Security in Cloud: Attacks & Prevention Techniques

Neha Khandelwal
M.Tech Student, KITE, Jaipur

Chetan Kumar
Asst. Prof, KITE, Jaipur

Abstract - Cloud computing is considered as the future of IT organizations. In weigh against to conventional solutions in which the IT services are under proper physical logical and personnel controls, it moves all the computing resources to the centralized large data centers, so users can enjoy services in a large scale on demand. Chiefly small and medium-size organizations can manage their projects by using cloud-based services and also able to achieve productivity enhancement with limited budgets. But, apart from all of these benefits, it may not be fully trustworthy. Cloud Computing do not keep data on the user's system, so there is a need of data security. The user pays progressively attention about data security due to this off-side storage of data on cloud computing. In this paper, all possible threats to security in cloud computing are presented.

Keyword: Cloud Computing, Distributed data processing, Security mechanism.

I. INTRODUCTION

The fundamental concern in cloud computing environments is to establish and provide security around isolation and multi-tenancy, giving clients and organizations more relieve besides the "trust us" proposal of clouds [1]. There is a survey reported that classifies security issues and threats in cloud computing based on the character of the service delivery infrastructure or environment of the cloud computing system [2]. Service delivery model is the basic aspects that should be considered for any comprehensive survey on the cloud computing security model. Security at many different levels like Application level, Network level, as well as Host level is compulsory to keep the cloud efficient up as well as running continuously. Various types of security threats may occur in accordance with different levels. The rest of section will describe them:

1.1 Basic Security

Web 2.0, a basic technology in the direction of enabling the utilization of Software-as-a-Service (SaaS) relieves the client or users of cloud from tasks like installation and maintenance Web 2.0 has been used worldwide from its beginning. And as the client community that are using Web 2.0 technology is increasing, the security of cloud data has become further important than ever for such an environment [3].

1.1.1 SQL injection attack is the one of attack in which the malicious code is include into the standard SQL code and using this the attackers finally gain the unauthorized access to the users database and also he becomes able to retrieve sensitive data and information of user. In some cases the input data of attacker is misunderstood by web-sites they treated it as the user data and allows attacker to access by SQL server and this situation lets the hacker to have know-how of functioning of the web-site and how to make changes into it. There are various types of techniques are like avoid the usages of dynamical-generated-SQL in code, use the filtering techniques for sanitize users input to check SQL injection attack.

1.1.2 Cross Site Scripting (XSS) attacks, this attack injects malicious scripts or code into Web contents has become much popular since the beginning of Web 2.0. The website can be known as dynamic or static based on the types of services provided. Static websites generally don't experience the security threats while the dynamic website does because their dynamism property in providing user multi-fold services.

1.1.3 Man in the Middle attacks (MITM). MITM is the class of attack that is much popular in the software-as-a-service (SaaS) environment. In these types of attack, an attacker tries to intrude in ongoing communication between the sender and the client to inject false or fake information and to get knowledge of important data or information communicated between them. There are various types of tools that implementing strong encryption technique such as Dsniff, Wsniff, Cain, Airjack, Ettercap, etc. have been implemented and developed for provide safeguard against

these threats. A detailed survey and study for preventing the man in the middle attacks is presented in [4]. Some important aspect such as evaluation of software-as-a-service-security, server security processes, separate endpoint and evaluating-virtualization at the end-point have been elaborated by Eric Ogren in an article which is give at Security.com to attempt to stop traditional security flaws [5].

1.2 Network Level Security

Networks can be classified into several types such as shared network, non-shared networks; private or public network, small area network or large area network and every one of them have a verity of security issues and threat. In order to ensure network security given points like integrity and confidentiality in the network, proper access mechanism as well as maintaining the security against any external third-party issue or threats must be considered when providing network-level security.

There are many problems are associated with network level security such as: Sniffer attacks, DNS attacks, issues of reused IP address and Distributed-Denial-of-Service-attacks (DDoS) etc.

1.2.1 DNS Attacks

The Domain-Name-Server (DNS) server basically performs the task of translation of any domain name to corresponding IP address. But there are many cases when having called server by name, the client have been routed to other evil cloud in its place of the server he asked for. Even though using a DNS security measures such as Domain-Name-System-Security-Extensions (DNSSEC) always reduces the overall effects of DNS security threats and issues but still there are many cases when these security solutions and measures are proved to be not enough when the connection between a the sender and the receiver is getting rerouted by an evil connection [6].

