A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing: Proceedings of ICICC 2018, Volume 1

Chapter · January 2019

DOI: 10.1007/978-981-13-2324-9_23

Shadab Alam
Jazan University
52 PUBLICATIONS 582 CITATIONS
SEE PROFILE

Mohammed Shuaib
Jazan University
38 PUBLICATIONS 405 CITATIONS
SEE PROFILE

Abdus Samad
Aligarh Muslim University
22 PUBLICATIONS 176 CITATIONS
SEE PROFILE

A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing

Shadab Alam, Mohammed Shuaib and Abdus Samad

Abstract Cloud computing is emerging as a powerful solution to ever-growing storage and processing requirements of an organization and individual without the burden of owning and handling the physical devices. Security is one of the primary concerns in cloud computing for large-scale implementation. Intrusion detection and prevention (IDP) techniques can be applied to secure against intruders. In this paper, we have studied different IDP techniques comprehensively and analyzed their respective strengths and weaknesses on various parameters to provide security in cloud computing. Hypervisor-based and distributed IDS have shown promising security features in cloud computing environment in comparison with traditional IDP techniques.

Keywords Cloud computing · Intrusion detection · Intrusion prevention · IDS
IPS · IDPS · Security

1 Introduction

Cloud computing has changed the perception of processing and data storage drastically, and it has the ability to use resources for processing and storage without physically owing them and with minimal setup time. Although cloud computing is not considered as very secure initially, now it has gained a lot of preference from businesses. Annual Cloud Computing Survey by Clutch has shown that around 70%

S. Alam · M. Shuaib
Department of Computer Science, Jazan University, Jizan, Saudi Arabia
e-mail: s4shadab@gmail.com

M. Shuaib
e-mail: talkshuaib@gmail.com

A. Samad (✉)
Faculty of Engineering & Technology, Women's Polytechnic, AMU, Aligarh, India
e-mail: abdussamadamu@gmail.com

S. Bhattacharyya et al. (eds.), *International Conference on Innovative Computing and Communications*, Lecture Notes in Networks and Systems 55,
https://doi.org/10.1007/978-981-13-2324-9_23

business organization are willing to adopt cloud computing for their storage and processing needs by applying some additional security features [1].

These days typically, IT technologies are dependent for its safety on message encryption and firewalls to guard their networks, but they are not adequate as the sole defense mechanisms [2]. Intrusion detection systems (IDSs) have been propagated as an alternate method, and are used to secure basic IT infrastructures [3]. Another option being explored for safeguarding hosts or network environments from unknown malicious behaviors is distributed middleware-based approach. This approach can provide security by analyzing log details, traffic analysis, configurations details, and normal user behavior for assessment and intrusion detection [4].

The real security concern after data protection is IDP for cloud computing safety in cloud infrastructures [5]. The new technologies of firewall protection and intrusion detection are providing great safety against assaults by providing cloud system distributed framework added security mechanism. They observe the user's traffic configurations of the system, log files, and upon detection of unknown or suspicious activity, IDS alerts the user or observing console through a message. This message can serve a guide to take preventive measures against the assaults.

In next section, the main security challenges in cloud computing security have been discussed and in further sections, the cloud-based intrusion detection and intrusion prevention techniques and their respective strength and challenges have been analyzed which provide suitable IDP techniques that can be applied for the high level of security against possible intrusion in cloud computing environment.

2 Literature Review

Cloud computing technology has brought some new safety and confidentially challenges which were not present in the conventional computing paradigm. These can be termed as cyber and physical security concerns.

Physical security is concerned with hardware aspects of the system. It is imperative to provide preventive security to incombustibility, continuous electric supplies, and safety measures against common catastrophes like flood, fire, earthquake when a provider infrastructure owns a data center [6]. As cloud computing system services are not free from cybersecurity assaults, cybersecurity measures are also needed to defend the system from the cyber world [7].

2.1 Attacks on Cloud Computing Systems

Following are some examples of known attacks types:

2.1.1 Insider Attack

Insiders are workers, executives, and associates who have the privileged authority of accessing the entire database [8]. Insiders, that may be present or former employees can pose a serious trust issue. They can commit fraud or disclose important information to another party.

2.1.2 Flooding Attack

In this sort of attack, the attacker sends large volume data packets and requests from the remote host to overwhelm the victim machine. Such packets are called as zombie [9]. Attackers use bogus or false network connections to launch an attack. VMs are set up over the Internet for cloud computing prototypes to ensure the safety of the cloud user from DoS and DDoS attacks via zombie.

2.1.3 User to Root (U2R) Attacks

In such type of attack, an invader starts as a normal user and then gain unrestricted access to the entire system by exploiting the vulnerabilities in the system [10]. To counter this sort of attack and to set up trouble-free connections for authorized processes, buffer overflows are applied, but they are not very effective as an intruder can also access information from this flooded data buffers.

