Suneeta Mohanty *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 3, March- 2018, pg. 38-43 **ISSN: 2321-8363**
Impact Factor: 5.515

CIA Triad for Achieving Accountability in Cloud Computing Environment

Suneeta Mohanty[1], Mrinmoy Ganguly[2], Prasant Kumar Pattnaik[3]

School of Computer Engineering, KIIT University, Bhubaneswar, suneetamohanty@gmail.com

Abstract

Cloud Computing Environment fulfils the computational requirements of individual, small organizations and large organizations with minimum cost. Generally, the data are the asset of the owners and the owner always concern about the security issue which they generally face while storing their data in the cloud. Once the data are stored in cloud, user loses his control over the data. Thus, the major security issues are to maintain data confidentiality(C), integrity(I) and availability(A) which forms the CIA triad. If CIA triad can be implemented in Cloud Computing Environment then Cloud Service Provider will be held accountable for cloud user's data confidentiality, integrity and availability. This paper addresses the availability issue which is not addressed in existing research paper to achieve accountability in Cloud.

Keywords: Confidentiality, Integrity, Availability, Cloud Service Provider (CSP), Denial of Service(DoS).

1. Introduction

Cloud Computing provides platform independent infrastructure where one can do various types of task smoothly without worrying about the large computational resources locally. As specified by Mohanty, S., et al (2017) the required computational needs are provided in terms of Virtual Machines(VM) in pay per use basis to cloud users. Data stored in cloud generally resides in a shared environment along with the data from other users in CCE. In agreement with Buyyaa, R., et al (2009), Infrastructure elements for pay per use, service level agreement and authentication control are generally provided by CSP. According to Sundareswaran, S., et al (2011),there exist various security issues related to data access, allocation strategies, various web attacks and information flow which became the major concerns in the era of Internet. Maintaining integrity is the way to secure sensitive data that is outsourced from different end user. As per Chakraborty, T. K. ,et al (2013) Cloud user's data which has not been used for long time can be discarded by the Cloud Service Providers for more space on data centre. According to Mohanty, S., et al (2014) Auditing for regulation or compliance, Auditing for Risk and Governance, Auditing for security, Database Auditing, Service level agreements (SLAs) Auditing & Third Party Storage Auditing Service Provider can be used to achieve accountability.CIA Triad comprises of confidentiality, integrity and availability plays an important role to address various security issues as discussed below:

Confidentiality:- Confidentiality of user's data is said to be maintained if user's data won't be leaked to unauthorized entity.
Integrity: - Integrity of user's data is said to be maintained if the contents remain same after outsourcing to Cloud Service Provider.

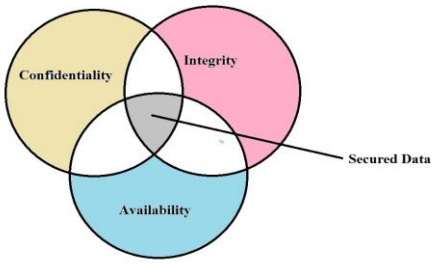

Figure1: CIA Triad

Availability:- Availability refers to ensure the authorized user will get access the information as and when required. Availability ensured by the maintenance of hardware as well as maintaining the operating system in proper functioning where any kind of software conflict doesn't take place.

If a Cloud Service Provider is providing confidentiality, integrity, and availability then that environment is always trustworthy environment for any cloud user as the data are secured as shown in Figure 1. So accountability can be achieved with the help of CIA triad in CCE.

This paper is organized as follows: The Section 2 discusses the literature review over some research work. The section 3 discusses attack on availability that is Denial of Service(DoS) attack and also discusses different defense strategies for DoS attack. Finally, the section 4 concludes our work.

2. Literature Review

Yu.S et al.(2010) addressed the issues related to defining and enforcing access policies. In this paper, they have applied KP-ABE , proxy re-encryption and lazy re-encryption algorithm to maintain data confidentiality and scalability. Through this scheme data owner can delegate the computational overhead to cloud servers. Proposed scheme also achieves user secret key accountability.

Nakahara.S et al.(2012) explained the requirements for link log data for multiple services which are supported by the non-local server and trace cloud-based services. This paper also discusses the methods to apply cryptography to achieve log data accountability.

