# A Survey on Data Security, Storage Issues, Goals and Solutions In Cloud

**B.Haritha[1], J.Manasa[2]**
[1, 2] Department of Computer Science And Engineering
[1, 2] G. Pullaiah College Of Engineering And Technology

***Abstract-*** *Cloud Computing is a technology that increasing rapidly with Distributed Computing, Utility Computing, Grid Computing. Due to simplicity nature of cloud many organizations are moving data to cloud centers. The cloud service providers are Google's application, Amazon IBM, Microsoft Azure etc. Cloud users can develop the applications in cloud environment and can access the information anywhere around the world. The Cloud service providers stores the data in remote servers. The major problem in providing the security arises when the data is transmitted to the remote server over a channel.*

***Keywords***- Cloud computing, Data security, Data Access, Cloud service provider (CSP), cloud data storage, security issues.

## I. INTRODUCTION

Cloud Computing provides the services to users for accessing various cloud applications. The cloud computing provides costless service elasticity of resources, easy access through the internet, etc to the client users. By this the cloud users can access the data from anywhere [1].The users can store their information in the Cloud[2]. As cloud computing has many benefits, cloud users are unwilling to place their sensitive data. Suppose if data is placed in a cloud datacenter; then the cloud users can loss their direct control over their data source. Security and storage are the major concerns in the cloud. If security measures for data transmissions are not provided properly then the data in the cloud is in risk[3]. The Cloud Service Provider (CSPs) provide the data security of stored data to the clients through firewalls and virtualization. But these techniques could not provide the complete data protection because of its vulnerabilities in the network. Therefore, cloud needs strongest security and storage are to be implemented and managed to preserve the data confidentiality by identifying security problems and solutions to handle these challenges[4].

## II. MODELS OF CLOUD COMPUTING

**A. SaaS:** Software as a Service are probably the most popular and are easy to use. To run the applications directly from a web browser the SaaS does not require any installations or downloads. SaaS does not require to install and run the applications on individual computers. Examples of SaaS are Gmail, Google+, Face book etc.

**B. PaaS:** With PaaS the developers' gains a framework, by this they can develop applications. Paas removes the need to buy the underlying layers of software and hardware and makes the testing and deployment of applications quick, simple, and cost-effective.

**C. IaaS:** Infrastructure as a Service (IaaS)delivers computer infrastructure, networking and storage. All sizes of businesses has to take advantage of the agility, flexibility and cost benefits of cloud infrastructure as a service(IaaS). Virtualization, servers, hard drives, storage, and networking are still managed by vendors. The infrastructure on which can install any platforms can be gained by the users with IaaS. If any new versions are released the users are responsible for updating.

**D. StaaS:** With Storage as a Service (StaaS) [5] users can access to their stored information on remote disks at any time from any place. Cloud storage systems are used to meet several requirements for maintaining information including high availability and data consistency and users' data. No system implements all of them together because of the conflicting nature of these requirements.

## III. CLOUD DATA STORAGE AND SECURITY CHALLENGE ISSUES

The cloud computing does not provide control over the stored data in data centers of cloud. The cloud service providers have full on control over the data; they can perform any malicious actions on the data. so, the data that contains in cloud require security and privacy of data. Data loss or leakage can have a severe impact on business and the Organizations. The cloud computing provides a certain level of control over the virtual machines. Greater security issues arise due to the lack of control over the data.

**A. Security:**

If the multiple organizations share data resources then the data misuse risks will arise. So, to avoid risks the secure data repositories and the data process. One of the important challenges in cloud computing is protection of data. To increase the security in cloud computing, it is necessary to provide authorization, authentication and access control for data stored in the cloud. The main areas in the data security are:

1) Confidentiality: Top vulnerabilities should be checked to protect data from attacks. So, test has to be done on the security to protect data from malicious users.
2) Integrity: To provide security to the clients' data the thin clients are used, where only a few resources are available. So, that integrity can be assured so users should not store their personal information like passwords.
3) Availability: In many organizations, the important issue is availability. The availability depends on the agreement between the clients and vendors.

**B. Access:**

Data access refers to the data security policies. In an Organization, the employees can access to the data based on their company security policies. The same data cannot be accessed by the other employees working in the same organization. To share the data only between the valid users' various encryption and key management techniques are used .Using the key management technique, key is distributed between the unauthorized parties.

To secure the data from hackers we should follow some security measures. The user must use the encryption and decryption to protect our data from the hackers.

**C. Confidentiality:**

The user stores their data in cloud providers and remote servers, vedios are stored in the single provder or multiple providers but the remaining data is stored in the remote server. To maintain confidentiality to the data stored in the cloud its accessibility should be aware by the users.

