Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 8, Issue. 1, January 2019, pg.16 – 20

An Analysis and Survey of Security Techniques for Cloud Computing

Manish Kumar
Research Scholar
Bhagwant Institute of Technology, Muzaffarnagar, UP, India
er.manishdba@outlook.com

Shivani Chauhan
Assistant Professor
Bhagwant Institute of Technology, Muzaffarnagar, UP, India
shivanichauhanbit@gmail.com

Ajay Singh
Assistant Professor
Bhagwant Institute of Technology, Muzaffarnagar, UP, India
ajaysingh221985@gmail.com

Abstract: The cloud computing is the type of network in which no central controller is present due to which security is the major issue of the network. The security attacks affect network performance in terms of certain parameters. This research work is related to detection of zombie attack in cloud computing. In the zombie attack, the clones of the virtual machine are created which interact with the cloud server. The various security enhancement techniques are reviewed in this paper in terms of certain parameters

KEYWORDS: Cloud computing, zombie, network performance

Introduction

Cloud Computing is the environment which provides on-demand and convenient access of the network to computing resources like storage, servers, applications, networks and the other services which are efficient. Cloud is a centralized data in which a user, who is actually the client in cloud, can retrieve and modifies the stored data. Cloud is a design, where Cloud Service Provider (CSP) provides services to the user on demand [1]. It means that the user or the client who is using the service of cloud has to pay for whatever he/she is using or being used and served. It is a technique which gives a huge amount of applications under different topologies and each topology gives some new specialized services. To secure the user data, enterprises use the security mechanism, such as USB port control, Full Disk Encryption (FDE), etc. But, are these mechanisms good enough to secure the user data in cloud? The systems which runs 24*7 or all the time the above solutions are not effective that much. They cannot prevent the attackers to access data. Cloud Computing is the environment which provides on-demand and convenient access of the network to a computing resources like storage, servers, applications, networks and the other services which can be released minimum efficiency way [2]. Cloud Service Provider plays an important role in cloud. Users need not to buy software licenses or hardware to access any service. Users demand services from CSP or ISP and can access the internet services. This reduces the customer's expenditure and called "pay-per-use" service. There are several types of clouds. In Public Cloud, resources allocated are publically. Applications in this cloud are on pay-per-use basis. Public clouds can be managed by government organizations or business. Private Cloud: In this cloud, resources are limited and used within an organization. It is more secure as employees in an organization can access the particular data only [3]. In Hybrid Cloud, there is a combination of both public and private cloud. The services within the organization are control by the customer and resources which need to be delivered externally are controlled by the service provider. Community Cloud is used by those organizations which have same concerns like security requirements; mission or policy. This is managed by organizations within a community or by the third party auditor. Network security, information security and many other security types like the computer security together make the term "Cloud Security". Because it consist all of the security mechanism given above. It gives the broad set of technologies, policies and controls that are used to secure the data and applications exist with the cloud computing environment [4]. Security is the most concerning point to any service. There are many types of security issues as we discussed above are there in cloud computing. Due to these issues, attacks are possible in cloud. Many security professionals have argued that the cloud is more vulnerable to Denial of Service (DoS) attacks because this is shared by larger number of users which can makes DoS attacks much more dangerous. In Side Channel attacks, an attacker could attempt to compromise the cloud through placing a malicious virtual machine in close proximity to a target the cloud server and then exploiting a side channel attack. Authentication is the weakest point in virtual services and hosted and is frequently targeted. There are many different kind of ways to authenticate users for example based on what a person knows, has, or is [5]. The technology used to secure the authentication process and the scheme used are a frequent target of attackers. Man-in-the-middle cryptographic attack is carried out when an attacker places himself between two communication parties. At anytime attackers can place themselves in the communication's path there is the possibility that they can intercept and modify communications message. An attack is where a user between the receiver and sender of information and sniffs any data being sent. In some cases users may be sending unencrypted information which means the man-in-the-middle (MITM) can obtain any unencrypted data information. On other hand a user may be able to obtain information from the attack but have to unencrypted the information before it can be read [6]. One of the advance attacks in cloud computing environment that degrades the network's performance and network throughout is known as the Zombie attack. Malicious nodes act as one of the connected users called zombie. Without any awareness of the system user, a system that is inserted with a program puts it under the malicious user's control. Malicious users use zombie for DoS or DDoS attacks launching. The illegitimate user sends the command to the zombie by an open communication port [7]. For blocking the route of the site and keep genuine users from having access to the site the zombie system sends a huge amount of packets of worthless data to a targeted website on command. To understand the flow of information sent out through the zombies, the result of the system received information used time, resource and traffic sent to the website mixed-up.

Literature Review

Rakshitha C M, et.al (2016) presented that due to small loop holes in the cloud security led to huge losses in business, as one of the major aspect in the field of network security was Cloud Security [8]. Without the interruption of user's ongoing applications and cloud services, the cloud security provider ensured that the network intrusion detection and prevention framework in a virtual networking environment. Side by side it was very beneficial if cloud service provider gives both security and utilization techniques of the cost. In this proposed approach, six approaches were surveyed in which each surveyed approach considered advantages and disadvantages also in this paper. IS an open problem for future research enhanced the approaches performance.

