International Journal of Library Science;
Volume 19; Issue No. 1; Year 2021;
ISSN 0975-7546; Int. j. lib. sci.

Data Storage Management and Security Issues in Cloud Computing

Anupam Chanda[1]

[1]Librarian, Assam Don Bosco University, Guwahati, Assam-781017, India.
Email: anupamchnd1988@gmail.com
Mo: 7002039631

ABSTRACT

Cloud computing provides an on-demand computational infrastructure to the users who have the latent to reduce the huge cost to assemble IT-based services. Security over the cloud has been stimulating for the investigators and they have been providing a good explanation. Most of the internet companies have built large data centres and day by day it is growing extremely. But it has several dark sides and uncertainty creates the foremost problem for cloud users.

This paper proposes and apparatuses a combined approach to solving multiple security issues simultaneously. This approach will help the cloud system to handle many security issues using a single solution. The primary aim of this paper is to focus on numerous security issues of cloud computing and analyse the different unexplained security problem that threatening the various organization to adopt this technology.

Keywords: Cloud computing, security issues, IaaS, PaaS, SaaS.

Library of Congress Classification Number: QA76.625 .R435 2009

1. INTRODUCTION

Cloud computing is a technology used to transport hosted facilities over the Internet. Through this technology, users do not have to accomplish their own IT resources; instead, they can obtain their IT needs as services over the internet. Cloud computing has allowed users to migrate there data and applications towards the cloud. Instead of working on a station with invaluable resources and apps, users take advantage of cloud-delivered on-demand resources and applications with low cost. Service models of the cloud are classified into three types such as SaaS, PaaS, IaaS and different deployment models are classified into Private, Public, and Hybrid. The cloud is developing as the latest way to approach substitute delivery models for IT competences. It is a way of providing IT-enabled services in the form of software, infrastructure and more.

In a cloud computing atmosphere data asset is very crucial depending on the business and the service delivery models. To provide the controlled access and authorisation, classifying data based on security level criteria becoming the area of interest by many organisations using or providing cloud services.

However, there are numerous services which cloud delivers to the client companies or any other users. All users can get a massive amount of storage ability. Still, most of the client are not prepare themself to implement cloud computing technology due to the restriction of security control strategy, restriction in protection data which leads to a dispute in cloud computing.

1.1 Objectives of the Study

- To know the different cloud storage platform;
- To identify the security issues of cloud storage;
- To find out the solution of multiple security issues of cloud storage.

1.2 Research Methodology

The study has been based on the information collected from the secondary sources. The researcher has tried to compile the information regarding security issues and its remedial measures in cloud storage. All the ideas related to the study has been gathered from different sources. The researcher also has taken interviews from the subject experts to validate the secondary data.

2. LITERATURE REVIEW

Pandey and Dubey (2018) have discovered that security over the cloud has been challenging for the researchers and they have been providing the right solution. But growth in technology is imposing new challenges and tackling these, a better solution is always needed. Their work proposes to use IDS, a Trust server and access control along with the encryption and decryption of the various data being used over the cloud.

Sarkar and Kumar (2018) conducted a survey on data storage security issues in cloud computing. Where they found that most of today's internet companies have built immense data centres and day by day, it is growing incredibly. Numerous types of security issues that need to be addressed in cloud computing. The article focused on various security issues of cloud computing and analysed the different unexplained security problem that intimidating the different organisation to adopt this technology

Vurukonda and Rao (2016) have mentioned in their article cloud computing is an innovative mechanism that is changing way to enterprise hardware and software design and procurements. Their study identifies the issues related to the cloud data storage such as data breaches, data theft, and unavailability of cloud data. Finally, they provided possible solutions to respective issues in the cloud.

Khan and Yasiri (2016) conducted a study on identifying cloud security threats to strengthen cloud computing adoption framework. In their research, they mentioned that cloud computing has struggled to grow among many established and growing organisations due to various security and privacy-related issues. This study enabled us to understand, current and future, security and privacy challenge with

cloud computing. The outcome of this study led to the identification of total 18, present and future, security issues affecting several attributes of cloud computing.