2.1.4 Attacks on the Hypervisor

An intruder can control the virtual environment of all the VMs through a successful attack and gain access to the lower layer of the hypervisor [9]. They can do this by attacking and gaining control over the server by adjusting the hypervisor. This type of intrusion is called the zero-day attack. It allows the attackers to take control of hypervisor or other installed VMs [10].

2.2 Techniques for Intrusion Detection in Cloud Computing

These are major IDS techniques in cloud computing environment:

2.2.1 Signature-Based Detection

A set of predefined rules are used to compare with the provided pattern to analyze any intrusion and achieve the high level of accuracy in identifying subtle intrusion but give away minimal false positives. Signature-based detection is a good solution against known attacks, but it falls short when it comes to unknown or variation of known attacks. If it is not properly configured, even small changes in known attacks can negatively affect its efficiency [11]. However, it still widely used because its maintenance is easy and preconfigured rules are easily updated.

2.2.2 Anomaly Detection

Anomaly detection technique identifies unusual activities with respect to normal system behavior [11]. In the event of an attack, the anomaly can only be detected by using a multidimensional approach, which can include techniques like statistical modelling, data mining, and hidden Markov models.

Many events occur in cloud at the network level or system level that makes it hard to use anomaly detection technique for monitoring or controlling purpose as unknown attacks on a cloud system can occur at many different levels. However, anomaly detection techniques are still considered the better options for intrusion detection at various layers of cloud [12, 13].

2.2.3 Artificial Neural Network (ANN)-Based IDS

ANN-based technique [14] for intrusion detection tries to firstly filter data as complete or incomplete and further classifies it as normal or intrusive [15]. The ANN techniques used in such IDS are multilayer feedforward neural networks, multilayer perceptron, and backpropagation [15].

2.2.4 Fuzzy Logic-Based IDS

Fuzzy logic has the ability to provide some sorts of flexible solution to the ambiguous issue of intrusion detection [14]. Fuzzy logic along with ANN can help in prompt recognition of unknown attacks and also reduce training time in cloud [13].

2.2.5 Association Rule-Based IDS

Some attacks are based on previous attacks with minor deviations. Association rules-based IDS can be useful in cloud to generate new signatures based on known attacks. A signature priori algorithm that has the ability to find regular subsets of given attack sets that can be used to detect such signatures or attacks [16].

2.2.6 Support Vector Machine (SVM)-Based IDS

When the dimension of data does not change or deviate the detection outcome, SVM is handy in detecting intrusions with minimal data set available [14].

2.2.7 Genetic Algorithm (GA)-Based IDS

GA-based IDS increases the accuracy of underlying IDS and can be used in cloud as its environment allows to choose best possible parameters or features for intrusion detection. This feature can also be transferred to other methods to improve accurateness of IDS [17].

2.2.8 Hybrid Techniques

When advantages of a combination of two or more of the efficient techniques are employed, it is called hybrid techniques because it effectively avoids drawbacks of other techniques and advantageous use of soft computing practices on traditional cloud-based IDS.

3 Classification of Cloud Computing-Based IDS Systems

Intrusion detection is defined as the field of computer security that aims to detect occurrences of malicious activities, which can be any action intending to disrupt the integrity, confidentiality, or availability of data and services of a system [18]. An IDS comprises of the following features [3]:

- Sensors that produce security alerts at regular intervals.
- The control of sensors are monitored and

The effectiveness of IDS relies heavily on methods of identification, IDS location in the network, and its formation [19] because they can be installed at various locations. Cloud-based IDSs have been classified into these four categories:

3.1 Host-Based Intrusion Detection Systems (HIDS)

A HIDS screens and examines the collected data from particular host machines. This program requires a host machine to run, enabling it to identify intrusion for the machine through information gathered from sources such as file systems worked on, system calls, and network analysis. HIDS looks closely at changes taking place in its host file system, kernel, and activities of the database. In case of any variation in normal behavior, it signals the presence of an attack.

3.2 Network-Based Intrusion Detection System (NIDS)

A NIDS relates present actions with already noted actions as it takes place to identify an intrusion. NIDS uses anomaly and signature-based techniques to detect intrusion and specifically supervises IP and transport layer headers of an individual packet to locate intrusive activities. It tries to identify intrusive activities by analyzing network traffic. The gathered data is correlated with data related to known attacks, and thus, an attack is caught.

3.3 Distributed Intrusion Detection System (DIDS)

A DIDS includes several IDSs (e.g., HIDS, NIDS, etc.). They interact with similar IDS, or with a central server over a wide network, enhancing network supervision. In DIDS, information is collected and converted into a uniform template by the intrusion detection apparatuses and passed on to a central analyzer that combines information from many IDS and scrutinizes it.