Andrey V. Smirnov, et.al (2016) studied that the part of the security component protecting Open Stack cloud computing platform against DDoS attacks was achieved from the results of the design of the network data processing module [9]. The security policies strictly regulated the list of used and running software of the clients whose latter is important. For the network traffic processing the current version of the module used the Net Flow sensor as a sensor gathering information that was de facto industry standard. The developed module was utilized in the cloud systems the networking architecture of which permits the usage of Net Flow sensors which is the fact. Exceeding modern powerful DDoS attacks the performance evaluation results reflected that the developed module was able to process network traffic volumes.

Mrs. Asma A. Shaikh, (2016) proposed an International Collection of Hardware and Software from hundreds of thousands of private and public computer network is known as cloud. Giving permission of the digital data for sharing and distribution at very low cost and very fast for usage refers to the cloud which is a global platform [10]. Due to organized criminals, terrorist and hostile nations would observe this as a new frontier to try to steal confidential information, interrupt services and route damage to the enterprise cloud computing network viruses, worms, hackers and cyber attacks enlarged. XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks, and its potential countermeasures are the issues of cloud computing security in this proposed approach. It appears that the security concern of cloud computing is most important in this era as always tried by the attacker for searching new way to attack cloud.

Aryachandra A A, et.al (2016) ports scan, IP spoofing, ping of death, and packet sniffing are the typesof attacks common in network security. From both inside and outside of the cloud computing infrastructure the possibility attacks can occur [11]. The best solution for the detection of the attack is shown by the several studies was Intrusion Detection System (IDS). Evaluation of the performance memory and CPU usage and IDS server placement scenario for the successful detection was presented in this paper. Three types of placement IDS server were proposed in this work. IDS server was placed inside the cloud server which was the first type of placement. Secondly, IDS placed was separated from the cloud server and the last types were IDS server both inside and separate cloud server was placed. Within and from outside cloud server each scenario was tested through the attacks. IDS dependent on the major attacks within this paper summarized IDS server placement.

Marwane Zekri, et.al (2017) presented that through the attackers the underlying technologies and legacy protocols considers bugs and vulnerabilities which could open doors for intrusion. One of the most frequent that inflicted serious damage and affected the cloud performance is the Attacks as DDoS (Distributed Denial of service) [12]. A major portion of the network bandwidth of the victim cloud infrastructure or consume much of the servers time might by occupied through this. On the basis of the C.4.5 algorithm to mitigate the DDoS threat a DDoS detection system was designed in this work. Generation of a decision tree for performing automatic, effective detection of signatures attacks for DDoS flooding attacks and also coupled with signature detection techniques were involved in this algorithm. Other machine learning techniques and the obtained results were compared for validating the system.

Himadri Shekhar Mondal, et.al (2017) proposed helpful for the detection of Distributed Denial of Service (DDoS) attack in cloud computing environment the author presented a Fuzzy based mechanism. If it is detected at first, then the attack might decrease as DDoS attack becomes powerful with the passing of time [13]. Using Fuzzy logic it was focused on attack detection mechanism to secure the cloud environment. In this paper it was presented Attack in cloud computing may be minimized but early detection was required. For making the system vulnerable the attackers always tried to discover a way to bypass the security system. For the prevention of the new discovered attacks the security system might require more research. To provide the better secure performance for the users and in future adding more variable utilizing the Fuzzy system that was more reliable and dynamic it is possible to acquire more fruitful result.

MGM Mehedi Hasan et.al (2017) due to these attacks can reveal crucial data or create DoS was important to defend against co-resident attacks. Its mitigation is highly challenging due to the nature of the co-resident attack. Malicious VM needs to be beyond a reasonable doubt was detected [14]. With an undue consequence or a malicious user may escape the due punishment a benign suffered. According to a conservative approach will not result in a desired outcome since a VM can be either malicious or benign. An appropriate choice as an attacker detection approach was the proposed CAMP game. While keeping the impact on the benign VMs limited solution to the CAMP game provides optimal strategies to detect and defend the malicious has been proved by the evaluation. For further evaluation the efficacy of the proposed defense mechanism performed real experiments in the future work.

Vishal, et.al (2018) proposed a policy premium payment application which aimed to secure the financial transactions being performed over the Internet services including cloud. For performing various transactions, the web applications are considered to be secure [15]. In order to deploy a financial transaction application, the Google App engine is utilized. It was successfully possible to design, develop and deploy the Policy Premium Payment application in J2EE. An application is hosted on the web server in order to provide services to the open source community. Attackers mainly target weak point of applications which is authentication of cloud computing. Here, for checking the security of applications, several authentication attacks were studied.

