International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 3, May-June-2021, ISSN (Online): 2395-566X

A Survey on Cloud Environment Intrusion Detection System Types and Issues

Asst. Prof. Ms. Amlesh Singh, Dean Dr. Pratima Gautam
Department of CS/IT
RabindraNath Tagore University,
Bhopal, India
dearamlesh@gmail.com, pratima.gautam@aisectuniversity.ac.in

Abstract- **Cloud reduces implementation cost and increases flexibility of data access around the globe. But this easiness of uses introduces the vulnerability in the network. So different type of attacks inform of intrusion was prepared and execute by insider or outsider virtual machines in the cloud. Detection of such type of attacks needs to develop intrusion detection system. This paper has found type of intrusion in cloud environment. Further paper has summarized various techniques proposed by scholars to develop a intrusion detection system. Various intrusion detection system were classified as per detection approaches adopt by researcher. Finally paper detailed the issues of cloud security that make this area of research more complex.**

Keywords- **Cloud Security, Intrusion Detection, ANN, Clustering, Genetic Algorithm, Intrusion Detection.**

I. INTRODUCTION

The appealing features of Cloud computing continue to fuel its integration in many sectors including industry, governments, education, entertainment, to name few [1].

Cloud computing aims to provide convenient, on-demand, network access to a shared pool of configurable computing resources, which can be rapidly provisioned and released with minimal management effort or service provider interactions [2].

The pay-as-you-go and the on-demand elastic operation Cloud characteristics are changing the enterprise computing model, shifting on-premises infrastructures to off premises data centers, accessed over the Internet and managed by cloud hosting providers. However, many security issues arise with the transition to this computing paradigm including intrusions detection. Regardless the important evolution of the information security technologies in recent years, intrusions and attacks continue to defeat existing intrusion detection systems in Cloud environments [3].

Attackers developed new sophisticated techniques able to brought down an entire Cloud platform or even many within minutes. New records are breached each year by attacker. Recently a destructive DDoS attack have brought down more than 70 vital services of Internet including Github, Twitter, Amazon, Paypal, etc. Attackers have taken advantages of Cloud Computing and Internet of Things technologies to generate a huge amount of attack traffic.

Employing an effective IDS in the cloud is a challenge from different aspects. One aspect is the complication of the security problem due to the cloud's deep stack of dependent layers. The functionality and security of a higher layer depend on its lower layers. This aspect is further augmented by the sophistication of modern attacks.

Another aspect is the new requirements stemming from the unique characteristics of the cloud environment such as scalability and elasticity. These requirements pose additional challenges on the traditional IDSs in many ways.

Hence, the development of robust cloud-oriented IDSs must identify and accommodate such unique cloud requirements. The last aspect is the deployment architecture selection as each choice has its own advantages and limitations with respect to the effectiveness of the IDS.

II. TYPES OF INTRUSION IN CLOUD

An intrusion is any attempt that can compromise the CIA of a system or network. The most common intrusions that affect the CIA of cloud are the following: [3]

1. Attacks On Hypervisor Or Virtual Machines:

An attacker may successfully control the virtual machines by compromising the hypervisor. The most common attacks on virtual layer which enable hackers to supervise host through hypervisor.

Attackers target the hypervisor or VMs to access them by exploiting the zero-day vulnerabilities in virtual machines, prior to the developers' awareness about such exploits [3]. The exploitation of a zero-day vulnerability in the HyperVM application caused damage to several websites based on virtual server [17].

2. User To Root (U2R) Attacks:
The attacker uses password sniffing to access a genuine user's account which enables him to obtain root privileges to a system by exploiting vulnerabilities, e.g. Root shells can be created by using Buffer overflows from a root-level process. In the cloud scenario, attacker achieves root privileges of host or VMs by first getting access to legal user instances. This attack violates the integrity of cloud based systems [3].

3. Insider Attack:
The attackers are the authorized users who try to obtain and misuse the privileges that are either assigned or not assigned to them officially [3]. This attack is closely related to trust since insiders may reveal secrets to opponents, e.g. Amazon Elastic Compute Cloud (EC2) suffered from an internal DoS attack [13]. This attack breaches the confidentiality of cloud users.

4. Port Scanning:
Attackers can use port scanning to obtain list of closed ports, open ports, and filtered ports and then launch attacks against the services running on open ports. Different techniques of port scanning are SYN scanning, ACK scanning, TCP scanning, FIN scanning, UDP scanning etc. In cloud environment, attacker can discover the open ports using port scanning and attack the services running on these ports [3]. This attack may cause loss of confidentiality and integrity on cloud.