3. CLOUD STORAGE AND ITS SECURITY ISSUES

3.1 Different Cloud Storage Platform

Cloud storage is a computer data storage where various types of digital data are stored in rational pools. The physical storage spans multiple servers in several locations, which typically owned and managed by a hosting company, they are accountable for keeping the data available and accessible, and the physical environment protected and running. In simple words, it means storing data in a remote location which is accessible from any device through the Internet. People and organisations buy or lease cloud storage from the hosting company to store their various kind of data. Many cloud hosting companies offer a free plan for those who need the minimum out of their service. Cloud storage providers provide much data security for business users.

There are three types of cloud data storage: Object storage, File storage, and Block storage.

Object Storage - Applications developed in the cloud frequently take advantage of object storage's vast scalability and metadata features. Object storage solutions are ideal for constructing modern applications from scratch that require scale and elasticity and can also be used to import existing data stores for analytics, backup, or documentation.

File Storage - Some applications require to access shared files and need a file system. This kind of storage is repeatedly supported with a Network Attached Storage (NAS) server. File storage solutions are perfect for use cases like vast content sources, development environments, media stores, or user home directories.

Block Storage - Other organisational applications like databases or ERP systems often require enthusiastic, low latency storage for each host. This is similar to Direct-Attached Storage (DAS) or a Storage Area Network (SAN). Block-based cloud storage solutions are provisioned with each virtual server and offer the ultra-low latency required for high-performance workloads.

3.2 Security Issues of Cloud Storage

Even though cloud computing provides less cost and less resource management, it has some security threats. Cloud computing properties are creating security as a remarkable concern. Though there are various tools and techniques are available which can be used to keep your data safe, it is tough to keep up the dependability of the system as you are sharing your data with others. Most of the time it is subcontracting from others. Another major risk is when data is outsourced to third-party storage by the

CSP. The key generation and key management in cryptography for cloud computing is not consistent up to the mark. But lacking standard and secure key management for the cloud doesn't allow the standard cryptography procedures to perform well in a generic cloud computing model. Such that cryptography may also ensure the potential risks to cloud computing. The cloud construction model has different types of loopholes and this architecture made cloud computing into various security and privacy threats.

IaaS Security Issues: The available option within the IaaS varies from a single server to entire structures including network devices, databank, web servers etc. It provides hardware resources for performing services to the user by using virtualisation technology but IaaS will face the following problems:

- Virtual Machine (VM) Security.
- Securing VM Images Repository.
- Virtual Network Security.
- Securing VM Boundaries.
- Hypervisor Security.

PaaS Security Issues: Out of numerous clouds computing services, platform as a service allows the user to customise the applications in the form of development, execution and management. So the security issue of PaaS is all lies on SOA security. SOA security includes numerous standpoints of security issues including access control, privacy and service stability while defensive both the cloud service provider and the cloud handler. Every kind of security attacks, preferably denial of service of attacks and man in the middle attack, may interrupt the service provided by PaaS. Application Programming Interface (API) offered by the platform as a service provides various functions related to business and management.

SaaS Security Issues: Software as a Service (SaaS) is the highest layer which has a comprehensive application and delivers services on request. It is a software distribution model which provide to access the application through the internet as a web-based service to the user without installing the application on the user's computers. Each service delivery model has different possible implementations, which complicates the development of a standard security model for each service delivery model. The SaaS model facing different types of issues as follows:

- Data Security.
- Network Security.
- Data Locality.
- Data Integrity.
- Data Segregation.
- Data Access.
- Authentication and Authorization.
- Data Confidentiality.
- Availability.

- Backup.
- Identity Management and Sign-on Process.
- Data Breaches.
- Web Application Vulnerability Scanning.
- Web Application Security Miss-configuration and Breaking.

The main essential tasks of the cloud are to offer various services in terms of processed data to the end-users. Many end-users keep their data in cloud data storage and cloud providers provide the security on those data. Now if the security policy is not standard, then the third party intruder or the attacker can quickly get the data of end-users. In that case, those particular cloud providers are not trustworthy and people will go for other cloud service providers who can provide better security services. If there are any security issues in any mission-critical system, there must smell of threat.