3.4 Hypervisor-Based Intrusion Detection Systems

Such IDS is designed mainly for hypervisors which is a base to run VMs. Such IDS allows users to monitor and examine exchanges committed by VMs, by a hypervisor or by the hypervisor-based virtual network. Its main benefit is its access to information, but as being a new technology and its insufficient experience are its drawbacks [20].

4 Comparative Analysis of Cloud Computing IDPS

IDS is a part of IPS and contains all its functionalities, but when it comes to preventing attacks it has the sophisticated capability to take immediate actions. Instead of just identifying an attack, IPS can defend against the attack by changing the attack's composition or altering the security configuration.

In Table 1, various IDS and IPS, their respective strength and challenges have been summarized.

Table 1 Summary of IDS/IPS

Type	Characteristics/strengths	Limitations/challenges
HIDS	• Check for attacks by supervising the network Schedule, file system or system calls of a host computer • Uses same hardware	• Individual installation on VMs, hypervisor, or host machine needed • Only host is supervised against attacks
NIDS	• Network traffic is checked for attacks • Placed only on underlying network • Multiple systems can be supervised simultaneously	• Identifying attacks from encrypted traffic is hard • Assists against external intruders only • Virtual network finds it hard to identify network intrusions
Hypervisor-based IDS	• Interactions between VMs, hypervisors, and virtual network based on these can be checked and examined by the user	• New and hard to comprehend
DIDS	• Uses benefits that it gets from both NIDS and HIDS features	• In centralized DIDS, the central server may be full and hard to handle • Costly communication and computational
IPS	• Safeguards against attacks • NIPS averts network attacks • HIPS averts system-level attacks	• Low accuracy in identifying and averting attacks as compared to IDS
IDPS	• Better at identifying and averting attacks	• Difficult and intricately designed

Separate IDS and IPS configuration have some strength as well as some drawbacks which prevent them from giving comprehensive security. IDS and IPS together are called IDPS, strengthens their effectiveness in identifying possible intrusions. IDPS can halt and inform about intrusions to security supervisors [21]. Thus, this combination can enhance security with proper configuration and management.

5 IDPS Challenges in Cloud Computing

Although there are many benefits offered by cloud computing still due to concerns about security and privacy, consumers do not readily adopt this technology [22]. The lack of visualization and security at the various levels, especially at network and application level, provide huge opportunities for researcher [13, 23].

5.1 Handling with Distributed Datacenters

Distributed IDSs (DIDS) can provide advance warning of an attack and detect intrusive actions as well as track down inside the network. They do this by interacting with an integrated server at the point of their deployment and monitoring the traffic of networks [24]. These IDS are rather easy to manage in a small network. This central approach becomes ineffective and costly in a large network as then it needs extra CPU, but this issue can be resolved by the shared allocation of the memory and CPU.

5.2 Organizational Challenges and Limitations

Risks of cloud computing as outlined in [25] are organizational, technological, legitimacy, and traditional risks. The loss of governance and cloud service termination or failure is policy and organizational risks.

5.3 Security and Trust Issues

Scholars in [26] highlight the privacy issues results from data gathering and checking in cloud. Ensuring data duplication without any security, privacy, and trust issues is required. Security and confidentiality of data is a major consideration that should be taken care in order to win the trust of users.

5.4 Managing the Control Mechanism at Various Cloud Levels

Control mechanism should be addressed and implemented at each level of cloud architecture like VPN establishment, and VMs management is required and can be addressed by applying access control along with suitable cryptographic tools [23]. A different access mechanism is required at various levels of cloud, and selecting a standard mechanism at each level is a challenge for IDPS [27].

5.5 Synching Automated Sensors

In DIDS, synchronizing the automated sensors at different machines is required to detect attacks in the distributed environment. A suitable mechanism is to be devised as well as costs the user due to high bandwidth usage for data exchange.

5.6 Scalability and Handling with Large-Scale Systems

Virtual machines (VMs) are frequently added and removed that requires IDS to be scalable to handle such frequent changes. VMs results in the large-scale system that needs to be handled with minimal human intervention. IDPS need to handle various issues dynamic in nature like load and traffic.

6 Conclusion

Various IDS and IPS techniques have been analyzed in this paper, and their respective strength and limitations have been critically presented. This paper further presents different security challenges and issues to the cloud environment. IDPS challenges in case of cloud computing and different available solutions have been summarized that can be used to overcome such security issues. IDPS can be a very handy and useful tool to provide security solutions to the cloud computing security requirements, and it can resolve the issues if privacy and trust. Among various types of cloud computing-based IDPS techniques, hypervisor-based and distributed IDS are much more suitable and provide a promising solution for the cloud-based environment that can provide the high level of security, but still, complexity and standardization of such systems are major issues that need to be addressed.