5. Backdoor Channel Attacks:
Hackers can remotely access the infected machines by exploiting this passive attack to compromise the confidentiality of user information. Hacker can use backdoor channels to get control of victim's resources and utilize it as zombie to launch DDoS attack [3]. This attack targets the confidentiality and availability of cloud users.

6. Denial Of Service (Dos) Attack:
The attacker exploits zombies for sending a large number of network packets to overwhelm the available resources. Consequently, legitimate users are unable to access the services offered over the Internet. In cloud environment, the attacker may send huge number of requests through zombies to access VMs thus disabling their availability to legitimate users which is called DoS attack [3]. This attack targets the availability of cloud resources.

III. RELATED WORK

Vajayanand et al. [7] has proposed a intrusion detection system where features were select from the training dataset by utilizing genetic algorithm and mutual information. Selected features from the training dataset were used to train support vector machine model. In this paper result shows that feature reduction by genetic algorithm has increase the learning or classification accuracy of the SVM model.

Kabir et al. [8] has develop a OALSSVM model (optimum allocation least square support vector machine). In this paper optimum allocation term select session from the whole dataset either from training or testing section of dataset. These selected session or samples were used to train the support vector machine model. So, output of proposed OALSSVM is depend on selected session which increase its accuracy of intrusion detection.

Chuanlong Yin [9] In this article, author examine how to present an interruption recognition framework in light of thoughtful learning, and this exertion offer a thoughtful knowledge approach for interruption recognition using recurrent neural networks (RNN-IDS). In addition, this exertion inspects the execution of the model in balancing categorization and multiclass arrangement, and the amount of neurons and characteristic learning rate impacts on the implementation of the planned show.

This effort compares it and those of J48, artificial neural network, arbitrary woodland, bolster vector machine, and further machine knowledge approach planned by history analysts on the standard information directory index.

Moukhafi et al. [10] has proposed a feature reduction model for increasing the detection accuracy of intrusion in the network. This paper has utilized a particle swarm optimization genetic algorithm for the selection of features form the input dataset as per number of class for detection. Selected feature from the training dataset were used to train support vector machine. This hybrid genetic and SVM model work well to detect DOS attacks.

Kaiyuan et. al. in [11] propose a network intrusion detection algorithm combined hybrid sampling with deep hierarchical network. Firstly, we use the one-side selection (OSS) to reduce the noise samples in majority category, and then increase the minority samples by synthetic minority over-sampling technique (SMOTE).

In this way, a balanced dataset can be established to make the model fully learn the features of minority samples and greatly reduce the model training time. Secondly, we use convolution neural network (CNN) to extract spatial features and Bi-directional long short-term memory (BiLSTM) to extract temporal features, which forms a deep hierarchical network model.

In [12] have proposed to utilize information mining system, order tree and bolster vector machine for intrusion discovery. Information mining system have made valuable strides towards arrangement of different issues in various issues, use information digging for tackling the issue of intrusion as a result of following reasons: It can process expansive measure of information.

Client's subjective advancement isn't vital, and it is more appropriate to find the disregarded and shrouded data.

Machine learning is a logical teach that enables PCs to learn in light of information and naturally figures out how to perceive complex examples and to settle on keen choice in light of information.

ID3 and C4.5 two basic arrangement tree calculation utilized as a part of information mining. Bolster vector machines are an arrangement of related administered learning techniques utilized for grouping and expectation. Author said C4.5 calculation is smarter to SVM in recognizing system intrusions and FAR (false caution rate) in KDD CUP 99 dataset.

Subramanian1 et. Al. in [13] shape the future generation of cloud security using convolution neural network because CNN can provide automatic and responsive approaches to enhance security in cloud environment. Instead of focusing only on detecting and identifying sensitive data patterns, ML can provide solutions which incorporate holistic algorithms for secure enterprise data throughout all the cloud applications.

IV. TYPES OF INTRUSION DETECTION SYSTEM

1. Network based Intrusion Detection System:
Network intrusion detection system monitors and analyzes network traffic by reading individual packets through network layer and transport layer. It searches for any suspicious activity or network based attack such as Denial of Service (DoS) attack, port scans etc. Once an abnormal behavior in network traffic is identified, alert can be sent to system administrator. Most of the commercial IDSs are based on the NIDS such as Snort, Tcpdump and Natural flight [14].

These are well known for general sized networks and convenient for implementation to detect intrusions. The main issues of Snort IDS when integrating with distributed computing environment.

To overcome the issues, they introduced new approach for handling these issues. For virtual network systems, multi phase distributed vulnerability detection and measurement technique has been proposed to detect DDoS attack. It has detected attacks based on attack graph by analyzing network traffic flowing through virtual machines. It has significantly improved attack detection and mitigates attack consequences.

