Review of CIDS and Techniques of Detection of Malicious Insiders in Cloud-Based Environment

Priya Oberoi and Sumit Mittal

Abstract Cloud computing has gained an extreme importance nowadays. Every organization is getting attracted toward the Cloud computing due to its attractive features like cost saving, adaptability, etc. Although it offers the attractive features but still Cloud threats need great consideration. The insider threat is critically challenging in the Cloud-based environments. In order to mitigate from insider attacks in Clouds, the use of Intrusion detection system (IDS) is quite challenging. Every type of IDS has different methods of attack detection. So, single IDS cannot guarantee the protection from all types of attacks. Thus, in this paper, we have studied the various types of IDS and their features which made them either suitable or unsuitable for cloud computing. Also on the basis of review, required features for the Cloud-based IDS are identified.

Keywords Intrusion detection system · Cloud computing · Cloud security CIDS

1 Introduction

In recent times, the IT infrastructure is outsourced by the companies to the Cloud in order to get the benefits offered by the Clouds like scalability, rapid provisioning, and reduced cost. In spite of the advantages offered by Clouds, security in general and malicious insider threats in particular has been the most critical area of concern of the organizations. Thus, gaining the trust of the Cloud users' security from the insider threats is important to achieve [1, 2]. The traditional mechanisms of intrusion detection are not flexible enough to manage with the needs of Clouds,

P. Oberoi (✉) · S. Mittal
M.M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India
e-mail: priya.hrt@gmail.com

S. Mittal
e-mail: sumit.mittal@mmumullana.org

M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_11

such as frequent changes in infrastructure. In this paper, we study the problem of insider threats within the domain of Cloud computing. Also, we have studied the various intrusion detection systems available for the Cloud environments and identified the characteristics which are offered by the existing systems and the needs for the future improvements.

2 Cloud Computing: A Security Perspective

The security remains the biggest issue in Cloud computing, as Cloud provides services which are located on a remote location and it is the trust of consumer on Cloud service providers that their data will be secured. The integrity and confidentiality of the user's data are at risk as they do not have physical control over the data [3]. This is because of the fact that the Cloud server is at different location and client is located at different locations. Therefore, the server cannot be trusted completely for managing details of users and access rights. The data of user is at risk due to insider attacks or compromised servers. This can be overcome if the users trust Cloud service providers to secure and properly manage their data [4]. Due to the fact that the insiders are very well familiar with the infrastructure, procedures of operation and terms and conditions of the organization the attack of malicious insiders are more severe [4]. Insider attacks are done by malicious employees at any location, i.e., provider's or user's. The attacks caused by the insiders have an adverse effect on the trust of the Cloud user on the provider. Passwords, cryptographic keys, and files can easily obtained by the malicious insider. These attackers not only damage the financial value but also the reputation of an organization [4].

3 Intrusion Detection System (IDS)

Intrusion detection is the process of monitoring computers or networks for unauthorized entry, activity, or file modification.

3.1 Classification of IDS According to Source of Data [5, 6]

1. **Host-based intrusion detection system (HIDS)**: in which sensors are responsible for detecting intrusions. Intrusions are found on single host. These operate on host side and monitors as well as detects malicious activities in system calls, application logs, etc.
2. **Network intrusion detection systems (NIDS)**: sensors are focused on network segment only. NIDS monitor the attacks in networks and detect the variation in the transmissions in the networks.

3. **Distributed intrusion detection systems (DIDS)**: combine both the types of sensors. It further has three types: (a) Mobile agent IDS (MA-IDS), (b) Grid-based IDS (GIDS), and (c) Cloud-based IDS (CIDS).

3.2 Limitations of Various IDSs

HIDS cannot be used as attackers may not leave traces in the operating system of the host where the IDS are residing. NIDS cannot detect the attack if the communication is encrypted. In clouds, distinct users share various resources. The attacks can migrate from and be intended for any of the Cloud resources. Thus only DIDs can be used. But, the challenges in the adoption of the DIDS in Clouds are (i) Distinct types of users and user requirements; (ii) Complex architecture; and (iii) Different requirement of security. MA-based IDS are not suitable as (i) Hierarchical structure poses problem of reliability and scalability, and (ii) Not flexible to protect from the attacks on IDS itself. GIDS are not suitable as (i) Every service model (SaaS, IaaS and PaaS) has different set of threats, users, and requirements; (ii) Clouds are highly scalable; (iii) GIDS solution cannot correlate the alerts from the different nodes; (iv) Performance and load balancing are needed more in Clouds than Grid [6].

4 Literature Review

Rule-based learning for the identification of insiders and a solution for the detection of wrong insider activities have been given by the authors [7]. Some of the threats identified include insecure shared technology vulnerabilities, application programming interfaces, and malicious insiders. When an attack occurs, machine learning techniques are used to raise an alarm. The seven common activities of the insiders are (Table 1):

For activity classification purposes, the following machine learning techniques are used (Table 2).

