Managing Cloud Applications Data and Security

Muhammad Zunnurain Hussainf[a], Muhammad Zulkifl Hasan [b] ✉ and Zaka Ullah[c]

[a] zunnurain.bulc@bahria.edu.pk,

Assistant Professor, Bahria University Lahore Campus ,Senior Lecturer LGU Lahore, Pakistan

✉, [b] zulkifl@ncbae.edu.pkzakaullah@lgu.edu.pk
Assistant Professor, NCBAE Lahore, Pakistan

ABSTRACT

Cloud computing is a malleable, reliable and low coast platform for commercial and IT applications and their services over the Internet. Its powers many technologies like service-oriented architecture, virtualization. Cloud Computing Security (CCS), consists of a variety of policies, procedures, controls and technologies that combine to provide security to a cloud-based system, infrastructure and data. These security measures are configured to provide protect customers privacy, support regulatory compliance and as well as setting authentication rules for individual devices and users. From authenticating access to filtering-traffic, CCS can be configured to the exact needs of the business. In actual, we argue three serious challenges such as controlling, security and privacy issues in the cloud.

Keywords: *Cloud computing, Cloud Computing Security (CCS), security problems, security aspects, data segregation, secure cloud data, ACID, SaaS, PaaS, IaaS, Data Integrity, Data Security, Cloud Application risks, Data Locality, Networking, Data Access*

1. INTRODUCTION

Cloud computing has many benefits for business and productivity applications. At present, many organizations and enterprises are recognizing the paybacks of using cloud services through hosting applications and their private data through an online cloud environment. Implementing the cloud services area big gain to the efficiency and productivity in development and helps setup services with reduced cost in running and maintaining the infrastructure. From the consumers' viewpoint, the two main concerns for users taking advantage of cloud application and data services are privacy protection and security issues. Security, privacy is some of the key concerns which persist to stay a major hurdle from embracing and implementing the cloud computing model.

Cloud computing (CC) provides different services through the Internet. CC resources include applications and tools like servers, data storage, networking, software and databases. Rather than to keep files on a proprietary hard drive(HDD) or local storage devices like Flash drives and DVDs, cloud base storage makes it possible to store data to remote database storage. As long as an electronic gadget has access to web connectivity, it has access to the store data and the various software programs to run it. CC is a popular option for people and businesses for several reasons including increased productivity, cost savings, speed, performance, security and efficiency. CCS is essential for the several different users who are concerned about the security of the data they store in the cloud database. They believe their data is secure on their local servers where they have more control over their stored data. Where data stored in the cloud databased may be more secured because CCS providers have much superior security measures. On-premise user's data can be more vulnerable to security breaches depends on the type of attack. Social engineering and malware types of attacks can make any data-storage system vulnerable. Cloud computing is deeply concerned with the security of data secrecy and lawful things. The reason is cloud gives a comparatively new computing technique and boundless deal of doubt in what way security at all ranks could be attained and in what extent applications safety is moved to cloud computing. Hesitation steered executives belongs to data state that safety is the first issue with the cloud.

2. METHODOLOGY

The paper is based on the qualitative research methodology which consists of inferences from studies and interviews of related cloud developers and professionals. The surveys were also conducted during the study to collect the information needed for analyzing risks and measures related to cloud environments.

A. Privacy, Reliability and Accessibility

Top fragility is to be squared to confirm that the data is secure from any unauthorized user. So, security test has been completed to safe data from the unauthorized use such as Access control and cross-site scripting mechanisms etc. To offer client data security, few clients can be used where some minimum resources are available. Clients cannot save their private data like a passcode, email etc. The correctness of data should be guaranteed. Accessibility is one of the best significant matter in many establishments that fronting the interruption as a most important matter. It relies on the settlement among the client and the vendor. Location in the cloud, most of the records are scattered above the areas and locate the position of data in memory is problematic. Data can also change when it is moved to terrestrial zones that governing the rules. In overall each transit in the cloud must track the stuff of ACID to conserve correctness of data. Many facilities appearance a portion of difficulties with the administration of transaction normally as it uses in Hypertext transfer protocol services.