2. Host Based Intrusion Detection System:
Host based intrusion detection system monitors the individual host or device on the network by analyzing any change in the activity performed by host and events occurring within that host. It looks at every activity of host by checking application logs, system calls, and file-system modifications, inbound and outbound packets to and from host. If any suspicious activity is found, an alert is generated and sent to administrator to protect the system from malicious attack. Since majority of sectors prefer HIDS also after NIDS which are mainly based on the log file analysis of system. A model of HIDS has been developed based on log file analysis of Microsoft Windows XP operating system. It detects intrusions by matching predefined pattern with the logs of operating system [15].

3. Distributed based Intrusion Detection System:
Distributed IDS (DIDS) also known as hybrid IDS, consists of two or more detection methods or systems i.e., NIDS, HIDS etc [16]. This type of system is deployed over large distributed network like cloud computing so as all entities can communicate with each other and with network monitor such as central server In this way, all hosts deployed over network collect system information and send it to central server by converting it into standard format.

4. VMM/Hypervisor based Intrusion Detection System:
Hypervisor provides a platform for communication among VMs. Hypervisor based IDSs is deployed at the hypervisor layer. It helps in analysis of available information for detection of anomalous activities [17]. The information is based on communication at various levels like communication between VM and hypervisor, between VMs and communication within the hypervisor based virtual network.

V. SECURITY ISSUES IN THE CLOUD

Each layer in the cloud stack has different implementations and different security requirements. This results in layer-specific or cross-layer vulnerabilities which complicate the development of a standard IDS model. Cloud computing inherits most of the core technologies used in the Web and Internet, virtualization, and other foundation technologies. The integration of these technologies in cloud computing systems makes the cloud more vulnerable to secu-rity risks [18].

Attackers can exploit novel attack venues as well as existing ones that are already associated with the use of these core technologies. Additionally, the complexity of the cloud that stems from the increased number of involved parties, devices, and applications often leads to an increase in the num-ber of security holes.

The cloud layers share three major security issues that hinder the acceleration of cloud services adoption as follows [19]: loss of control, lack of isolation, and lack of regulation enforcement.

1. Loss of Control:
Data, applications, software services, and other assets in the cloud are typically hosted and maintained in a virtualized environment by third parties.

2. Lack of Isolation:
This is very critical due to the multi-tenancy characteristic of the cloud. Virtualization, which is the motor behind multi-tenancy in cloud layers, may suffer from vulnerabilities that can allow an attacker or an insider user to gain access to sensitive assets belonging to co-located tenants.

3. Lack of Regulation Enforcement:
Cloud consumers may not be able to enforce regulations that govern the flow and storage of their information, or even verify if the provider complies with their security requirements.

The aforementioned issues are emerged due to wide attack vectors within or across the different layers of the cloud. The cloud application layer is a prime target by attackers due to the existence of various vulnerabilities. In a recent study, 96% of tested cloud applications have one or more serious security vulnerabilities. Cloud-hosted application development relies mostly on existing web and internet technologies. Hence, most of the secu-rity problems related to web-enabled applications remain relevant when the same applications migrate to a cloud environment [20].

Vulnerabilities such as injection, cross site scripting, and information leakage are still prevalent in cloud applications as they account for more than 55% of the reported security flaws. The cloud infrastructure and virtualization layers are also prime targets by attackers due to the existence of operational and configuration vulnerabilities.

According to the NIST's bug report, the virtualization layer is considered a dangerous attack surface as a miss configured VMM could result in a single point of compromise for the security of all hosted components. Attackers can focus their efforts on breaching vulnerabilities in the infrastructure layer (VMs) and then escape from one VM to another VM or to the virtualization layer (VMM).

They may also directly exploit vulnerabilities in the virtualization layer in order to gain full control over the underlying physical machine on which the VMs are running. Virtualization vulnerabilities ac-count for only a small subset of all vulnerabilities. However, it still represents a growing virtualization security concern especially in the cloud by creating a new attack surface against the VMM which can lead to various attacks such as cross-VM side channel, denial-of-service (DoS), malware, and rootkit attacks.

VI. CONCLUSION

As more and more of our modern computing infrastructure migrates to the cloud, intrusion detection will become an ever more important piece of the research landscape. To protect infrastructures, organizations all over the world are spending considerable amounts on information security and privacy.

This paper has found that reducing the dimension of session dataset increases the detection accuracy. It was found that because of dynamic nature of cloud vulnerability increases and this directly raise the chance of attacks. It was found from the survey that machine learning approach was mostly used by scholar to detect the intrusion on the cloud. In future scholar can develop a less false alarm generator algorithm.