It has been found by the analysis that decision tree C4.5 and multilayer perception are better for activity classification in Cloud-based environment. The result of the confusion matrix reveals C4.5 as the best classifier.

Authors in [8] have used technique of multithreading for improving the performance of the IDS. NIDS proposed sensitizes as well as monitors the network traffic using the sensors. In this model, the Cloud user accesses the remote servers over the Cloud network. The monitoring and logging of the requests and the actions of the user are done by a multi-threaded NIDS, which has large data handling capacity and also reduces the packet loss.

Table 1 Common activities of insiders

S. No.	Activity
1	No activity
2	Reboot physical machine
3	Malicious insider cloning
4	Malicious insider copying everything from a VM
5	Malicious insider taking snapshots of VM
6	Installing new guest VM on the same physical hardware
7	Turn on any guest VM on to same physical hardware

Table 2 Machine learning techniques

S. No.	Technique	Basis
1	Naive Bayes	Probability-based technique
2	Multilayer Perception	Function estimated based technique
3	Support Vector Machine	
4	Decision Tree	Rule-based technique
5	PART	

A combined approach for malware detection and root kit prevention used in [9] in virtualized Cloud environment. The IDS is intended to execute on VM instances with a backend Cloud to share out malware scanning operations among numerous back ends. Flexible, distributed security solution is given with a minimal overall resource footprint on the end host. The traditional signature checks are performed for the detection of known as all as the novel malware. An integrity check of authorized Kernel modules is given which can prevent the installation of root kits through the corrupted kernel modules. This approach is easy to maintain as only change is to be made in the kernel of the system. Infrastructural security is focused not the attacks against VM monitors.

Authors [5] in their research presented a review of various methods and tools used for detection and prevention of intruders in Cloud computing. Four concepts for the development of the CIDS identified are (a) automatic computing; (b) oncology; (c) risk management; and (d) fuzzy theory. The taxonomy gives two layers functional layer and structural layer. The requirements identified for CIDPS on the basis of review are (i) large-scale handling of multi tiered autonomous computing and data processing environments; (ii) detection of variety of attacks with least positive rates; (iii) super fast detection and prevention; (iv) self-adaptive automatically; (v) CIDPS Scalability; (vi) deterministic; (vii) synchronization of autonomous CIDPS; (viii) resistance to compromise. A Cloud intrusion detection and prevention system which meets all the requirements is considered to be good one.

A framework of CIDS is presented in [6], which has a module to review the alerts and notify the administrator of the Cloud. The features identified are (i) point-to-point solution which is applicable to various platforms and expandable; (ii) as there is no central coordinator, so single point of failure is not there; (iii) distribution of processing to different Cloud locations protects the CIDS from the threats which can organize a job in the VM and alter its workings if it was executed in monitored VM; (iv) installing middleware where the framework resides increases the flexibility and portability; (v) it uses knowledge base combined with the behavior base which increases attack coverage; (vi) every node has audit system for monitoring of the messages and logging. It gives the benefit that every node has the capability to detect the masqueraders. The following three models have been given as CIDS detection models:

1. **Audit Exchange Model (Model A)**: The nodes Cloud swap over audit data. It has high detection efficiency and the low survival of the masquerader. Its limitations include need of rapid cyclic updates of audit data at the CNs.
2. **Audit Exchange Model with a neural network (Model B)**: Combines model A to neural networks. It offers the benefit of less survival of masquerader than Model A and C. Also the hit rate is high with lower false positive and false negative alarms than Model A and C. Other than limitations of model A; it has a limitation of low performance due to overhead to update neural network.
3. **The Independent Model (Model C)**: Every node of Cloud calculates its own audit data without swapping data with Cloud nodes. The benefits offered are no need of periodic update and less burden for Cloud network, as no swapping of data is there. Also there are low processing overheads than model A and C. Limitations include longer survival of masquerader than model A & B and low hit rate than model B as neural cannot be used.

The applications of the three proposed models are to be done to find the best one. Also the summarizer and parser algorithms are to be parallelized in order to reduce the corresponding overhead.

An Insider threat detection model to detect despiteful insiders has been proposed in [10]. An observational system to test this possibility was implemented to sustain the applicability in a SaaS Cloud deployment model. This method uses the sequential rule mining approach to discover malicious utilization patterns for a particular profile.

Authors in [11] have given an ICAS (IDS Cloud analysis system). MapReduce algorithm of Hadoop is used for the analysis of intrusion detection system in log files. It creates a user-friendly output view in which user can easily and clearly monitor the behavior of the attack. In experimental study, it has been found that the calculation speed is increased by 80%. IDP8200, NK7 Admin and Snort logs are used as ICAS analysis object record in this paper. The main advantage of ICAS is the scalability and reliability offered by it. ICAS can be improved for the processing large-scale data.

