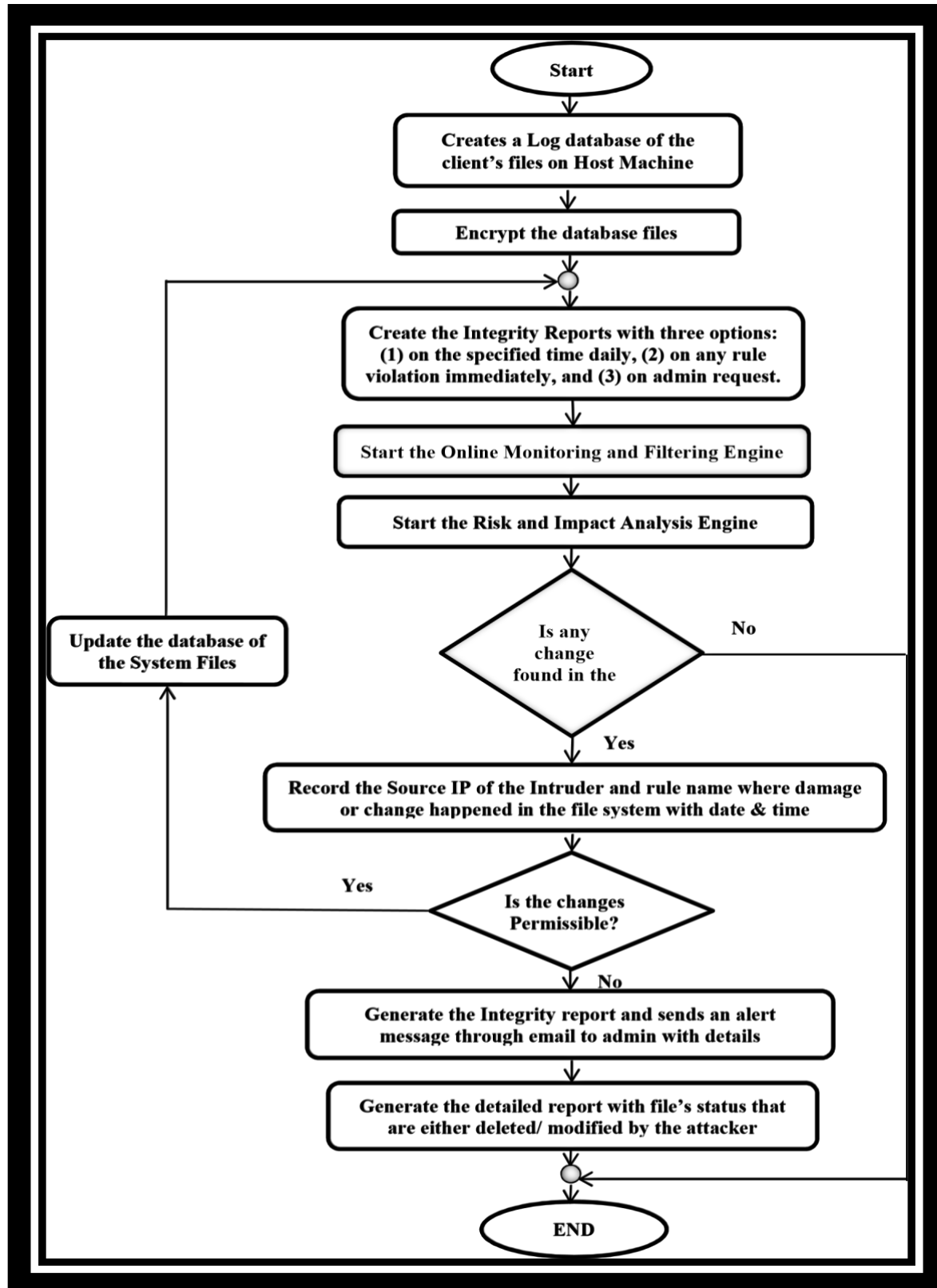


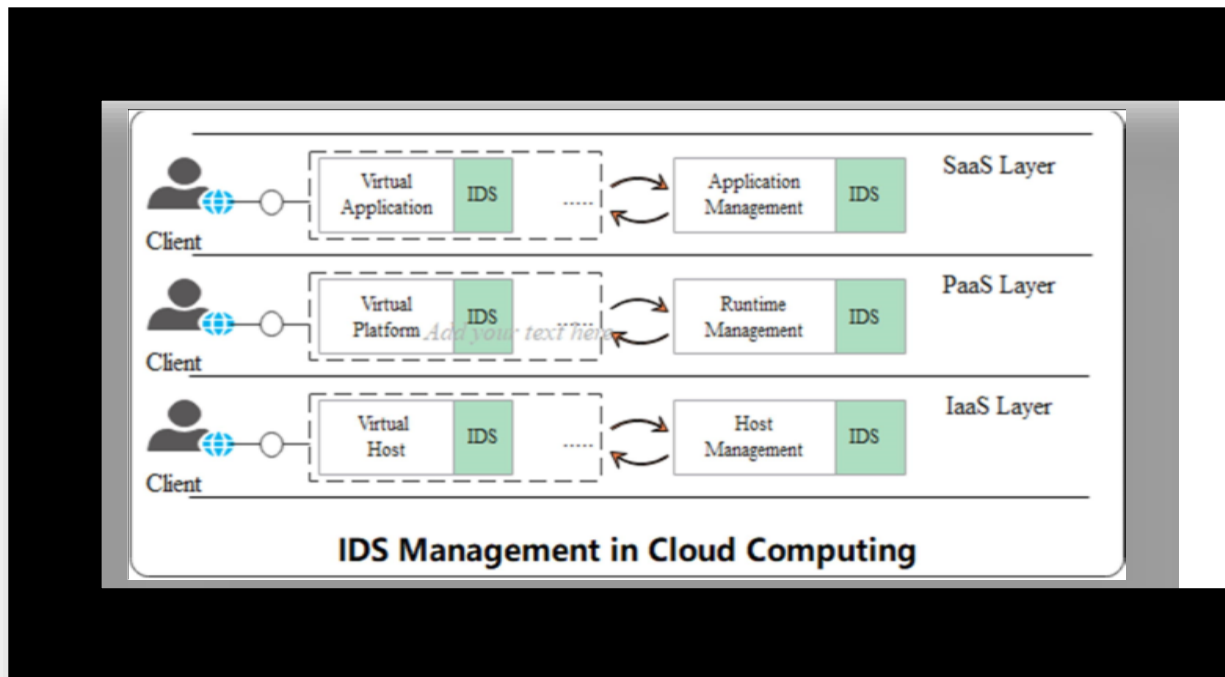
Figure 2: Proposed HITS Intruder Detection System

The proposed HITS system [Host based Intruder Tracing System] will be designed by keeping the requirements of Host based Intruder Detection System and it includes the important features like Log management, online monitoring and filtering system, Risk and Impact Analysis Engine, Encryption algorithm, and Prompt Alert System.

This system when started prepares a Log database of the existing files on the host machine and also prepares the logs of the data of executing virtual machines on the host machine. It will apply change detection techniques on this Log Database to monitor the status. It then applies encryption on the Host Machine's configuration and setup files including policy and other important files of the Host Machine.

The proposed HITS system will provide the option to generate integrity reports as per the requirement of the administrator, either as a daily report on the pre-specified time, on any violation of the pre-decided rule, or on the administrator's request.

This proposal also includes a very important feature i.e. Online Monitoring and Filtering Engine. This engine will



continuously monitor the activities done on the Host Machine either between the Host Machine and Virtual Machines, between Virtual Machine and client, and between Virtual Machines to Virtual Machines. This also filters the transactions and data found malicious or seems to be malicious activities. The engine also marks such VMs and nodes by keeping details like its IP address, time-stamps, and transaction history to identify the intruders. It is complex system and has to apply different strategies for such filtering.

Another important feature of this proposed HITS system is the Risk and Impact Analysis Engine. As we know that security is a strategic issue and there may be the accidents after keeping lot of security measures. The risk and impact analysis is very helpful for planning a foolproof strategy. This Risk and Impact Analysis Engine will keep the track of accidents and their impacts on the Host Machine, its other concurrent executing virtual machines, data, configuration files, level of damage, time taken to take the actions for controlling and restating the correct status.