Hypertext transfer protocol services do not maintain any transaction or confirmation of distribution. It can be applying by the management of transit in the API itself. Data admittance mostly mentions to the policies of data privacy. Within the business, the workers will be having rights to the piece of data on their safety policies. Cloud computing services providers faced outdated communication systems need to solve common data security challenges. CC can be a single function application, an infrastructure on which these CC applications can run, a various set of services that offer the huge amounts of computing resources, and the capacity to store huge amounts of data remotely. At the same time, they also have to treat with many issues integrally presented by the cloud computing standard itself.

Six detailed areas of the cloud setting wherever apparatus and application need extensive security responsiveness. These six regions are (a) data security at rest, (b) data security in transit, (c) verification of users/applications/ processes/clients (d) vigorous segregation between data belonging to different clients (e) lawful and controlling issues (f) event reaction.

B. Which cloud model should one use?

As referenced, each cloud model demonstrated is special in its offering, value, focal points and burdens. Open cloud contributions commonly comprise of a virtualized domain with every purchaser sitting alongside one another on a similar box. These are generally less expensive alternatives that enable buyers to buy a lot of capacity or figure control at a moderately reasonable cost. In this situation, nonetheless, shoppers can have less trust in the security of their information.

Another model is that of private cloud administrations[1]. These are typically much increasingly costly yet enable associations to have a die-hard devotion with no different buyers present on a similar framework. This gives more confirmation to ensuring touchy information, be that as it may, this might be pointless excess if the association is simply putting away generally uncaring information. Associations can basically observe this administration as an expansion of their present space and apply controls properly, there is generally okay from different customers in this model.

Buyers ought to survey the kind of information that will be handled or put away in the cloud condition, or that may be available from this condition. It is normally fitting to have a proportionate way to deal with this – for instance, acquiring a private cloud administration to have free open substance is pointless excess. In any case, facilitating touchy HR records on an open distributed storage administration isn't prudent if the provider has not given enough affirmation that information detachment has been accomplished.

C. How to gain assurance that data separation has been achieved?

Picking up affirmation for information partition in distributed computing is dependent on the kind of administration you are expending. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Application as a Service (SaaS) each have their very own innate dangers and methods for picking up an affirmation that information partition in distributed computing has been accomplished.

For instance, an IaaS administration that gives processing, system or capacity administrations can be accomplished through a properly verified or guaranteed hypervisor. A hypervisor controls the virtualized condition on a container and, whenever traded off, enables an assailant to get to every virtual machine on that crate. If an aggressor claims a hypervisor, they possess the crate and every one of the information on that container. Guaranteeing the hypervisor is secure is principal for IaaS administrations to accomplish information partition in distributed computing. Also, the partition can be accomplished at the system level using a suitably designed virtual neighborhood (VLANs). Cloud suppliers can isolate every buyer into discrete VLANs and lock these down fittingly to counteract VLAN jumping[2].

Accomplishing information partition in distributed computing turns out to be increasingly troublesome for SaaS-based contributions. As SaaS is ordinarily programming based administrations, the partition must be accomplished through fitting application design and setup. The hidden framework and stage won't keep an assailant trading off an inadequately coded application so care must be taken by the cloud supplier when programming applications for open utilization. For this situation, it is prescribed that purchasers wishing to devour SaaS contributions do as such inside a private cloud condition to diminish dangers to their delicate information.

D. Level of Cloud Security

The CCS classification recognizes the risk levels as low aka less vulnerable, medium, and high aka more vulnerable depending on the exposure of CCS requirements. Authentication, data encryption, data privacy, multi-tenancy and authorization are the security requirements for cloud services.

E. An Issue in Cloud Service Models

In SaaS, the implementation of these applications may increase some security worries like Application Security, Multi-tenancy, Data security and Accessibility. In PaaS, the implementation of applications may increase some security worries like third-party dealings, expansion life cycle and underlying infrastructure security. In case, the implementation of PaaS applications may increase some security worries like virtualization, virtual mechanism displays and shared resource, public virtual machine image repository, virtual machine rollback, virtual mechanism life round and virtual networks. To make the distributed computing be received by clients and undertaking, the security worries of clients ought to be redressed first to make cloud condition dependable [3].