Zhang.R, Chen.P(2013) presented a cryptographic access control scheme to achieve security and flexible accesscontrol. This cryptographic access control scheme called as CS-CACS was based on encryption (CP-ABE) and implemented on the HDFS workstation. The proposed scheme achieves confidentiality and secret key accountability.

Chandra.R, et al.(2013) introduced a framework to focus on data correctness, authentication and authorization for outsourced data. Also this framework supports data integrity and access control through tracking.

Zheng.X, et al.(2013) presented an extensive research to discuss various approaches adopted by service providers to achieve accountability. This paper also discusses various issues related to data confidentiality, privacy and accountability framework.

Chraibi.M et al.(2014) presented an architecture of Policy-Based Security Middleware as a Service .Through this architecture they have enforced confidentiality and integrity in each level of cloud in terms of policy to achieve accountability.

Hande .S et al.(2015), has done an extensive research on different security issues in Cloud Computing like integrity, confidentiality, transparency, accountability, availability, assurance. They have analyzed various models like RSA based storage security model, data security model, privacy manager and Cloud Information Availability framework to achieve accountability in cloud.

Timothy.D et al.(2017) proposed a hybrid cryptosystem to handle the different security issues in the Cloud Computing by combining the symmetric and asymmetric algorithm. This hybrid cryptosystem achieves data confidentiality by using symmetric algorithm(Blowfish) and data achieves authentication by using asymmetric algorithm (RSA). It also achieves data integrity by using SHA-2 algorithm.

Table 1: Comparison of existing accountability schemes for Cloud Computing Environment

Accountability Scheme	Confidentiality	Integrity	Availability
Yu.S et al.(2010)	**YES**	NO	NO
Nakahara.S et al.(2012)	NO	**YES**	NO
Zhang.R, Chenl.P.(2013)	**YES**	NO	NO
Chandra.R, et al.(2013)	NO	**YES**	NO
Zheng.X, et al.(2013)	**YES**	NO	NO
Chraibi.M et al.(2014)	**YES**	**YES**	NO
Hande .S et al.(2015)	NO	**YES**	NO
Timothy.D et al.(2017)	**YES**	**YES**	NO

Existing accountability schemes partially implemented CIA triad as shown in Table 1 to achieve accountability in cloud. Availability issue is not addressed by any of the existing scheme. Thus in this paper we have discussed some methods through which the availability issue can be addressed in CCE to achieve accountability.

3. Denial of Service(DoS) Attack

In DoS, the attacker uses the large number of host for the attack in the server by sending the request continuously in the server as shown in figure2. Every server has the limitation for handling the request at any particular point of time. This is the major drawback of any server and attacked access this advantages, the attacker sends huge number request so that server gets slow and valid user cannot access the data. The main target of the attacker is to compromise the Availability of cloud computing. Generally, attacker tries to degrade the performance of the system. The illegitimate user consumes a lot of communicational bandwidth, processor speed, disk space so that the system gets slow down and authorized user cannot access the resources as and when required. Thus DoS attack is an attack on availability. If we can defense DoS attack then we can address the availability component of CIA triad to have an accountable CCE.

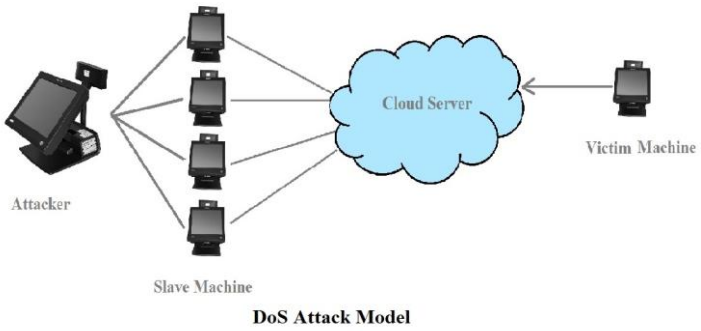

Figure 2: DoS Attack Model

4. Defense strategies for Denial of Service(DoS) Attack

Defense strategy for DoS includes prevention and attack mitigation. DoS attack can be prevented by blocking the path where the attacker already attacked or through continuous monitoring. These are the theoretical aspect by which we can defense the DoS attack, although it is very difficult to stop DoS attack. We can prevent the DoS attack in CCE to achieve availability by enforcing Service Level Agreement and the attack can be mitigated through Virtual Machine Monitor, Intrusion Detection System, Firewall and trace back with cloud filter as discussed below.
As per Latanicki, J. et al.(2010) , the Dos attack can be resisted through the following steps:

1. For determining its intensity we have to quickly detect the attack.
2. Try to alleviate the outcome of the attack up to a maximum.
3. If step 2 is not possible, then move the virtual machine to safe physical servers.
4. To evaluate the step 3 high network bandwidth will be required.
5. Countermeasure to the attack of their rank from very basic to higher.