With the passage of time the system will be more perfect and security strategies are analyzed and compared with other strategies. The administrator may choose the best according to the nature of the client, traffic, cases on their site. The Risk and Impact Analysis Engine will help in decision making and strategy development for future.

After starting the HITS system, Online Monitoring and Filtering Engine, and Risk and Impact Analysis Engine, it will continuously monitor the activities on the Host Machines. If there is no change found, the system will continue its working, but if some changes are noticed either in the configuration, access rights, or any other violation of rules, etc. the proposed system will record the source IP of the Intruder and entity detail where the change or damage is happened with time-stamps. It will also compare the level of damage using change management strategies and also report to the administrator with detailed report. After reporting these details it will ask the administrator either permit the changes if they are authentic and valid, or reject the changes. If the administrator permitted these changes, the HITS system will update the Log database and continue its work.

But if the administrator rejected the changes, it will do the Risk and Impact Analysis of the damage and generate a detailed report and send it to the administrator immediately through email to its registered email. The administrator will then takes the required action and manage the system in best possible way.

The implementation of multi-level IDS in Cloud Computing will monitor all the activities either between the client and its Virtual Machine, between VMs and other VMs, between VM and Host Machine. The scenario of MultiLayer IDS implementation in Cloud computing is shown in figure 3 below.

Figure 3: Multi-Layer IDS implementation in Cloud computing

As shown in the figure 3, when multi-level IDS is implemented in cloud computing, it will work across all the layers of the cloud i.e. Infrastructure as a Service Layer, Platform as a Service Layer, and Software as a Service Layer. As client access the resources of the cloud through Virtual Machines, so when client is hiring a Host Machine using virtualization at IaaS Layer, then the IDS will attached with it and monitor the activities between client and Virtual Host and on the cloud server side it will be attached with hypervisor to do the Host Management as shown above in figure 3 at IaaS layer.