F. Data Availability

Data given by the client is ordinarily verified in various servers [4] from time to time setting in various regions or various hazes. Data Storage, Backup and Recovery the cloud clients move their information to the cloud supplier ought to guarantee satisfactory flexibility hoarding structures. The cloud suppliers will store the information in two or three spots crosswise over different free servers.

G. Risk Analysis

Adopting the cloud environment for your services could end up in risky situations. Some serious threats and vulnerabilities should be studied to realize whether if it is feasible to adopt for your service or not. Different risks are discussed below:

H. Security-Risks

For inhibiting a cloud’s environment from dangerous exploitation attacks are reflected as security of the system. Risks associated with security that are tangled with administrative usage of cloud infrastructures have plenty of risks associated. Some of the important factors as a risk in cloud computing are accessibility, data integrity, data security, data segregation and data location[5].

I. Accessibility

Privileges must be specifically provided to particular users to reduce such threats. If an attempt is made to access internal source from an external source, the threat is likely to be targeting the sensitive data. Data segregation plays an important role in cloud environments as the data is in distributed form over the network’s physical devices. There are also chances that data may become corrupt if segregation is not maintained appropriately.

J. Data Location

Most cloud vendors are not located on a single specific location and scattered throughout different regions. Due to unfamiliarity amid the customers regarding the precise location of the cloud environment. It results in difficulty to access cloud's activity, where data may not be stored at a specific data-centre location but through a scattered arrangement.

K. Data Segregation

The data is not encrypted by most of the customers and encryption itself could potentially make the data unusable, because it may cause ruined the data file format. Cloud models don't work as a toolkit for the environment. Compromised systems are shutdown each time data is desired to be recovered. At the time of recovery, the data could consist of multiple instances of duplication of data. The data must be restored rapidly and completed on time to avoid additional risks.

3. SECURITY ISSUES IN CLOUD

The study suggests that deployment models in the cloud are based on SaaS, PaaS and IaaS. It gives framework support for the clients. These deployment models are established over one another therefore, their abilities are acquired as well as security issues and dangers [6].

In the cloud deployment model of Software as a Service, an end-user needs to be influenced by data security from service providers. Cloud service providers may produce copies of your data resulting in replication of your data. Some attention-demanding security concerns in a SaaS deployment model are:

A. Data Security

Once a company's profound data is saved in a cloud environment, providers should be responsible for the security, alongside secure policies for accessibility with extra security should be implemented. Data control enable cloud services to make it difficult to protect and administer identity theft as well as cyber-crime security[7].

B. Data Integrity

The validation and security of data affect the processes and results of a system. A relatable scenario is a mobile vendor who had stored customers data containing customer's messages, contacts list in Microsoft subsidiary[2]. If unfortunately, the provider loses the data and cloud is not available over the network. The customers would have to wait in anticipation of their basic information to be restored from the cloud.

C. Network Security

Data is transferred through the Internet; therefore, the data flow is an imperative concern to evade information leakage. Network packets could be sniffed by an intruder who could make misuse of the data packets and determine network security weaknesses[8].

D. Data Locality

End-users may be uninformed about the location of them. In some cases, it could become an issue due to laws regarding data privacy in several countries. Therefore, the model needs to be proficient in providing security centered on regional factors[9].

E. Access Control

When an employee has left the company, users must enable or disable the user's account to prevent a security breach. The SaaS service providers must offer policies in a cloud architecture that ensure to elude any intrusion of data by any unauthorized user[10].

4. FUTURE WORK

With the growing demand and use of cloud computing models, the field is growing mature and there are several aspects to look for security risks that will moderate and certainly emerge new concerns. For overall security service measures, both the vendors and consumers should be analyzed clearly[11].

- Every component should be analyzed at tiniest and largest level.
- All service providers should provide some standards and list of risks and instructions to safeguard against them.
- Service Level Agreements should grant constant security assessment.
- Service Level Agreements should grant constant security assessment.