A framework which is an open source solution has been given in [12]. APIs and interfaces are given which are used in the development of the security components in a distributed manner and building of customized event correlation rules. The framework consists of a collection of components which are organized in a hierarchical manner. The three main components of the framework are probes, agents, and security engines.

According to the three architectural layers, the security engines are organized in a hierarchical manner. At the lowest layer, the raw security data collected by the security engines. It can be offered by the Cloud provider as service which includes IDSs; Log analyzers; and specific security mechanisms provided by the Cloud platform. It is the responsibility of the Cloud provider, at the higher level, to enable additional IDSs and attack them to independent VMs. The provider is able to recognize the compromised virtual components of the clients by correlating the information provided by the higher layer with the data collected by the lower layer. Attack Evaluation Tree (AET) is used to represent the attack in a tree like structure. The goal of the attacker is the root node while the access path is through the offsprings.

Authors in the research [13] introduced three concrete MI attacks with a proof of concept implementation based on existing tools. Three introduced MI attacks in this paper are: memory scanning, template poisoning, and snapshot cracking.

Authors [14] described the differences between the traditional insider and insider in the Cloud. The two types of insider threats identified in Cloud computing, viz., (a) at the Cloud providers end, and (b) at the Cloud clients end. Both have different set of problems and area of attacks. The countermeasures of the insider threat in the Cloud provider are:-At client side: Cryptographic techniques, geo-redundancy are used; and At provider side: Separation of duties, logging, legal binding, and insider detection models. The problems in various methods are: (a) IDS/IPS: in IaaS host-based IDS can be used, (b) Separation of duties: As in Clouds, same person has multiple roles, it is difficult to implement it in Clouds; (c) Attack origin identification: (i) In case of Clouds, the access is usually done by some remote computer. So there are no physical evidence for the attack, only digital evidence like IP etc can be used and (ii) In case of shared credentials, it is difficult to fix the responsibly; (d) Single point of failure and data leakage: Access to console of administrator can cause heavy loss of that, that without any sign of intrusion. The countermeasures of the insider threat in the Cloud outsourcer are (a) At client side: Log auditing, host-based IDS/IPS are used and (b) At provider side: Anomaly detection, separation of duties, and multifactor authentication are used.

5 Comparative Study

The various techniques being used for the detection of the intruders revealed by review are proactive forensics, graph-based analysis, honey pots (based on network sensors), IDS (based on network sensors), system call analysis (host based user profiling), command sequences and windows usage events, file system, memory, I/O, and hardware monitoring, metrics about user sophistication (Usage Anomalies), insider threat specification language, knowledge graphs, customized minimal attack trees, technological, social and educational and psychological parameters [15–21].

Selecting the best one is quite challenging. The characteristics desired in a CIDS are (i) Scalable and distributed IDS for Clouds without the failure points, (ii) Combination of Knowledge base and behavior base in order to detect the known as well as the unknown attacks with reasonable false alarm rates, (iii) Avoid single point of failure, (iv) the IDS should be protected from the attacks by isolating it, (v) flexible architecture, (vi) take into consideration various service models and requirements of user, (vii) dynamic policies as the security needs of each VM are varied, (viii) reduction in data transfer cost by reducing the network bandwidth, (ix) easy to adapt.

6 Future Scope

In this paper, we studied the insider attacks in the Cloud-based environments. An insider can easily attack in the Cloud environment. The effect of the attack is more severe than the traditional environments. Also the entity that physically performed the attack is difficult to detect and identify. The literature review has revealed the fact that in order to secure Cloud environment from the insiders a new insider prediction and detection models is needed. Also to evade the false estimations and generate correct user profiling new CIDS is required. Moreover, it appears that there is an adorning necessity for developing transparent network in Clouds. Also application intrusion detection systems (IDS) for Clouds are required. These systems can be given as a service to their clients who want to protect their infrastructure which has been outsourced. In future, model for predicting and detecting insider threats will be developed.

