 ISSN: 2454-4248
85 – 88

Data Security Predicament in Cloud

Madhu Tickoo[#1]
Assistant Professor
PG Department of Computer Science
BBK Dav College for Women, Amritsar
Email:madhutickoo@gmail.com

Ruchi Kundra[#2]
Assistant Professor
PG Department of Computer Science
BBK Dav College for Women, Amritsar
Email:kundraruchi1983@gmail.com

Ramanjit Kaur[#3]
Assistant Professor
PG Department of Computer Science
BBK Dav College for Women, Amritsar
Email:raman_jit29@yahoo.co.in

Ridhima Sehgal[#4]
Assistant Professor
PG Department of Computer Science
BBK DAV College for Women, Amritsar
Email:ridhimasehgal2333@gmail.com

Shagun Arora[*]
Assistant Professor
PG Department of Computer Science
BBK DAV College for Women, Amritsar
Email:shagun.arora490@gmail.com

Abstract--Cloud computing a tremendous technology that today becomes the part of almost everyone's life. The cloud computing is used in homes, business organizations, in banking industries etc. Today, everyone is using cloud may be ranging from posting their pictures on social networking sites or by storing their crucial information. Although, the cloud is using in different areas, but for using cloud services, everyone faces some challenges associated with cloud. This study enlists some of the challenges of using cloud. Moreover, this study also describes some security requirements to limit threats and also some standards of cloud.

***KEYWORDS**: Cloud computing, Challenges, security requirements, protection standards.*

*****

I. INTRODUCTION

Among different resources available in the cloud, the most important is the user data. Data is increasing continuously, organizations with internet based revenue realized that most of their data is not being used. The renting of space for unused data adds to the cost. Organization can replace resources such as,server, memory or processing power by purchasing new resources. Furthermore, can get more bandwidth ondemand and pay for only the part that is used. The bandwidth belongs to cloud service provider and they can use as much as they want on a pay per use basis [1,2].

Every industry has to content with various data security perils and risks, for example, financial service organizations must allow certain data practice similarly, software development organizations face challenges with timely delivery, application security, and quality. Healthcare organizations too have problems associated with maintain patient's privacy. Therefore, cloud consumers must be aware of the kind of issues they are likely to face and the solutions to those problems.

II. ISSUES IN CLOUD

Data stored in cloud, faces the following crucial threats.

1. ***Data availability:*** A software or hardware fault or data integrity problem in one part of the infrastructure or data storage unit impacts not only that the part of the database, but also the entire environment. Hence, data availability and integrity are critical for the cloud to function.
2. ***Data Performance:*** Data is located at various data centers owned by the cloud provider. Data is far from the users has higher distance induced latency, and has low performance with synchronous rights, mirroring, and parallel read and write operations.
3. ***Price:*** Price for storage space and bandwidth to access the data varies by different cloud service providers. Some services offered by cloud service providers are more costly as compared to owing these resources
4. ***Underlying Complexity***: The underlying storage hardware can be heterogeneous, but it must be presented as a simple storage device and as a virtual storage pool to the end user.
5. ***Data Security:***Data security is the major concern in using the cloud services. Although, cloud service providers uses different parameters to secure user's data, but consumer

 ISSN: 2454-4248
85 – 88

always have some doubts about the security of data stored in cloud.

6. ***Data integrity***: With ease of access by the varied user types it is critical to manage data integrity. It is important for the cloud provider to understand the challenges and built in measures to resolves their issues because of all the data related problems.

III. Challenges with Cloud Data

In this section, we will discuss data related challenges in the cloud and how to implement effective mitigation measures.