**D. Data privacy and Integrity:**

Cloud computing has some issues even though it provides security but it provides minimum cost and resource for the users. The cloud computing should have integrity, confidentiality, privacy, and availability of data. Because of simplicity of the cloud, many users want to store data in the cloud. This lead to greater security threats to cloud clients. If an attack is made on the data or any unauthorized access data leads to data breach to data breach. Because of these attacks data in the cloud can lost multi-tenant nature. Especially SaaS providers may also lose their technical data and they have great risk over data storage. While data is transferred from one person to another there may be chance to get risk for that data. Because of virtualization, many resources are shared among users, this lead to the attacks by malicious insiders of the CSP or organization. The malicious users can perform the attacks on the data in the cloud while preceding the data. Other major risks arise when the data in the cloud is outsourced to the third party storage by the CSP.

**E. Data recoverability and vulnerability:**

Because of some characteristics, the cloud ensures dynamic and on-demand Resource provisioning to the users. The resources allocated to a particular user may be assigned to the other user at some later point in time. In case of memory and storage resources, a malicious user can perform data recovery techniques to obtain the data.

**F. Data backup:**

The data which the user wants to be protected is to backup. To ensure that the data is present ,we have to perform regular data backup to the stored data by using CSP. To protect the backup data from the unauthorized persons we have to use some security guidelines.

## IV. DATA STORAGE AND SECURITY TECHNIQUES IN CLOUD COMPUTING

**A. Take responsibility for security:**

In cloud data is being kept permanently; so many companies are working with cloud service providers. But sometimes conflicts can be raised; who should be accountable for making sure the cloud is secure.First, the organization need to know that what service actually cloud is providing and also where they have to place their information securely in the cloud.To keep the information securely we have to use the software called automated security software to detect the authorized persons who wants to access our data.

**B. Encryption:**

Encryption means to protect the data by the transformation of our data into the cipher text. By using this technique we can able protect our data from the unauthorized persons and they are not able read the information present in the cloud. To protect our data from hackers we have to use some encrypted keys and that keys should be given by

authorized users.To protect the data in the cloud we have to use some cloud service providers to store the data in the cloud. The most effective approaches for data security is encryption. We cannot decipher the content of any system, database, or file without a decryption key.

**C. Data protection:**

Even encrypted data may lead to damage due to the failed hardware, malicious operators or bad software .To reduces the frequent use of data we have to use snapshots or backups. Snapshots are technique where it keeps data as it is without any change but it adds the new versions only when a change occurs. In both cases, only a very small amount of data is exposed.

Backup is most familiar and easiest process for most situations. The copy of a backup is a data protection which is derived from the manufacture copy. When we restart an application, in order to regain data a backup copy is utilized.

**D. Data management:**

Many clouds and data centers suffer from sloppy data management. Trash collection is an extensive and challenging task, complicated by versioning of files. Trash collection mainly leads to more files with same or related names. The main responsibility of a critical file getting into a security less area can't be avoided. This leads to security risk. The answer is de-duplication on data which was intended to save storage space and removes extra copies from storage. De-

duplication won't get rid of files in wrong places. To puts, a life expectancy and location, copying and other controls on data require a metadata-driven approach. These tools are just entering the storage market.Data management provides the various flexibility and access to the data in a most efficient manner and it also provides the sharing of data to one another in a efficient purpose in business level.

**E. Protecting APIs and images:**

When app code get out of sync on images create some errors on the data. The data corruption occurs when the file contains the wrong data and it happens because of the careless of code. Because of lack of sync it is possible for malware. For automated updating of code images across all nodes the solution is to use available software.

**F. Secure Access:**

Many organizations' stores the data in the cloud. But the cloud service providers do not produce secure access. so, use multi-factor authentication, it's a bit slower but much safer.Many of the people face the issue is admin error. There is a risk with CLI-based software. Much of the data stored today is tied to mobile devices. So use two-factor authentication, but the risk of a mobile user accessing data in unauthorized places and stealing files is a crucial risk.

**G. Control shadows IT:**

Shadows IT stands for the portion of total IT spend today. Many organizations that are having back and forth in between shadow setups, that are in the cloud and corporate-control space, that is outer of IT's control and insecure. When a business team becomes frustrated with IT's lack of ability to deliver the needs which shadow IT wants.

This causes a major role in the security wall. By adding the encryption we can provide the more attractive service and also we can tightly controlling the access to the data by following just two steps by solving the shadow IT.

## V. CONCLUSION

The cloud computing stores the data without the effort of management and also it stores the software applications and it provides the services to the customers through the internet. But with this type of clod service management customers don't have trust commitments or policies. This effects the data storage and issues. To overcome the risks involved in the cloud we must follow some security challenges and also for storage of data. We took a look on Amazon s3 and third-party auditing (TPA) mechanisms which are used for data storage and security for data in the cloud.

## REFERENCES

[1] L.M. Vaquero, L. Rodero - Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud definition, in: ACM SIGCOMM Computer Communication Review,2008.p.50-55.

[2] M.B. Mollah , K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6.

[3] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010

Proceedings IEEE, 2010.p.1-9.

[4] Amazon.com, “Amazon Web Services (AWS),” Online at http://aws.amazon.com, 2008.

[5] http://www.business.att.com/enterprise/Service/hosting-services/cloud/storage/.