Study of Vulnerabilities in Cloud Computing

Vinayak Shinde[1] Dnyaneshwar Bhabad[2] Pratik Sankhe[3]
[1]HOD & Assistant Professor [2,3]M.E. Student
[1,2,3]Department of Computer Engineering
[1,2,3]Shree L. R. Tiwari College of Engineering, Mumbai University, MS, India

Abstract—An organization can use internet-based services with the help of cloud computing. This mechanism reduces the cost of applications which are required by those organizations as such application will be shared among multiple organizations and they have to pay on pay-as-you-use basis. In today's world, most of internet users are moving their vital information and data on cloud because of its easy access from any location and from different Platforms. Users need not to worry about processing of data or where physical servers are exist but one thing that can aside all positive things about cloud is information security. Customers are doubtful about security mechanisms implemented by Cloud Service Provider (CSP). They are worried to place their data on a cloud storage area which is shared among various other organizations and users. This paper provides information about current loopholes and vulnerabilities in cloud security at different phases of data and at its carrier, cloud-specific vulnerabilities.

Key words: Cloud Computing, Information Security, Vulnerabilities, Data Carrier, Cloud-Specific Vulnerabilities, Data Linage, Data Remanence

I. Introduction

IT governance and management systems can spread awareness regarding security systems and standards of cloud computing [1]. These bodies have designed a cloud security management framework and they can define the standard processes and policies to be followed for better security [1]. We have summarized data related vulnerabilities and relative encryption Mechanism in Section II and Section III gives details about vulnerabilities at carrier and cloud-specific vulnerabilities.

II. Protection for Data on the Cloud

As we know the data is manipulated and processed by various applications, so it is very important to provide application level security to the data throughout its life cycle. Confidentiality, integrity and availability are the main parameters of data security [6] [7].

A. Data-In-Transit:

It is equally important to provide security to the data while it is being transmitted, as to implement the security policies at data centres in cloud.

There are two different ways to provide security to the data during its transfer between cloud customer and the storage at CSP.

- Confidentiality and integrity using secured protocols
- Confidentiality with non-secured protocol and encryption

Either we can use any of the secured protocol for transmitting the data from cloud users to CSP and vice versa, or we can use encryption mechanism.

B. Data at Rest:

Data centres of cloud computing can be the target of attackers, as it contains data of multiples companies and if attackers get into the data centre then attacker will have the access to data of all the companies. So, data should be stored at cloud storage in the encrypted form. But due to this encryption of the data users might be unable to use the cloud services like searching or indexing on data. Because these services can be coded by other developers and cannot be directly applied to our encrypted data. To overcome this problem two special encryption techniques like Homomorphism encryption and Predicate encryption can be used.

Homomorphism encryption allows users to apply various operations like indexing or searching even if our data is in the encrypted form. Predicate encryption uses a secret function. This function f will be evaluated on encrypted data if it returns 1, then specific data properties are considered as valid, if it returns 0 then then those properties will be considered as invalid (improper or wrong data.)

Data integrity should be maintained at data centre as various characteristics of data might affect the integrity. Data lineage is the process of knowing when and where the data was located in the cloud and it is important for audits. Data remanence is the property which states that data remains for some time after deletion as Cloud Service Provider makes various copy of data for better availability. It arises some questions regarding data confidentiality when organization uploads its business-critical information on cloud as

- How we can know if CSP had retain some additional copies of data?
- Can CSP just make that inaccessible to organization after deletion process and use that for its own usage?

Physical security of the data centres is also have same importance. It can be implemented through IAA (Identity, Access mechanism, Authentication) techniques. Retention policies should be defined appropriately. It states who owns a data which is present on the data centre, and how long that data will be maintained on that data centre.

III. Vulnerabilities in Cloud

Cloud carrier is the wide area network which connects consumer and cloud service provider for transmitting services between them. It is composed of intra-cloud network and wide area delivery network. Intra-cloud network is used for connectivity among various data centres of the cloud service provider and wide area delivery network connects end users or consumers to the data centres [3].