1. ***Challenges with Data Redundancy***: Concurrent data access by multiple customers at all times and due to a mix of hardware types, complicated setting up data protection in any cloud. In any case, the copies of data must be stored at various locations and replicated in synchronized manner. When replicating across data centers, the system must be aware the data location latency, user workload and activity such as backup, report generation application testing etc.
2. ***Challenges with Disaster Recovery (DR):***Disaster Recovery in cloud computing is one of the most vital selection criteria when evaluating cloud providers. On one hand, DR with cloud computing has several benefits such as cost effectiveness, ease of implementation, scalability and quick provisioning on the other hand, there are numerous issues with the cloud-based DR which are as follows:
    - *Initial Data Copy for Existing Data*: For large sets, it is not possible to make the first data copy over the wide area network by cloud consumer to the cloud provider. Hence, a manual process, such as copying data to tape or hard disk and shipping the device to the cloud provider datacenters, takes less time.
    - *Limited or No support for Some Operating Systems:* Most public clouds DR providers support common operating environments such as MS windows or Linux. There is no support for older, non-Web-based or less common operating systems such as, Solaris or AIX.
    - *Insufficient Bandwidth:* Most DR providers prefer to create backup with incremental updates instead of taking a full copy.
    - *Financial Consideration:* It makes financial sense for small and mid-sized organizations that have less data to use cloud for DR. however, for organizations that have vast amount of data, a captive or owned DR site is more cost effective.
    - *Supplier Issues:* Some cloud providers do not take the effort and time to understand the customer-specific needs. They, therefore, cannot justifiably meet all the DR requirements of the customers.
3. ***Challenges with Data Backup:*** there are several problems related to backing up of cloud data. Following are some of them:
    - If you download cloud data to your in-house hard disk or tape, you need to pay for the bandwidth.
    - You need a safe place to store the data and frequently check the media integrity of the backup device.
    - If you keep the backup data in the cloud, you need to harden the security around it to protect it from hackers and malware attacks.
    - Data recovery to a cloud based service site is tough, slow and prone to transfer interruptions. This is more pronounced if you need to upload a large amount of data to the cloud over a WAN connection.
4. ***Challenges with Data Replication:*** Data replication is the process of creating copies of user data and application to use in case the data at primary service site is corrupted, deleted, or unavailable. The problem with the replication is that the location of data copies is dynamic.There are two types of replication, each having its own issues when resident in cloud:
    - *Synchronous Replication*: in this type of replication, replicate copies are always in-sync with the primary site. This is used to replicate with distances of kms, where latency is not expected to impact performance. This type of replication is not preferred in the cloud, because data is copied over the WAN, and its performance can impact many customers.
    - *Asynchronous Replication:* In this type of replication, the replicated data lags behind the primary data by a time period of minutes to a few hours. This is common in the cloud, but it impacts performance. It is inconvenient and difficult to freeze a database, even momentarily, to gets snapshots.
5. ***Challenges with Data Residency or Location:*** In the cloud, the location of data can pose a compliance and legal problem. For your data, you need to know which legal requirements you must comply with. Certain governments restricts the access of data according to the local or country laws. For certain data types, you must keep the data within the region or the country.

 ISSN: 2454-4248
85 – 88

6. ***Challenges with Data Reliability:*** service reliability in the cloud is a concern because of several reasons. Some of them are the following:
   - Heterogonous hardware and software components
   - Connectivity over multi-vendor WAN
   - Massive user-base sharing the same resource pool
   - Ease of access for users.
7. ***Challenges with Data Fragmentation***: With numerous users simultaneously working on different datasets in the cloud, the user data is slit or fragmented into many pieces and stored in various storage locations. The spread of data and overhead of keeping tracks of where different parts of the data are located, leads to inefficiency and degrades read-writes performance. The provider must adopt comprehensive data management techniques to reduce user-data fragmentation.
8. ***Challenges with Data Integration:*** Various factors leads to challenges in cloud data integration, such as the following:
   - *Content Distribution:* Contents of the file resides in different datacenter and various subsystems in the same datacenters.
   - *Exchange of Data*: The cloud data interacts with applications residing on other public or private clouds. This exchange of data between cloud applications presents the challenges of having a compatible data format and application interfaces.
   - *Speed of Change*: The are innumerable changes per second and keeping track of the data poses a tough challenge for integration
   - *Distribution control*: The control over the data is shared between the cloud provider and the consumer. This increases the integration challenges.
   - *Connectivity:* Cloud data can be accessed only when the user and the services are online. The integration and work done require bandwidth, which in turn depends on the amount of transaction and work at hand.