1.2.2 Sniffer Attacks

There are such types of application that launch attack by capture the packets when they flowing in the network and if the information that is transferred by these packets is not use encryption, then it can be read as well as there is a chance that the information that flowing through the network can be captured or traced. A sniffer program, through the (NIC) ensures that data or traffic correlated to other systems which also exist on the network is also gets recorded. This can achieve by placing the Network Interface Card (NIC) in promiscuous mode then in promiscuous mode it will track all information, transmitted on the same network.

A malicious-sniffing-detection platform that is based on Address Resolution Protocol (ARP) and Round Trip Time (RTT) , that is basically used to detect a sniffing-system that is running on a network [7].

1.2.3 Issue of reused IP addresses

Every node of the network is has an IP address hence an IP address is definitely a finite quantity. There are a large number of cases that are related to reuse of IP address issue have been observed. When a client or user moves out to the network then IP address that is associated with him earlier is assigned to new users. This sometimes may be risks to security of the new user because there is a always certain time-lag between the change of the previous IP-address in the DNS server and the clearing of that particular address from DNS caches. Hence, we can observe that though the previous IP-address is assigned to the new user but still there is always a chances of accessing the information by other user and it is not negligible because the address still exists in the DNS server cache and the data belonging to that particular user can become accessible to other user and that is violating the privacy of original user.

1.3 Application Level Security

In the application level security we can use the software as well hardware resources in order to provide the security to the applications in such a way that the attackers should not be able to obtain control on the applications as well as make any desirable changes into their format. At present time, attacks are launched; attacker is disguised as a trusted client and the application or system considers them like trusted user, and allow them full access and gets victimized. The basic reason behind type of problem this is that the out of date network level security guidelines is not capable to stop attacker.

So that, it is always necessary to install a higher level of network security tools to minimize such type of risks. In the traditional method, a task-oriented ASIC device is developed in order to deal with increased security issues; this device is able to handle a specific task that providing higher levels of security with great performance [8]. But this type of closed systems is observed as slow in comparison with open ended system; because of the application threats are dynamic and adaptable to the security checks.

The potential of closed-systems and the adaptability of the open-ended-systems is incorporated in order to develop the security platforms that is based on Check-Point Open Performance Architecture using the Quad-Core-Intel-Xeon-Processors. In the virtual environment, many companies that work with virtualization technique such as VMware are also using Intel-Virtualization-technology for the security base and the better performance. The threats and security issues that break down application-level-security include Cookie Poisoning, XSS attacks, Hidden field manipulation, DoS attacks, SQL injection attacks, Debug Option, Backdoor and CAPTCHA Breaking etc

consequential from unauthorized usage of applications.

1.4 Security concerns with the hypervisor

Cloud Computing depends basically on the virtualization concepts. In the virtualization technology, the hypervisor is basically defined as the controller and it is known as the virtual machine manager (VMM) and that allows multiple operating-systems to be run on a single system at a time, it provides the resources to every operating-system in such a way that they can't interfere with each. As the operating systems that are running on the hardware unit increased, the security issue that are concerned with those that of the new operating-systems also needs to be considered. There are multiple OS is running on the single hardware infrastructure, so it is never possible that keep track all the OS and thus maintaining all these operating systems securely is very difficult. It is always possible that a guest or visitor system tries to run a malicious script or code on the provider host system and that can bring the overall system down or can take full control of the system and can block the access to other guest-operating-systems (GOS).

1.5 Denial of service attacks

A denial of service attacks (DoS) is an attempt to make unable the services that is assigned to an authorized user to be used by them. In this type of attack, the server providing the service to the users is extremely flooded by a huge number of requests so that the services become unavailable to any authorized client or user.

The occurrence of the denial of service attacks (DoS) increases tremendous bandwidth consumption that causing congestion, and making some parts of the cloud system inaccessible to the authorized users. By using the Intrusion Detection System (IDS) we can defense against DoS type of attacks. A defence federation that is used in for guarding against denial of service attacks. Every cloud is loaded with such separate Intrusion Detection System (IDS).

1.6 Cookie poisoning

It this type of attack the change and modification in the contents of cookies is made in order to gain unauthorized access to any particular application or to a webpage by an attacker. The identity related credentials of the user basically contained by these cookies and once these cookies have accessible by attacker; the identity related content of these cookies can be used to impersonate any authorized user. This problem can be avoided by either performing regular cookie-cleanup or by implementing the encryption scheme for the cookies data.