A. Secure Application Interfaces

A set of application interfaces are open to the end-users to interact with the cloud services. These interfaces of the software offer the security of cloud services[10]. The Cloud-Security-Alliance commends must use secure software interfaces for the cloud services to interact with.

B. Separating-The Application's Data

i. Segregating Data

The data segregation is where data of one customer to the data of another customer. Multiple customers share similar service resources (As shown in Fig.2) but because of data segregated, they have their data separate from each other [13].

ii. Data Fragmentation

If a set of data is divided into pieces, files are encrypted and fragmented before moving from the system. Security and confidentiality can be provided for the data using fragmentation in the environment of cloud computing [9].

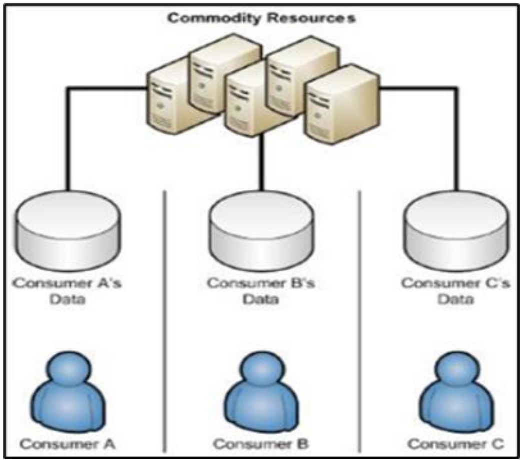

Fig. 2: Data-Segregation across data stores for multiple customers [12]

5. CONCLUSION

Even though cloud computing is a relevantly new form of technology in the field of IT for utilizing various applications. It offers great value and benefits to its users, on the other hand, security challenges are also expected. This study primarily discussed the data security challenges and solutions. Henceforward tangible standards could be established for the security of cloud computing. Secure data access could be provided in the cloud environment through progressive encryption practices for storing and retrieval of data from the cloud. Similarly, appropriate key organization techniques help distribute the key to the specified cloud users so only authorized persons can only access the specific data.

REFFERENCES

[1] C. Pettey, “Gartner identifies the top 10 strategic technologies for 2011,” *Gart. http//www. gartner. com/it/page. jsp*, 2011.

[2] N. Cubrilovic, “Letting Data die a natural death,” *Int. J. Electron. Gov. Res.*, 2009.

[3] K. Kaur and S. Vashisht, “Data separation issues in cloud computing,” *Int. J. Adv. Res. Eng. Technol.*, vol. 1, no. X, pp. 26–29, 2013.

[4] H. Tianfield, “Security issues in cloud computing,” in *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2012, pp. 1082–1089.

[5] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, “A strong user authentication framework for cloud computing,” in *2011 IEEE Asia-Pacific Services Computing Conference*, 2011, pp. 110–115.

[6] K.-K. R. Choo, J. Domingo-Ferrer, L. Zhang, and others, “Cloud Cryptography: Theory, Practice and Future Research Directions.,” *Futur. Gener. Comp. Syst.*, vol. 62, pp. 51–53, 2016.

[7] J. Brodkin, “Gartner: Seven cloud-computing security risks,” *Infoworld*, vol. 2008, pp. 1–3, 2008.

[8] P. Mell, T. Grance, and others, “The NIST definition of cloud computing,” 2011.

[9] S. Carlin and K. Curran, “Cloud computing security,” in *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments*, IGI Global, 2013, pp. 12–17.

[10] J. Che, Y. Duan, T. Zhang, and J. Fan, “Study on the security models and strategies of cloud computing,” *Procedia Eng.*, vol. 23, pp. 586–593, 2011.

[11] W. Zeng, Y. Zhao, K. Ou, and W. Song, “Research on cloud storage architecture and key technologies,” in *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*, 2009, pp. 1044–1048.

[12] R. R. Chowdhury, “Security in Cloud Computing,” *Secur. Cloud Comput.*, vol. 15, p. 96, 2014.

[13] J. L. Duffany, “Cloud computing security and privacy,” in *10th Latin American and Caribbean Conference for Engineering and Technology*, 2012, pp. 1–9.