IV. Security Requirements to Limit Threats

1. ***Data Confidentiality and Encryption***: Data confidentiality in the cloud is a way to protect data or messages from being understood or used by unintended users or tenants of the cloud. A common way to achieve data confidentiality is to encrypt the data [4]. Even if unauthorized party access the data, he or she cannot use it. Cloud data is encrypted with an algorithm or a key. The encrypted data is called cyphertext.
2. ***Data availability***: If the user keeps the data confidential and secure, it must also be available to them whenever they need it. The SLAs (service Level Agreements) with your cloud provider must have uptime agreements. Data or service availability is expressed as a percentage of uptime in given year or month. The SLA with cloud service provider must refer to monthly allowed downtime. If the downtime is more on the monthly or annul basis, the SLA must specify how much of the extra downtime is converted to service credits and how it is converted.
3. ***Data Integrity***: Data integrity is one of the most critical elements in any information system. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Managingdata confidentiality makes sure that the data in the cloud cannot be read or understood by unauthorized parties [3,5]. Data availability makes sure that user can access data when they want to. However, the encrypted data in the cloud must not be intercepted or modified by unauthorized parties while it is in-transit or at rest. If it gets modified, users are unable to trust the content. In other words, the data is invalid and lacks integrity. The user needs to reactively detect if the data has been modified and prevent such occurrences from happening again.

V. Standard To Protect Data in Cloud

1. ***Cloud Data Management Interface:*** A new standard to protect the data is the Cloud Data Management Interface (CDMI) from Storage Networking Industry Association (SNIA). CDMI allows user to tag the data with special metadata. The metadata can be used to code services that must be provided such as encryption, backup, reduplication, replication, compression, archiving etc. These services increases the value of user data existing in the cloud.

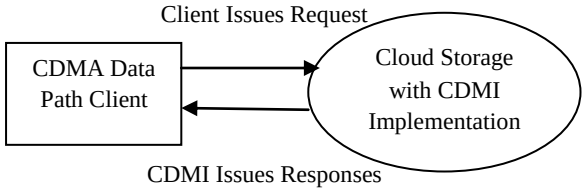

Figure1: Implementation of SNIA's CDMI

CDMI is the first industry-developed open standard for cloud data. It enables inter-operable cloud storage implementations from various cloud service providers and

 ISSN: 2454-4248
85 – 88

storage vendors. The standard was created by the SNIA Cloud Storage Technical Work Group (TWG).

2. ***Cloud Storage Gateways (CSGs):*** To address the security and performance issues in pubic clouds, consumer organizations can use CSGs. The CSG in an appliance residing in the customer's premises and provides the data protection by encrypting, compressing and archiving datasets before moving the data to a cloud. A CSG could be in the form of the hardware appliance with a cache that can be installed within your corporate office or datacenter.

A CSG at the corporate office intercepts and manages all the input/output between the users and the cloud storage providers. A CSG could also be a downloadable software program that can be installed on sever at the customer location. CSGs have a local cache to store data temporarily. Users can download CSG software and configure a local storage device as the cache. CSGs eliminate the issue of vendor lock-in, because they support various formats and facilitates data backup.

VI. Conclusion

In nutshell, we can say that cloud computing is the demanding technology in almost every business organisation. It reduces the work load and cost of the resources to the organisation by providing the resources over the internet at cheaper rate. This study provides the brief details about the cloud computing. This study provides the information about the challenges in the cloud. The future scope of this study is to compare the standards entitled in this study by applying them in a simulation environment.

References

[1] Beri, R. (2015). Descriptive Study of Cloud Computing : An Emerging Technology, (March), 1401–1404.

[2] Gupta, K., Beri, R. &Behal, V., 2016. Cloud Computing : A Survey on Cloud Simulation Tools. , 2(11), pp.430–434.

[3] Sun, Y. et al., 2014. Data Security and Privacy in Cloud Computing. , 2014.

[4] Agarwal, T., 2012. Cloud Computing : Security Issues , Mitigation and a Secure Cloud Architecture. , (December).

[5] Munir, K. &Palaniappan, P.S., 2013.Secure Cloud Architecture. , 4(1), pp.9–22.