1.7 Hidden field manipulation

While accessing the web page of any cloud website or application, there are several fields that may be hidden and that contains the web page related information that is basically used by the developers of application or web page. Although, such types of fields in web pages are highly prone to the attacker, hacker can attack because they can be modified easily and then that can be posted on the web-page or underlying application. This may be result in the violation of severe security.

II. SAFETY REQUIREMENT FOR A SECURE CLOUD COMPUTING

International Standards Organization (ISO) defined a standard ISO 7498-2 that states that prevention, detection and elimination all are needed to control and minimize threat in Information Security. Same concept is followed in Cloud computing, but prevention and detection processes are difficult to implement due to complex nature of Cloud. Security requirement for a secure Cloud computing are discussed below

2.1 Identification and authentication

Users are provided rights to access information in Cloud, but the access can be limited by some constraints. Information Assurance (IA) Technology Professionals defined that Cloud provider controls the access privileges of Cloud user. Users or enterprises are provided a unique ID and corresponding password for their identification and level of services are provided to that authenticated entity after successful verification.

2.2 Authorization

Authorization ensures that integrity of the Cloud is maintained, thus it plays an important role in security of Cloud. It is kept in back end of any Cloud as all Cloud facilities lies there. Information Assurance team stated that any organizations will be immune from damage from insiders if authorized access is maintained to protected information assets.

2.3 Confidentiality

In Clouds, Data or information is stored across multiple distributed databases and any attacker can access data if confidentiality is not kept under notice during development of Cloud. Confidentiality ensures that only authorized data can only be accessed by authorized users not by any unauthorized user. Safety of Cloud data is not only the major concern but preventing any attacker to access personal information of any Cloud user is also need to addressed

2.4 Integrity

The integrity ensures that Cloud data is not modified or tampered. So Cloud should be in same state if no authorized operation is performed on Cloud. Unauthorized alteration or modification of Cloud data may lead to low trust rating of Cloud.

2.5 Non-repudiation

Non-repudiation is a major problem in Cloud as it cannot be proved that whether that action was performed or not for e.g. in a faulty environment and without any precaution we cannot be ensured that a search query in Cloud was performed properly. Jun Feng showed that applying token provisioning in Cloud applications for data transmission using digital signature and confirmation receipts (i.e. digital receipt of message sent or received confirmation) may ensure non-repudiation.

2.6 Availability

Availability is major requirement for information security in Clouds .The NIST defined Availability as whether resources of any Cloud are accessible or available to Cloud user or not. It can be affected permanently or temporarily. It can be attacked by blocking some resources so that Cloud user cannot access them anymore, such attacks are equipment outages, Denial of service attacks, and natural disasters etc.

III. CONCLUSION & FUTURE WORK

The contents of data security are more extensive in the cloud. This security policy designed the data in the cloud computing that it just to solve the client's own data security protection. Once the data is stored into the public cloud, the protection of its data security will be more complex both from a technical and management. Especially the users require a higher for data integrity, security and controllability. If you want to enjoy the additional benefits of public cloud, you must still to wait for cloud computing security technology. We believe that the proposed "technology + management" Safety management philosophy which will be an important direction to address the cloud computing security issues in the future.

REFERENCES

[1] Peter Mell, Timothy Grance, “NIST Definition of Cloud Computing v15,” 2011 www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

[2] Zhang, Q., Cheng, L. & Boutaba, R., “Cloud computing: state-of-the-art and research challenges.” Journal of Internet Services and Applications,1(1), p.7-18. 2010.

[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. “Above the clouds: a Berkeley view of cloud computing,” EECS Department University of California Berkeley Tech Rep UCBEECS200928, 2009 http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

[4] Guo C, Lu G and Li D “BCube: A high performance, server-centric network architecture for modular data centers”. In: Proceeding SIGCOMM ACM (2009).

[5] Ghemawat S, Gobioff H, Leung “The Google file system”. Proceeding SOSP '03 Proceedings of the nineteenth ACM symposium on Operating systems principle Pages 29-43, 2003.

[6] Hadoop Distributed File System, www.hadoop.apache.org.

[7] Dean J, Ghemawat S, “Map Reduce: simplified data processing on large clusters”. Communication of the ACM, Volume 51, Pages 107-113, ACM 2008.

[8] Hanqian Wu; Yi Ding; Winer, C.; Li Yao; , "Network security for virtual machine in cloud computing," Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on , vol., no., pp.18-21, Nov 30 2010.

[9] Behl, A.; "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," Information and Communication Technologies (WICT), 2011 World Congress on , vol., no., pp.217-222, 2011.