Service Level Agreement (SLA)
A legal contract between the user and the service provider about the level of services that should be provided by the service provider to end user. DoS attack should be prevented by making proper service level agreement (SLA). Kandukuri et al.(2009) explained the necessity of standardized SLA between the cloud user and the cloud service provider for maintaining integrity, confidentiality, and availability.SLA ensures that any malicious should not attack any user's sensitive data. SLA also focuses on proper encryption of data while user sharing their information.

Virtual Machine Monitor (VMM)
VMM is software or hardware which is used for creating and running the virtual machine. In any computer if VMM runs virtual machine (one or more) then that machine is known as host machine, every virtual machine is known as guest machine. According to Zhao, S . et al.(2009) ,VMM is composed of a detector, a duplicator, and tagger. The main target is to compute the available resources and monitor for detecting the attacker.

Intrusion Detection System (IDS):- IDS is a kind of software application or devices which is used to monitor malicious activity in systems or a network or policy violations. Intrusion Detection System can be used in the virtual machine. According to Bakshi et al.(2010), IDS block the attacker address by analyzing the outbound and inbound traffic. Generally, IDS are of two types: Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS).

HIDS: Host-based Intrusion Detection System is applied to the individual host which monitors the transmission and receiving of packets from devices and informs the administrator if any kind of mistrustful activity is detected.

NIDS: Network-based Intrusion Detection Systems issued for all the traffic inside a specific network. NIDS analyses the passing traffics on the specific network and informs the administrator if any kind of mistrustful activity is detected.

Firewall:- Firewall is a security system used for controlling and monitoring the network traffic. Modi et al.(2013) described the Firewall as the first stage of defense in the cloud computing. By the help of header information such as source IP and destination IP and port address firewall investigate and filter the packet with the help of state table. Ismail et al.(2012) proposed a framework where the virtual switch and internet gateway accesses the virtual machine which contains web services in CCE. In this framework, virtual switch uses a matrix of routine traffic to know the attack sources for finding the IP address. Then that IP address is blocked by virtual switch. Liu et al.(2014) has introduced Clusterized firewall for cloud computing. The author divided the cloud services into application layers where all servers are grouped into a cluster. Every cluster holds a firewall, according to the arrival rate of application the firewall of cluster protects and guarantees QoS for valid users.

Trackback with Cloud filter:- Yang et al. (2012) proposed a SOA-based tracing approach(SBTA) to trace the source of DoS attack through cloud filter. Generally it is located before the web server and all the service requests are noticed by SBTA. This algorithm performs reconstruction of the path to find the source of DoS attack. Once the source of attack is detected, cloud filter filters the attack message.

5. Conclusion

In Cloud Computing Environment, security is the major concerns of all types of stakeholder. The Cloud Service Provider stores user's data in a shared environment which may lead to security issues like confidentiality, integrity and availability of user's data. The Cloud Service Provider is accountable for loss of confidentiality, integrity and availability of stored data. Thus, in this paper we have discussed how important it is to implement the CIA Triad in CCE to achieve accountability.

References

[1] Timothy, D., Santra, A.(2017) "A Hybrid Cryptography Algorithm for Cloud Computing Security" *in International conference on Microelectronic Devices, Circuits and Systems (ICMDCS).*

[2] Hande, S.A. , Mane, S.B. (2015) "An Analysis on Data Accountability and Security in Cloud", *in International Conference on Industrial Instrumentation and Control (ICIC)*, pp. 713-717.