REFERENCES

[1] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, P. R. Inacio, Security Issues In Cloud Environments: A Survey, International Journal ´ Of Information Security 13 (2) (2014) 113–170.

[2] P. Mell, T. Grance, The Nist Definition Of Cloud Computing.

[3] S. Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. K. Khan, K. K. R. Choo, On Cloud Security Attacks: A Taxonomy And Intrusion Detection And Prevention As A Service, Journal Of Network And Computer Applications 74 (2016) 98–120.

[4] Wikipedia, 2016 Dyn Cyberattack[Online; Accessed 10-November-2017)].

[5] The Guardian, Ddos Attack That Disrupted Internet Was Largest Of Its Kind In History, Experts.

[6] Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, “A Survey Of Intrusion Detection Techniques In Cloud”, Journal Of Network And Computer Applications 36 (2013), Pp. 42–57.

[7] R. Vijayanand, D. Devaraj, And B. Kannapiran, ‘‘A Novel Intrusion Detection System For Wireless Mesh Network With Hybrid Feature Selection Technique Based On GA And MI,’’ J. Intell. Fuzzy Syst., Vol. 34, No. 3, Pp. 1243–1250, 2018.

[8] E. Kabir, J. Hu, H. Wang, And G. Zhuo, ‘‘A Novel Statistical Technique For Intrusion Detection Systems,’’ Future Gener. Comput. Syst., Vol. 79, Pp. 303–318, Feb. 2018.

[9] Chuanlongyin, Yuefei Zhu, Jinlong Fei, And Xinzheng He. “A Deep Learning Approach For Intrusion Detection Using Recurrent Neural Networks” Current Version November 7, 2017.

[10] M. Moukhafi, K. El Yassini, And S. Bri, ‘‘A Novel Hybrid GA And SVM With PSO Feature Selection For Intrusion Detection System,’’ Int. J. Adv. Sci. Res. Eng., Vol. 4, Pp. 129–134, May 2018.

[11] Kaiyuan Jiang, Wenya Wang, Aili Wang, and Haibin Wu. "Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network". IEEE Access February 24, 2020.

[12] Kalpesh Adhatrao, Aditya Gaykar, Amiraj Dhawan, Rohit Jha And Vipul Honrao. "Predicting Students’ Performance Using Id3 And C4.5 Classification

Algorithms". International Journal Of Data Mining & Knowledge Management Process (IJDKP) Vol.3, No.5, September 2013.

[13] E. K. Subramanian, Lathatamilselvan. "A Focus On Future Cloud: Machine Learning-Based Cloud Security". Service Oriented Computing And Applications, 12 August 2019.

[14] M. Ahmed, R. Pal, M. M. Hossain, M. A. N. Bikas And M. K. Hasan, "NIDS: A Network Based Approach To Intrusion Detection And Prevention," 2009 International Association Of Computer Science And Information Technology - Spring Conference, Singapore, 2009.

[15] Zegzhda P., Kort S. (2007) Host-Based Intrusion Detection System: Model And Design Features. In: Gorodetsky V., Kotenko I., Skormin V.A. (Eds) Computer Network Security. MMM-ACNS 2007. Communications in Computer and Information Science, Vol 1. Springer, Berlin, Heidelberg.

[16] Y. J. Ou, Y. Lin, Y. Zhang And Y. J. Ou, "The Design And Implementation Of Host-Based Intrusion Detection System," 2010 Third International Symposium On Intelligent Information Technology And Security Informatics, Jian, China, 2010.

[17] Shabnam Kazemi; Vahe Aghazarian; Alireza Hedayati. “Improving False Negative Rate In Hypervisor- Based Intrusion Detection In Iaas Cloud Full Text” Volume 2 Issue 9.

[18] Grobauer, B., Walloschek, T. And Stocker, E.: Understanding Cloud Computing Vulnerabilities, Proc. IEEE Security & Privacy, Vol.9, No.2, Pp.50-57 (2011).

[19] Xiao, Z. And Xiao, Y.: Security and Privacy in Cloud Computing, Proc. IEEE Communications Surveys & Tutorials, Vol.15, No.2, Pp.843-859 (2013).

[20] Almorsy, M., Grundy, J. And Muller, I.: An Analysis Of The Cloud Computing Security Problem, Proc. 2010 Asia Pacific Cloud Workshop, Australia (2010).

[21] Vollmer, W., Harris, T., Long. L. And Green, R.: Hypervisor Security In Cloud Computing Systems. Proc. ACM Computer Survey (2014).

[22] Perez-Botero, D., Szefer, J. And Lee, R.: Characterizing Hypervisor Vulnerabilities In Cloud Computing Servers. Proc. 2013 International Workshop On Security In Cloud Computing. Pp.3-10 (2013).