It is very important to have proper security implementations during transfer of data via these cloud carriers. There should be some more security mechanisms except network firewalls. Routers present in the cloud carrier may have some vulnerable points, which can be exploited by the attackers. So, it is also important to secure the router OS because it is found that router OS is more vulnerable than any other computer system [3].

A. *Cloud Specific Vulnerabilities:*

It is very important task to separate the cloud specific issues from general issues. As we know security is main roadblock for realization of the cloud, we have to analyse how cloud computing affects the existing security policies. Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. Frequency in which the loss event may occur and the magnitude of loss which may happen due to that event are the two main risk factors. Cloud computing era doesn't change anything regarding the magnitude of loss, so our study should be in the direction to focus the second parameter i.e. frequency of the occurrence of loss event [2].

According to the Open Group's risk taxonomy: Vulnerability can be defined as the inability of a system to resist the actions of a threat agent. It exists when the object's ability to resist the force differs from the force applied by threat agent. Vulnerabilities in simple word can be described as resistant to particular kind of attack [2].

On-demand self-service, ubiquitous network access, resource pooling, rapid elasticity and measured service are the essential characteristics of cloud computing [2]. With help of these characteristics we can identify the cloud specific vulnerabilities from general vulnerabilities. If 1)A vulnerability is frequent in Core technologies of cloud such as Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS) and cryptography 2)the root of any vulnerability belongs to essential characteristics 3) when innovation in cloud computing becomes roadblock in application or implementation of the tried and tested security mechanism 4) when certain vulnerability is frequent specific to cloud's state-of-art then that specific vulnerability is called cloud specific vulnerability [2][8].

Vulnerabilities in cloud computing core technologies can be in its nature itself or can be most frequent in certain cases. Virtualization is at very heart of cloud computing if attacker able to escape the virtual environment then these cloud specific vulnerability is in its nature of virtualization.one cloud specific vulnerability is regarding cryptography. Most cloud specific security mechanism requires cryptographic data should be stored on cloud. Attacker can use modern novel methods to breaking or due to bad implementation of good cryptographic algorithm, strong encryption turns into weaker one or in some case, no encryption at all [2].

Vulnerability associated with cloud computing essential characteristic have root cause in one or more characteristics.

1) In on-demand self-service user can have access to management interface without human interaction for example web portal and management interface when services and their resources can be managed automatically. Traditionally when only few administrator can have access to the management interface. Now, any cloud customer can have access. So, unauthorized access to management interface is relevant high-risk vulnerability [2].
2) Ubiquitous network access characteristic state that cloud user can able to access cloud services using network with standard protocol. Mostly, these network is internet and internet protocols used are vulnerable to attacks such as man-in-the-middle attack and this arises relevant vulnerability for cloud computing [2].
3) Pooling and elasticity characteristics of cloud computing state that resources allocated to one user will be reallocated to another user in future and that arises cloud-specific vulnerability as it is possible to retrieve data written by previous user [2].
4) Measured services characteristic include constantly metering, usage reporting to customer and pay-as-you-use business model. Vulnerability here is associated with manipulation of data used for billing purposes [2].

Vulnerabilities in standard security control should be considered as cloud specific if cloud innovation directly affects implementation of these control. These vulnerabilities are known as control challenge. For example, poor key management as cloud computing infrastructure requires storage and management of different kinds of keys. In cloud, virtual machine has changing hardware infrastructure and cloud-based data is geographically distributed, it's become difficult to implement standard security controls such as Hardware Security Model (HSM). Currently security matrices are not adapted to cloud infrastructure so cloud user cannot use any matrices to check security of its cloud resources[2][11].