[3] Chandar, R. , Kavitha, M.S. , Seenivasan, K. (2013) "A Three Tier Scheme For End To End Security In Cloud Computing", in *International Conference on Advanced Computing and Communication Systems (ICACCS -2013), Dec. 19 – 21, 2013, Coimbatore, INDIA.*

[4] Zhang, R., Chen, P.(2012), "A Dynamic Cryptographic Access Control Scheme in Cloud Storage Services" , *8th International Conference on Computing and Networking Technology (INC, ICCIS and ICMIC)* , pp.50-55.

[5] Nakahara, S. , Ishimoto, H. (2012), "A Study on the Requirements of Accountable Cloud Services and Log Management"

[6] Zheng, X., Ye, H., Tang, C., Rong, C., Chen, G. (2013), "A Survey on Cloud Accountability", in *International Conference on Cloud Computing and Big Data*, pp. 627-632.

[7] Pearson, S. et al. (2012), "Accountability for Cloud and Other Future Internet Services", in *IEEE 4th International Conference on Cloud Computing Technology and Science*, pp. 629-632.

[8] Yu, S., Wang, C.,Ren, K., Lou, W.(2010), "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", *in Proceedings IEEE INFOCOM.*

[9] Kandukuri, B.; Paturi, V.; Rakshit, A(2009). "Cloud Security Issues". *In Proceedings of the 2009 IEEE International Conference on Services Computing, Bangalore, India,* pp. 517–520.

[10] Latanicki, J.;Massonet, P.; Naqvi, S.; Rochwerger, B.; Villari,M(2010). "Scalable Cloud Defenses for Detection, Analysis and Mitigation of DDoS Attacks", *In Towards the Future Internet; IOS Press: Amsterdam, The Netherlands,* pp. 127–137.

[11] Zhao, S.; Chen, K.; Zheng, W(2009). "Defend Against Denial of Service Attack with VMM", *In Proceedings of the 2009 Eighth International Conference on Grid and Cooperative Computing, Lanzhou, China*, pp. 91–96.

[12] Modi, C.; Patel, D.; Borisaniya, B.; Patel, H.; Patel, A.; Rajarajan, M(2103). "A survey of intrusion detection techniques in Cloud", J. Netw. Comput. Appl., 36,pp. 42–57.

[13] Bakshi, A.; Dujodwala, Y.B(2010). "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine", *In Proceedings of the 2010 Second International Conference on Communication Software and Networks, Singapore*, pp. 260–264.

[14] Yang, L.; Zhang, T.; Song, J.;Wang, J.S.; Chen, P.(2012) "Defense of DDoS attack for cloud computing", In proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, Volume 2, pp. 626–629.

[15] Ismail, M.N.; Aborujilah, A.; Musa, S.; Shahzad, A. (2012)"New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment" in Int. J. Comput. Sci. Secur., 6, 226–237.

[16] Liu, M.; Dou,W.; Yu, S.; Zhang, Z(2014). "A Clusterized firewall framework for cloud computing", *In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia,* 10; pp. 3788–3793.

[17] Buyyaa, R. Yeoa, C.S. , Venugopala, S., Broberga,J., Brandicc, I.(2009) "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", in *Future Generation Computer Systems*, Volume 25, Issue 6, pp. 599-616.

[18] Jensen, M., Gruschka, N., Herkenhoner, R., Luttenberger, N.(2007)"SOA and Web Services: New Technologies, New Standards – New Attacks", in *5th European Conf. on Web Services*, 26, pp. 35-44.

[19] Mohanty, S., Pattnaik, P.K. , Mund, G.B.(2014) "Framework For Auditing In Cloud Computing Environment",in *Journal of Theoritical And Applied Information Technology*, Vol.65, pp.261-267.

[20] Sundareswaran, S., Squicciarini, A., Lin, D., Huang, S.(2011) "Promoting Distributed Accountability in the Cloud", in *4th IEEE International Conference on Cloud Computing*, pp. 113 - 120.

[21] Chakraborty, T. K. , Dhami, A., Bansal, P., Singh, T.(2013) "Enhanced public auditability & secure data storage in cloud computing", in *IEEE 3rd International Advance Computing Conference*, pp.101-105.

[22] Mohanty, S., Pattnaik, P.K. , Mund, G.B.(2017) "Privacy Preserving Auction Based Virtual Machine Instances Allocation Scheme for Cloud Computing Environment", in *International Journal of Electrical and Computer Engineering*, Vol.7(5), pp.2645-2650.