At the PaaS Layer, the client access the platform through virtualization are called Virtual Platform as illustrated in the figure 3 and these multiple virtual platform are monitored and Managed by the Runtime Management tools and both Virtual Platforms and Runtime Management tool are secured by using the IDS as illustrated in the figure 3.

In the similar manner at the SaaS layer, client access various cloud based applications as Virtual Application and these Virtual Applications are managed by the Application Management tools. The activities between Client and

Applications and between Virtual Applications and Application Management tools are monitored and secured by the IDS as illustrated in the figure 3 at SaaS Layer.

IV. CONCLUSION

Cloud computing affords an smooth to access environment with lots of computing assets and supports improvements within the area of computing and communicate. A style of applications human beings are the use of that are primarily based on cloud computing. The achievement of cloud based applications endorsed the researcher and builders to do innovations in this area also. Security is one of the critical component from the starting of cloud computing and lot of studies has been for imparting secured computing and verbal exchange surroundings, but as attackers are regularly changing their attacking strategies. So, new studies is always required to cozy the gadget. The proposed HITS gadget have protected all the complexities of safety hole in cloud infrastructure and computing. The essential contributions of

HITS are software of encryption on Log database, Online Monitoring and Filtering Engine, Prompt Alert to the administrator, and Risk and Impact Analysis Engine. We wish that this model will offer a cozy surroundings in cloud computing and protect the important assets and information on the Host Machine.

REFERENCES

- [1] C.N. Modi, D.R. Patel, A. Patel and M. Rajarajan, "Integrating signature Apriori based network intrusion detection system (NIDS) in cloud computing," 2nd International Conference on Communication, Computing and Security, 2012, pp.905-912.
- [2] T. Alharkan and P. Martin, "IDSaaS: Intrusion Detection System as a Service in Public Clouds," Proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2012, pp. 686-687.
- [3] S.M. Manthira and M. Rajeswari, "Virtual Host based Intrusion Detection System for Cloud," International Journal of Engineering and Technology (IJET), vol. 5, 2014, pp. 5023-5029.
- [4] J.K. Khatri and G. Khilari, "Advancement in Virtualization Based Intrusion Detection System in Cloud Environment," International Journal of Science, Engineering and Technology Research (IJSETR), vol. 4, 2015, pp.1510-1514.
- [5] S. Gupta and P. Kumar, "Immediate System Call Sequence Based Approach for De-tecting Malicious Program Executions in Cloud Environment," Wireless Personal Communications, vol. 81, 2015, pp.405-425.
- [6] N. Pandeewari and G. Kumar, "Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN," Mobile Networks and Applications, 2015, pp.1-12.
- [7] B. Muthukumar B. and P.K. Rajendran, "Intelligent Intrusion Detection System for Private Cloud Environment," Communications in Computer and Information Science, vol. 536, 2015, pp.54-65.
- [8] C.N. Modi and D. Patel, "A novel Hybrid-Network Intrusion Detection System (H-NIDS) in Cloud Computing," IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2013, pp. 23-30.
- [9] P. Ghosh, A.K. Mandal and R. Kumar, "An Efficient Network Intrusion Detection System," Chapter Information Systems Design and Intelligent Applications, vol. 339 of the series Advances in Intelligent Systems and Computing, 2015, pp 91-99
- [10] .
- [11] C. Ambikavathi and S.K. Srivatsa, "Improving virtual machine security through intel-ligent intrusion detection system," Indian Journal of Computer Science and Engineering (IJCSE), vol. 6, 2015, pp.39.
- [12] S. Roschke, F. Cheng, and C. Meinel, "An extensible and virtualization-compatible ids management architecture," vol. 2, pp. 130-134, 2009
- [13] 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 Applica-tions, vol. 36, no. 1, pp. 42-57, 2013.
- [14] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a network id into an open source cloud computing environment," pp. 265- 270, 2010.
- [15] A. K. Jones and R. S. Sielken, "Computer system intrusion detection: A survey," Computer Science Technical Report, pp. 1-25, 2000.
- [16] C.-C. Lo, C.-C. Huang, and J. Ku, "A cooperative intrusion detection system frame-work for cloud computing networks," pp. 280-284, 2010.
- [17] T. Garfinkel, M. Rosenblum et al., "A virtual machine introspectionbased architecture for intrusion detection." vol. 3, pp. 191-206, 2003.
- [18] Aborujilah, A., & Musa, S. (2016). Critical review of intrusion detection systems in cloud computing environment. 2016 International Conference on Information and Communication Technology (ICICTM).
- [19] Aryachandra, A. A., Arif, Y. F., & Anggis, S. N. (2016). Intrusion Detection System (IDS) server placement analysis in cloud computing. 2016 4th International Conference on Information and Communication Technology (ICoICT).
- [20] Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2016). A survey of intrusion detection systems for cloud computing environment. 2016 International Conference on Engineering & MIS (ICEMIS).
- [21] M. Yasir, M.A. Shibli, H. Umme and M. Rahat, "Intrusion Detection System in Cloud Computing: Challenges and Opportunities," 2nd National Conference on Information Assurance (NCIA), 2013, pp.5966.