If vulnerability is widespread in state-of-art offered by cloud computing, then such vulnerability should be listed as cloud-specific. Weak authentication schemes and injection vulnerabilities can be listed in this category. Authentication schemes such as username and password can be vulnerable due to irresponsible user behaviour such as weak password or reuse of password and usage one stage authentication schemes. Injection vulnerabilities occur when service or application input are manipulated to execute some of its parts against programmer intention, such injections are SQL commands or cross site scripted.[9]

B. *Vulnerabilities At Public Cloud:*

As compared to the private cloud, the public cloud has more vulnerabilities and threats. Whenever we are migrating from the general system into cloud system, we should be concerned to the security of data to be stored on cloud data centres [5]. Two different communities are facing the security issues in public cloud computing, these communities are cloud providers and cloud users. Cloud providers are concerned with the cloud infrastructure and network security as well as the security of the data of cloud data centres, cloud users are usually doubtful about the security implementations and mechanisms applied to cloud storage [5][10].

Below figure shows the rough cloud architecture which consists of different components like cloud platform, cloud storage, cloud infrastructure and cloud services. Each of these components should be secured with proper security control.

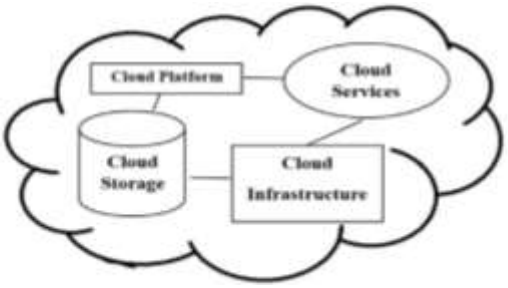

Fig. 1: Public Cloud Architecture

Following security controls are used to secure the public clouds: deterrent controls, preventive controls, corrective controls, detective controls.

Deterrent controls are used to provide the warning message to the cloud user (or provider) in case of any threat detection but these are not responsible for threat removal. Preventive controls are used to keep away our cloud system from the attacks. Corrective controls can take corrective actions on the data which is affected by the attacker and it will block that threat also. Detective controls will be continuously looking for any attacks or threats which unauthorized people are trying to access the cloud data [5].

IV. Conclusion

Cloud computing has great future as internet-based computing platform but it has to overcome security issues. Information security is important for both customer as well as cloud service provider. This paper has discussed vulnerabilities at different phases of data, vulnerabilities at cloud carrier and cloud-specific vulnerabilities at cloud’s core technologies, essential services and state-of-art.

References

[1] Grobauer, Bernd, Tobias Walloschek, and Elmar Stöcker. "Understanding cloud computing vulnerabilities." Security & privacy, IEEE 9.2 (2011): 50-57.

[2] Lenkala, Swetha Reddy, Sachin Shetty, and Kaiqi Xiong. "Security risk assessment of cloud carrier." Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on. IEEE, 2013.

[3] Fakhar, Faiza, and Muhammad Awais Shibli. "Comparative analysis on security mechanisms in cloud."Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013.

[4] Zhao, Gang. "Holistic framework of security management for cloud service providers." Industrial Informatics (INDIN), 2012 10th IEEE International Conference on. IEEE, 2012.

[5] Sandeepraja Batchu, J.N. Chaitanya, Sai sagar.N, Eswar Patnala. “A study on Security Issues Associated with Public Clouds in Cloud Computing.” Advanced Computer Technology(IJACT), 2013: 28-32.

[6] Kaufman, Lori M. "Data security in the world of cloud computing." Security & Privacy, IEEE 7.4 (2009): 61-64.

[7] SO, Kuyoro. "Cloud computing security issues and challenges." International Journal of Computer Networks 3.5 (2011).

[8] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov. 2010.

[9] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28.3 (2012): 583-592.

[10] Jansen, Wayne, and Timothy Grance. "Guidelines on security and privacy in public cloud computing." NIST special publication 800 (2011): 144.

[11] Hashizume, Keiko, et al. "An analysis of security issues for cloud computing."Journal of Internet Services and Applications 4.1 (2013): 1-13.