Proper identification and the classification of security threat is essential prior to implement the security techniques and a rigorous survey on the threat can achieve that. Privacy and Security at different cloud layers such as application layer, Host layer and Network layer are compulsory to keep the cloud up and running uninterruptedly.

3.3 Solution of Multiple Security Issues of Cloud Storage

Many end-users keep their data in cloud data storage, and cloud providers provide the security on those data. Now if the security techniques are not standard, then the third party intruder or the attacker can quickly get the data of end-users. In that case, those particular cloud providers are not trustworthy and people will go for other cloud service providers who can provide better security services. Most of the state of the art attacks such as Flooding Attack, Side Channel Attack, port scanning, Denial of Service (DoS), Distributed Denial of Service (DDoS) etc. disrupt the services of cloud.

Some of the security threats of the cloud computing platform and their corresponding probable solutions are also listed below in the following table:

Table – 1: Security threats of the cloud computing platform and their corresponding probable solutions.

Threat	Description	Methods
Google hacking	Identifies login passwords, pages containing logon portals etc. from the databases	Web Vulnerability Scanner.

SQL Injection	In this process, some malicious code is injected into a Structure Query Language	Avoid dynamic SQL code, use meta-structure, proper user validation, and avoid unwanted data.
Cross-Site Scripting (XSS)	injecting mischievous scripts into web-based contents	Data Leakage Prevention Technology based on Content, Active Content Filtering, Vulnerability Detection Technology based on Web Application.
DoS or DDoS	Denying access to the internet, slowing down the website, unable to give service to legitimate users.	Game theory against bandwidth-consuming of DoS and DDoS
IP spoofing	Manipulation of an IP packet to get unauthorised access user machine or cloud service, provider	Performing filtering for incoming and outgoing packets and enabling encryption for sessions, spoofing attacks can be reduced IPSec based solution.
Sniffer Attack	Unencrypted packets transferring between the sender and receiver get captured	ARP and RTT based solution

4. CONCLUSION

Multiple security issues of cloud storage and how to overcome the risks have been deliberated in this paper. Many security issues that need to be controlled along with security threats in a cloud storage platform. Despite many security issues, cloud storage system which is measured as dominator of the IT market. Privacy and honesty of data should be the main concern while opting for cloud services from a cloud service provider. Examining at regular intervals is also compulsory to deal with security threats. Errors from cloud service provider side should be minimalized.

It is not possible to offer full security in the Cloud computing environment. Those who are applying cloud computing by increasing their on-premise structure must be aware of the security challenges faced by cloud computing. To generate a defence against the collaboration of the agreement truthfulness and security of their applications and data, a defence-in-depth approach must be applied.

5. REFERENCES

Brar, I. S., 2016, Cloud Computing in Libraries: Special Reference to India. *J. International Journal of Library Science.* **14**.

Khan, N., Al-Yasiri, A., 2016, Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. *J. Procedia Computer Science*.

Kumar, J., 2019, Cloud Computing Security Issues and Its Challenges: A Comprehensive Research. *J. International Journal of Recent Technology and Engineering.* **8**, 10-14.

Kuyoro, S. O., Ibikunle F., Awodele O., 2011, Cloud Computing Security Issues and Challenges. *J. International Journal of Computer Networks (IJCN).* **3**, 247-255.

Nadeem, M. A., 2016, Cloud Computing: Security Issues and Challenges. *J. Cloud Computing: Security Issues and Challenges.* **1**, 10-15.

Padhy, R. P., Patra, M. R., Satapathy, S. C., 2011, Cloud Computing: Security Issues and Research Challenges. *J. International Journal of Computer Science and Information Technology & Security.* **1**, 136-146.

Pandey, V., Dube, M., 2018, Integrated Approach to Cloud Security. *J. International Journal of Applied Engineering Research.* **13**, 9794-9801.

Ramesh, M. R., 2013, Impact of cloud computing on libraries. *J. International Journal of Library Science.* **8**.

Sarkar, M. K., Kumar, S., 2018, A Survey on Data Storage Security Issues in Cloud Computing. *J. International Journal of Applied Engineering Research.* **13**, 8390–8406.

Vurukonda, N., Rao, B. T., 2016, A Study on Data Storage Security Issues in Cloud Computing. *J. Procedia Computer Science.*