References

1. Panko R (2017) The cloud in 2017: trends in security. https://clutch.co/cloud/resources/cloud-computing-security-survey-2017
2. Bokhari MU, Alam S, Hasan SH (2014) A detailed analysis of Grain family of stream ciphers. Int J Comput Netw Inf Secur 6:34–40
3. Mishra P, Pilli ES, Varadharajan V, Tupakula U (2017) Intrusion detection techniques in cloud environment: a survey. J Netw Comput Appl 77:18–47
4. Hatef MA, Shaker V, Jabbarpour MR, Jung J (2017) Zarrabi H (2017) HIDCC: a hybrid intrusion detection approach in cloud computing. Concurrency Comput Pract Experience 30:e4171
5. Samad A, Alam S, Mohammed S, Bhukhari MU (2018) Internet of vehicles (IoV) requirements, attacks and countermeasures. In: Proceedings of 12th INDIACom; INDIACom-2018; 5th international conference on "computing for sustainable global development" IEEE conference, New Delhi (2018)

6. Singh A, Chatterjee K (2017) Cloud security issues and challenges: a survey. J Netw Comput Appl 79:88–115
7. Samad A, Shuaib M, Beg MR (2017) Monitoring of military base station using flooding and ACO technique: an efficient approach. Int J Comput Netw Inf Secur 9:36–44
8. Flynn L, Huth C, Buttles-Valdez P, Theis M, Silowash G, Cassidy T, Wright T, Trzeciak R (2014) International implementation of best practices for mitigating insider threat: analyses for India and Germany (2014)
9. Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M (2013) A survey of intrusion detection techniques in cloud. J Netw Comput Appl 36(1):42–57
10. Roberts JC, Al-Hamdani W (2011) Who can you trust in the cloud? In: Proceedings of the 2011 information security curriculum development conference on InfoSecCD 11 (2011)
11. Ernst J, Hamed T, Kremer S (2017) A survey and comparison of performance evaluation in intrusion detection systems. In: Computer and network security essentials, pp 555–568
12. Modi CN, Acha K (2016) Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review. J Supercomput 73:1192–1234
13. Jouad M, Diouani S, Houmani H, Zaki A (2015) Security challenges in intrusion detection. In: 2015 international conference on cloud technologies and applications (CloudTech), pp 1–11
14. Pandeeswari N, Kumar G (2015) Anomaly detection system in cloud environment using fuzzy clustering based ANN. Mobile Netw Appl 21:494–505
15. Ibrahim LM (2010) Anomaly network intrusion detection system based on distributed time-delay neural network (DTDNN). J Eng Sci Technol 5(4):457–471
16. Buczak AL, Guven E (2016) A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutorials 18:1153–1176
17. Desai AS, Gaikwad DP (2016) Real-time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA. In: 2016 IEEE international conference on advances in electronics, communication and computer technology (ICAECCT)
18. Morin B, Mé L, Debar H, Ducassé M (2009) A logic-based model to support alert correlation in intrusion detection. Inf Fusion 10:285–299
19. Oktay U, Sahingoz OK (2013) Proxy network intrusion detection system for cloud computing. In: 2013 the international conference on technological advances in electrical, electronics and computer engineering (TAEECE)
20. Rahim ER (2012) Information security in the internet age. In: Beyond data protection, pp 157–186
21. Scarfone KA, Mell PM (2007) Guide to intrusion detection and prevention systems (IDPS)
22. Das SK, Kant K, Zhang N (2012) Handbook on securing cyber-physical critical infrastructure. Morgan Kaufmann, San Francisco, CA
23. Shuaib M, Samad A, Siddiqui ST (2017) Multi-layer security analysis of hybrid cloud. In: 6th international conference on system modeling & advancement in research trends. IEEE, pp 526–531
24. Platonov VV, Semenov PO (2017) An adaptive model of a distributed intrusion detection system. Autom Control Comput Sci 51(8):894–898
25. Gurkok C (2013) Chapter 6—Securing cloud computing systems. In: Vacca JR (ed) Computer and information security handbook, 2nd edn. Morgan Kaufmann, Boston, pp 97–123
26. Khorshed MT, Ali AS, Wasimi SA (2011) Trust issues that create threats for cyber attacks in cloud computing. In: 2011 IEEE 17th international conference on parallel and distributed systems
27. Manvi SS, Shyam GK (2014) Resource management for Infrastructure as a Service (IaaS) in cloud computing: a survey. J Netw Comput Appl 41:424–440