International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 03, March 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SECURITY IN CLOUD COMPUTING

Sunanda[1], Sakshi Arora[2]

[1,2]*Department of Computer Science & Engineering, Faculty of Engineering,*

Shri Mata Vaishno Devi University, (India)

ABSTRACT

Advancements in the field of cloud computing have gained huge success and popularity. It has provided a cheap and fast alternative for providing a plethora of services to its customers by providing access to virtual resources available over the internet. It has revolutionized the work culture for the bountiful benefits it provides. However, this rapid growth also raises some security concerns, as the companies rely dominantly on outsourcing their valuable data and applications. Despite, being able to provide huge benefits, companies are still hesitant in adopting them due to the threats posed by it to the consumers and service providers. This paper aims to provide a comprehensive survey of security issues and threats posed in the cloud environment. The study will be of help to users and service providers as it would provide an insight to the security threats in the cloud computing environment for both the cloud service user and cloud service provider.

Keywords: Cloud Computing, Issues, Security, Security Models, Threats.

I. INTRODUCTION

Cloud computing as a new computing archetype appeared around 1996, with the earliest known mention in a compaq internal document [1]. The evolution of cloud is attributed to the advancements in the fields of parallel and distributed computing, grid computing, utility computing and its further amalgamation with virtualization and load balancing [2]. The cloud as a host offers access to various computing resources (hardware, software and data) by establishing a centralized virtual pool of resources accessible over network, and thus providing infrastructure, platform and software as a service [3]. The consumers using these services are charged according to their usage. It has provided boom to the IT sector by revolutionizing the usage of hardware and software resources by incorporating the policies framed by government and the international agencies [4][5][6]. The ability to provide users with flexible services, scalable computing applications and access to huge storage databases contribute towards the exorbitant growth in the number of users for cloud computing [5]. People interested in IT startups are quite successful as they get to focus on the core aspects of business without worrying about the capital outlays and technicalities associated with the setting up of hardware and software infrastructure. However, despite its exorbitant success, there are still certain grey areas in the world of cloud computing. Security is one such area which needs deliberations, both from the side of users and service providers. Both tangible and intangible security threats are posed as the sensitive information and applications are shared over the virtual computing resources. Accessibility vulnerabilities, web application vulnerabilities, and virtualization vulnerabilities i.e. providing physical access to control the data, identity and credentials

management which in a way may lead to tempering of data, integrity , data and confidentiality loss etc. are some of the prime security challenges faced [7].

This paper aims to highlight the issues, threats and challenges viz-a-viz the security of cloud and provide a comprehensive survey. Section II provides a survey of security issues in cloud computing environment section III provides a survey of threats posed to cloud service users and Section IV throws light on the threats from the providers perspective. Finally conclusion is given in section V.

II. SECURITY ISSUES IN CLOUD COMPUTING ENVIRONMENT

2.1 Trust

As the management of data and applications is out sourced, leaving very little control in owners hands; the onus of enforcing stringent security policies for ensuring risk management, lies in the hands of service providers. This poses serious concerns to the security as the users blindly trust the processes and applications implemented by the cloud owner. Moreover, sharing of vital information over internet provides a vent for unauthorized access to activities for tampering or misusing or for remotely carrying out malicious activities. Deployment of security measures meant for static systems is not permissible due to architecture variation of cloud, thereby making concepts of handling security issues fuzzy and thereby weakening its efficacy.

2.2 Privacy and Confidentiality

Threat to data confidentiality is high in the cloud environment due to the access provided to number of authorized parties, processes and applications. This leads to number of issues pertaining to data remanence and multi latency [8]. Multi latency is a broad term used in context of cloud environment for sharing of resources such as memory, data, network etc at network level, host level and application level. Software applications designed for multi tenant architecture virtually partition the data and configures each virtual section created for different client organizations. This framework poses serious threats to the privacy and confidentiality as it permits and promotes the concept of object reusability.

Data remanence on the other hand may lead to breach in data confidentiality due to unintentional disclosure of vital information. It happens primarily because of virtual separation of logical drives.

2.3 Integrity

Ensuring integrity of processes, data and information is of utmost importance in cloud environment. Preventing data from modification from unauthorized party is data integrity. Mechanisms which assure that valuable information and assets are not altered or fabricated or stolen, increases the organizations confidence in data and system integrity. Authorization is one such mechanism which pre establishes a level of access to different users for different secured resources thereby providing ways and means of identifying the attempts made to affect the integrity. Maintaining integrity in a cloud environment is crucial due to the cloud model which poses serious threats due to its architecture model which provides access to increased number of access points, and thus the onus lies on cloud service provider for maintain integrity and accuracy of hardware, software and the network.