References

1. https://en.wikipedia.org/wiki/Cloud_computing
2. Forrester-2012, Cloud survey. http://www.bmc.com/industryanalysts/reports/forrester-2012-cloud-survey.html (accessed May 2012)
3. Yusop ZM, Abawajy JH (2014) Analysis of insiders attack mitigation strategies. Procedia Soc Behav Sci 129:581–591
4. Ren K, Wang C, Wang Q (2012) Security challenges for the public cloud. IEEE Internet Comput 16(1):69–73. https://doi.org/10.1109/MIC.2012.14
5. Patel A, Taghavi M, Bakhtiyari K, Júnior JC (2013) An intrusion detection and prevention system in cloud computing: a systematic review. J Netw Comput Appl 36(1):25–41

6. Kholidy HA, Baiardi F (2012) CIDS: a framework for intrusion detection in cloud, systems. In: 2012 ninth international conference on information technology—new Generations, 978-0-7695-4654-4/12 $26.00 © 2012 IEEE
7. Khorshed MT, Ali ABMS, Wasimi SA (2011) Monitoring insiders activities in cloud computing using rule based learning. In: IEEE 10th international conference on trust, security and privacy in computing and communications (TrustCom-2011), 16–18 Nov 2011
8. Gul I, Hussain M (2011) Distributed cloud intrusion detection model. Int J Adv Sci Technol 34
9. Schmidt M, Baumgartner L, Graubner P, Bock D, Freisleben B (2011) Malware detection and kernel rootkit prevention in cloud computing environments. In: 19th Euromicro international conference on parallel, distributed and network-based processing (PDP-2011), pp 603–610, 9–11 Feb 2011
10. Nkosi L, Tarwireyi P, Adigun M (2013) Insider threat detection model for the cloud. 978-1-4799-0808-0/13/$31.00 ©2013 IEEE
11. Yang S-F, Chen W-Y, Wang Y-T (2011) ICAS: an inter-VM IDS log cloud analysis system. In: IEEE international conference on cloud computing and intelligence systems (CCIS-2011), 15–17 Sept 2011
12. Ficco M, Tasquier L, Aversa R (2013) Intrusion detection in cloud computing. In: 18th international conference on P2P, parallel, grid, cloud and internet computing (3PGCIC-2013), pp 276–283, 28–30 Oct 2013
13. Nguyen M-D, Chau N-T, Jung S, Jung S (2014) A demonstration of malicious insider attacks inside cloud IaaS vendor. Int J Inf Educ Technol 4(6). https://doi.org/10.7763/ijiet.2014.v4.455
14. Kandias M, Virvilis N, Gritzalis D (2013) The insider threat in cloud computing. In: Critical information infrastructure security. Lecture notes in computer science, vol 6983. Springer, Berlin, pp 93–103
15. Mehmood Y, Habiba U, Muhammad AS, Masood R (2013) Intrusion detection system in cloud computing: challenges and opportunities. In: 2nd national conference on information assurance (NCIA), pp 59–66, 978-1-4799-1288-9/13©2013 IEEE
16. Gupta S, Kumar P, Sardana A, Abraham A, A fingerprinting system calls approach for intrusion detection in cloud environment. In: 4th international conference computational aspects of social networks (CASoN-2012), published by IEEE, pp 309–314
17. Martinez-Moyano IJ, Rich E, Conrad S, Andersen DF, Stewart TR (2008) A behavioral theory of insider threat risks: a system dynamics approach. ACM Trans Modeling Comput Simul 18(2):7.1–7.27
18. Dileep Kumar G, Morarjee K (2014) Insider data theft detection using decoy and user behavior profile. Int J Res Comput Appl Robot 2(2):51–55. ISSN: 2320-7345. www.ijrcar.in
19. Young WT, Goldberg HG, Memory A, Sartain JF, Senator TE (2013) Use of domain knowledge to detect insider threats in computer activities. IEEE security and privacy workshops
20. Wongthai W, Rocha F, Van Moorsel A (2013) Logging solutions to mitigate risks associated with threats in infrastructure as a service cloud. In: International conference on cloud computing and big data, pp 163–170
21. Claycomb WR, Nicoll A (2012) Insider threats to cloud computing directions for new research challenges. In: Proceedings of the 2012 IEEE 36th annual computer software and applications conference, pp 387–394. IEEE Computer Society, Washington, DC, USA ©2012

Author Biographies

Ms. Priya Oberoi received her Master's degree from Maharishi Dayanad University, Rohtak. Presently, pursuing Ph.D. from M.M. (Deemed to be University), Mullana, Ambala, Haryana, India. She is working as Assistant Professor in Department of Computer Science, D.A.V Centenary College, Faridabad. She has 10 publications in International/National Journals and Conferences.

Dr. Sumit Mittal received his Ph.D. degree & Master's degree from Department of Computer Science & Applications, Kurukshetra University, Kurukshetra. Presently, he is working as Professor & Principal, M.M. Institute of Computer Technology & Business Management, M.M. (Deemed to be University), Mullana, Ambala, Haryana, India. He is a life member of Computer Society of India and member of various professional societies of India & Abroad. He is also a member of various academics bodies of M.M. University, Mullana. He has more than 35 publications in International/National Journals and Conferences. His research area includes Cloud Computing, Wireless communication and Distributed Environments.