Authors Names	Year	Description	Outcomes
Rakshitha C M,	2016	In this proposed approach, six approaches were surveyed in which each surveyed approach considered advantages and disadvantages also in this paper.	IS an open problem for future research enhanced the approaches performance.
Andrey V. Smirnov	2016	For the network traffic processing the current version of the module used the Net Flow sensor as a sensor gathering information that was de facto industry standard. The developed module was utilized in the cloud systems the networking architecture of which permits the usage of Net Flow sensors which is the fact.	Exceeding modern powerful DDoS attacks the performance evaluation results reflected that the developed module was able to process network traffic volumes.
Mrs. Asma A. Shaikh,	2016	XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks, and its potential countermeasures are the issues of cloud computing security in this proposed approach.	It appears that the security concern of cloud computing is most important in this era as always tried by the attacker for searching new way to attack cloud.
Aryachandra A A,	2016	From the server cloud, or placed in a cloud server IDS can be placed separately. A major influence on the CPU and RAM usage on the cloud server was on IDS placement in the server cloud and separated placement of cloud server.	IDS are dependent on the major attacks within this paper summarized IDS server placement.
Marwane Zekri,	2017	On the basis of the C.4.5 algorithm to mitigate the DDoS threat a DDoS detection system was designed in this work.	Other machine learning techniques and the obtained results were compared for validating the system which showed that the proposed technique was better.
Himadri Shekhar Mondal,	2017	In this paper it was presented Attack in cloud computing may be minimized but early detection was required. For making the system vulnerable the attackers always tried to discover a way to bypass the security system.	To provide the better secure performance for the users and in future adding more variable utilizing the Fuzzy system that was more reliable and dynamic it is possible to acquire more fruitful result.
MGM Mehedi Hasan	2017	An appropriate choice as an attacker detection approach was the proposed CAMP game.	While keeping the impact on the benign VMs limited solution to the CAMP game provides optimal strategies to detect and defend the malicious has been proved by the evaluation.
Vishal,	2018	A policy premium payment application was proposed which aimed to secure the financial transactions being performed over the Internet services including cloud.	Attackers mainly target weak point of applications which is authentication of cloud computing. So, for checking the security of applications, several authentication attacks were studied.

Conclusion

In this paper, it is concluded that due to decentralized nature of cloud environment various type of security attacks are possible which affect network performance. In this paper, various security enhancement techniques are reviewed in terms of certain parameters. In future novel technique will be proposed for the isolation of zombie attack in cloud computing

References

[1] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, 2013. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications,* Volume 4, Issue 5.

[2] Jian Yu, Quan Z. Sheng, Yanbo Han, 2013. Introduction to special issue on cloud and service computing. *Service Oriented Computing and Applications,* Volume 7, Issue 2, pp 75–76.

[3] Joel Gibson, Darren Eveleigh, Robin Rondeau and Qing Tan, 2012. Benefits and Challenges of Three Cloud Computing Service Model. *Fourth International Conference on Computational Aspects of Social Networks (CASoN).*

[4] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, 2012. Cloud Computing Security: From Single to Multi-Clouds. *45th Hawaii International Conference.*

[5] Anas Bouayad, Asmae Blilat, Nour el houda Mejhed, Mohammed EL. Ghazi, 2012. Cloud computing: security challenges. *Colloquium in Information Science and Technology*.

[6] Sanjoli Singla, Jasmeet Singh, 2013. Cloud Data Security using Authentication and Encryption Technique. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* Volume 2, Issue 7, pp.- 2232-2235.

[7] Singh, A., & Shrivastava, M., 2012. Overview of Attacks on Cloud Computing. *International Journal of Engineering and Innovative Technology (IJEIT)*, volume 1, issue 4, pp- 321-323.

[8] Rakshitha C M, Ashwini B P, 2016. A survey on Detection and mitigation of zombie attacks in cloud environment. *2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*

[9] Andrey V. Smirnov, Konstantin A. Borisenko, Evgenia S. Novikova, 2016. Network Traffic Processing Module for Infrastructure Attacks Detection in Cloud Computing Platforms. *XIX IEEE International Conference on Soft Computing and Measurements (SCM)*

[10] Mrs. Asma A. Shaikh, 2016. Attacks on Cloud Computing and its Countermeasures", International conference on Signal Processing. *Communication, Power and Embedded System (SCOPES)*

[11] Aryachandra A A, Fazmah Arif Y, Novian Anggis S, 2016. Intrusion Detection System (IDS) Server Placement Analysis in Cloud Computing. *Fourth International Conference on Information and Communication Technologies (ICoICT)*

[12] Marwane Zekri, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi, 2017. DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments. *3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*

[13] Himadri Shekhar Mondal, Md. Tariq Hasan, Md. Bellal Hossain, Md. Ekhlasur Rahaman and Rabita Hasan, 2017. Enhancing Secure Cloud Computing Environment by Detecting DDoS Attack Using Fuzzy Logic. *3rd International Conference on Electrical Information and Communication Technology (EICT)*

[14] MGM Mehedi Hasan and Mohammad Ashiqur Rahman, 2017. Protection by Detection: A Signaling Game Approach to Mitigate Co-Resident Attacks in Cloud. *IEEE 10th International Conference on Cloud Computing*

[15] Vishal, Rahul Johari, 2018. SOAiCE: Simulation of Attacks in Cloud Computing Environment. *8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*