2.4 Availability

Availability refers to providing access to all the resources hardware, software and data to authorized users for carrying out operations. This implies making the system available and carrying out of operations even if the authorities misbehave or in the case of security infringement. The cloud service providers have to depend heavily on the networks availability as that is the medium through which all the hardware and software infrastructure demands are leveraged from users. It requires from the providers side, maintenance of detailed documentation of each and every users requirements for assuring sufficient achievement of these requirements. However, verifying identities and understanding their needs for data protection and information security in a multi user distributed environment poses very complex security challenges.

III. THREATS FOR CLOUD SERVICE USERS

3.1 Responsibility Indistinctiveness

Ambiguity in the definition of responsibilities among cloud service users (CSU) and cloud service providers (CSP) may result in conflicting issues. This inconsistency in taking charge of responsibilities may lead to anomalies or incidents pertaining to security breach.

3.2 Loss of Authority

Organizations relying on cloud for hardware, software, or network resources my benefit by passing on chores to the cloud, but also in this process transfer control or authority over its processes to the service providers. The loss of control/governance varies from the model to model.

3.3 Data Exposure

Data is a sensitive matter as far as cloud is concerned, as it stores data of various customers. Loosing data or data getting exposed to unauthorized users is quite possible due to sharing of resources, especially if it is not protected by incorporating proper cryptographic management means. Loosing this vital information may have a catastrophic effect on its business. Several brute force attacks and malware attacks have been reported in the past, resulting in data loss, data destruction and data leakage [9]. The major anticipated threats falling under this category are: inconsistent use of encryption and authentication keys, data center reliability, insufficient authentication, authorization and audit (AAA) controls etc.

3.4 Loss of Trust

At times it becomes difficult for CSU's to anticipate CSP's trust level because of its black box property. In the absence of distinctive formal strategies for identifying the stringent security measures, the cloud service users are always at a threat of misusing vital information, in the garb of resources offered by the cloud service provider.

3.5 Lack of Information Management

Cloud Service Users are normally unaware of how the information and assets are managed. For example the users are unaware about the location where information and assets are stored, how data backup is done in a

reliable and secure fashion , what measures and counter measures strategies are incorporated by cloud service providers in case of disaster recovery.

3.6 Unsecure Cloud Service User Access

An unauthorized access to your credentials by an attacker may have devastating effect. It not only can manipulate data, transactions or activities of the user but may redirect information of a user or company/organization to an illegitimate site.

IV. THREATS FOR CLOUD SERVICE PROVIDERS

4.1 Responsibility Ambiguity

Cloud service provider, cloud service user, admin, data owner are the domains of different entities in a cloud system model. Different set of rights are applicable if the cloud company is the keeper of data; and different set of rules/rights are applicable, if cloud company acts as a processor of the data. The responsibilities and duties assigned to each are not crisply segregated. However, an overlapping in terms of access control, data ownership , infrastructure maintenance etc is quite evident and noticeable. Such ambiguities in the basic structure may lead to legal dispute in business. The terms of service agreements on the question of ownership are not clear [10].

4.2 Business Discontinuity

Availability of resources to cloud service users is of utmost concern due to the heavy reliance of cloud infrastructure over internet for allocating resources and delivering services to the users. Discontinuity in delivering of these services ranging from hardware to application may have adverse effect related to the basic characteristic of cloud, that is availability..

4.3 Conflicting Legal Issues

Legal issues arise when there is a change in the landscape of computing i.e. when the paraphernalia of cloud extends beyond the domain of one country to other countries. Trademark violation, security issues and sharing of land owners data resources are among several issues that crop up. The electronic frontier foundation [11] condemned US government during the mega upload seizure process as people lost their property rights by storing data on cloud computing service [12]

4.4 Unsecure Administration API

The cloud application programming interfaces (APIs) used for designed applications for the cloud have gained popularity many folds; still face challenges due to patching of exposed APIs leading to potential risks of accountability, confidentiality and availability. The main cause associated to this is how APIs are written and protected. The researchers of Stanford University and University of Texas in their work have shown that interfaces used by third party developers have numerous flaws. Their work suggests that apps can provide access to important data by inappropriate means through API utilization. Non protected APIs are always at a soft target of attackers.

4.5 Virtual Machine Monitor responsible for isolation

The Virtual Machine Monitor (VMM) also known as a hypervisor is a low level software being used for controlling and monitoring virtual machines. Any compromise made in the development of software would have an adverse effect on the virtual machine [13]. Keeping the software simple and small reduces the risks associated with security. Not only this, virtualization enables these virtual machines to move between physical servers for load balancing, maintenance etc. [14]. This migration though a useful feature, raises serious security issues [15, 16].

4.6 Shared Resources

VMs deployed on the same server are permitted to share resources such as CPU, memory, I/O etc. This may result in weakening of security of each VM. A malicious VM in order to seek vital data or important information about other VMs through shared resources and memory [14]. The possibility of two VMs communicating through hidden means by avoiding the rules framed by the security module of VMM or supervising shared resources without getting noticed by its VMM and their adverse effect on the security, is quite evident through literature [17].

V. CONCLUSION

Rapid growth in the graph of Cloud computing has been observed for the characteristic features like portability, utilization of resources, portability, speed etc it provides. However despite its rapid success, firms/organization are still not very comfortable with the thought of completely relying on it. This is perhaps because of the susceptibility of cloud to various attacks and the strategies it follows in handling the security issues. This paper provides an insight to the security threats and issues faced by cloud service users and cloud service providers in a cloud environment. From our study we inferred that many of the processes or solutions offered are not mature enough to handle security breaches and threats. Virtualization, storage, sharing of resources are of prime security concern in cloud. It has been observed that a new security paradigms need to be developed and implemented in the context of cloud environment for making cloud more resilient against security breaches and attacks.

REFERENCES

[1] Antonio Regalado (31 October 2011). "Who Coined 'Cloud Computing'?". *Technology Review* (MIT). Retrieved 31 July 2013.

[2] Vaquero L.M., Rodero-Merino L, Caceres J., Lindner M. A break in the clouds: towards a cloud definition. In: ACM. SIGCOMM, editor. Computer communication review 2009. New York: ACM Press; 2009. p. 50–5.

[3] Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing, 2009. http://www.ibm.com/developerswork/websphere /zones/hipods/ library.html.

[4] Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*; 2009;**25(6)**:599–616.

[5] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. *Communications of the ACM*; 2010;**53(4)**:50–58.

[6] Mell P, Grance T. The NIST Definition of Cloud Computing. *Communications of the ACM*; 2010;**53(6)**:50.

[7] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*; 2011;**34(1)**:1–11.

[8] Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.

[9] T. Roth, "Breaking Encryptions Using GPU Accelerated Cloud Instances," Black Hat Technical Security Conference, 2011.

[10] *Maltais, Michelle (26 April 2012). "Who owns your stuff in the cloud?". Los Angeles Times. Retrieved 2012-12-14.*

[11] "A history of protecting freedom where law and technology collide". *Electronic Frontier Foundation*. Retrieved 20 February 2015.

[12] Cohn, Cindy; Samuels, Julie (31 October 2012). "Megaupload and the Government's Attack on Cloud Computing". Electronic Frontier Foundation. Retrieved 2012-12-14.

[13] Reuben JS: *A survey on virtual machine Security*. Seminar on Network Security; 2007. . Technical report, Helsinki University of Technology, October 2007 http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf . Technical report, Helsinki University of Technology, October 2007

[14] Hashizume K, Yoshioka N, Fernandez EB: Three misuse patterns for Cloud Computing. In *Security engineering for Cloud Computing: approaches and Tools*. Edited by: Rosado DG, Mellado D, Fernandez-Medina E, Piattini M. Pennsylvania, United States: IGI Global; 2013:36–53.

[15] Dawoud W, Takouna I, Meinel C: Infrastructure as a service security: Challenges and solutions. In *the 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany*. Washington, DC, USA: IEEE Computer Society; 2010:1–8.

[16] Venkatesha S, Sadhu S, Kintali S: *Survey of virtual machine migration techniques*. Technical report, Dept. of Computer Science, University of California, Santa Barbara: ; 2009. http://www.academia.edu/760613/Survey_of_Virtual_Machine_Migration_Techniques

[17] Ranjith P, Chandran P, Kaleeswaran S: On covert channels between virtual machines. *Journal in Computer Virology Springer* 2012, 8: 85–97. 10.1007/s11416-012-0168-