Survey of Data Protection Mechanisms to Protect Data at Rest on Cloud

Omkar Ghaisas[1], Prof. Yogita Borse[2],
Department of Information Technology, K. J. Somaiya College of Engineering, Mumbai, India

***Abstract*— Cloud computing is very advanced and widely used technology of today's world. Cloud computing became famous after the advancements in storage capability of cloud. But cloud is a shared pool of resources. Hence our data is stored on public storage along with data of other cloud subscribers. This possesses the risk that our data might be compromised. Storage security mechanisms are required to protect data privacy and integrity. Data can be categorized into two categories which are data at transit and data at rest. This paper discuss the survey of different cloud providers with respect to data encryption, access control and data recovery on data at rest.**

***Index Terms*— Cloud computing, Data protection mechanisms, Storage security, Data at rest, Cloud comparison.**

I. INTRODUCTION

Cloud computing has been envisioned as the next generation paradigm in computation. As lot of industries are recently moving towards cloud computing they tend to store their data on clouds which may contain confidential data. Data security or storage security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places all over the globe. Cloud service providers are responsible to provide security of that data. Also cloud subscriber is responsible to protect their data as they cannot just rely on service providers for protection of their data.

Currently there are different cloud service providers like AWS, Microsoft azure, Microsoft onedrive, Google cloud, Dropbox and many more. These service providers allow subscribers to store large amount of data on cloud. Hence they also provide various security mechanisms in order to protect user data.

Data can be categorized into two categories based on providing protection-

1) Data at transit- Data at transit means data moving from one location to another location over internet or over a private network. Data protection during transit includes protecting data from network to network or local storage to cloud.
2) Data at rest- With respect to cloud data at rest includes the data stored in cloud storage. Data protection of cloud storage includes protecting data which is stored on cloud.

In order to provide protection to this data cloud providers provide various security mechanisms. These mechanisms include-

1) Access control- Access control involves restricting access to resources which could include confidential data. This prevents unauthorized users from accessing data stored on cloud. Access control generally includes authentication, authorization, auditing and accountability.
2) Encryption- Encryption mechanisms makes information unreadable for unauthorized users. This is achieved by using encryption algorithms. This mechanism is used for protecting sensitive and confidential data and can only be decrypted by using a shared secret which can be encryption key.
3) Data recovery- Data recovery is a process of recovering lost, damaged or corrupted data. Data recovery mechanism is required when we are storing critical and sensitive data.
4) Physical security- Cloud data is stored in data centers and servers. This data centers should be protected from intruders. These data centers can be a target for attackers as they contain sensitive data of multiple cloud users. Server racks and data centers should be locked in a rack suits or cages.

II. LITERATURE SURVEY

AWS has multiple services when it comes to data storage. Amazon s3, Amazon EBS, Amazon EMR, Amazon DynamoDB and Amazon RDS. Amazon s3 provides repository for internet data. It is a object storage and is suitable for storing huge data like backups. Amazon EBS can be used by Amazon Ec2 instances and can be used to store drives of virtual machine. Hence they are accessible only via virtual machines. Amazon RDS can be used to store database. Amazon takes into consideration multiple concerns which are Accidental data disclosure, accidental data deletion, data integrity and data availability.[1] Amazon S3 provides bucket level and object level permissions along with IAM to provide access control. It also offers both server side as well as client side encryption. Amazon EBS offers Microsoft EFS encryption if using Microsoft Windows

TABLE I

COMPARISON BETWEEN CLOUD PROVIDERS WITH RESPECT TO DATA SECURITY

	AWS	Google Cloud	Azure	One Drive	Dropbox
Encryption	AES-128, AES-256	AES-128	AES-256, RSA-256	AES-256	AES-256
Type	Symmetric	Symmetric	Symmetric, Asymmetric.	Symmetric	Symmetric
Key Management	Microsoft Windows EFS	Google-wide KMS	Azure Key Vault	Azure Key Vault	Dropbox key management infrastructure
Client side encryption	✓	×	✓	✓	×
Access Control	AWS IAM	Google IAM	Azure Active Directory (AAD)	Azure Active Directory (AAD)	×
Multi Factor Authentication	✓	✓	✓	✓	✓
Role based access control	✓	Kubernetes version 1.6	✓	✓	×
Data recovery	✓	✓	✓	✓	✓
data on cloud after deletion	persists till data is overwritten	upto 25 days	till data is overwritten	upto 30 days	from 30 days to 1 year
Data recovery mechanism	versioning	call techincal support	Recovery services vault	Recover from recycle bin	versioning

server. Amazon RDS include mechanisms like encryption, hashing and compression.[2]

Google cloud provides storage service which can be categorized into two types which are high frequency storage for storing objects and low frequency storage for storing backups and archives.[3] Google storage is designed for 99.999999999% durability. The data stored in Google Drive can be from Gmail, calendar, drive, docs, sheets etc. This data is encrypted and stored on Google cloud.[4]

Microsoft Azure provides variety of data storage solutions like file storage, disk storage, blob, table storage.[5] The services which offer storage are Azure SQL database, CosmosDB and Azure data lake. Azure provides complete encryption services at both server side and client side.[6]

Another cloud service that Microsoft gives is Microsoft SharePoint and onedrive. Both the services are available in Office365. Onedrive can be thought as a part of documents folder whereas SharePoint can be used as internal website. These services manage data with versioning and metadata. Microsoft has financial back guarantee with commitment to deliver 99.9% uptime.[7]

DropBox contains storage server, block server and metadata servers in order to store data. Hence Dropbox stores two kinds of files which include Metadata and Actual file content[8]. Dropbox can store data in AWS or magic pocket. Files are encrypted before storage.[9]

III. SECURITY ANALYSIS

Please refer to TABLE 1 given below for comparative study of different cloud providers on basis of protecting data at rest.

A. Encryption-

Generally all the service providers provide symmetric encryption which is either AES-128 or AES-256. In terms of providing encryption Microsoft Azure would be consider as better than other services as it allows user to encrypt data using Data Encryption key which AES-256 encryption and this key is encrypted by using Key Encryption Key which is done using RSA-256. As Google Drive and Dropbox comes under Saas(software as a service) it doesn't support client side encryption. But users of Google drive and Dropbox are free to Encrypt data before uploading.

B. Access Control-

All the service providers have identity access management polices apart from Dropbox where AWS allows group based and role based access control policies. AWS has separate credentials for each user and has multi-factor authentication. In Google Drive the End-user makes RPC request to the contact which is central user identity for End-user permission ticket. When user accepts the end-user gets cookie or OAuth token. Microsoft Azure and OneDrive both have access control based on Azure Active Directory. These Directories are placed at 28 data centers around the world and have very high availability. It gives IAM services and also stores keys.

C. Data Recovery-

In AWS and Azure if we delete data it still persists on the cloud and is not deleted. It is overwritten by new data. If different user tries to use that data block then previous data is zero filled. Onedrive and Google drive removes the deleted data within 25 to 30 days. Dropbox also removes deleted data in 30 days but if user has subscribed to extended version history pack. Microsoft Onedrive sends data recovery to recycle bin which makes recovery of data much easier. Azure use recovery services vault where user can store backups. AWS and Dropbox use versioning for data recovery. If any user accidentally deletes data then user can recover cloud to previous version state. For recovering Google data there is

no specified mechanism but technical support can recovery data.

IV. CONCLUSIONS

In this paper survey of different Cloud providers with respect to data stored in cloud servers or data at rest. The comparison is done with respect to three data security concepts which are encryption, data recovery and access control. If encryption or confidentiality is the primary concern then Microsoft Azure provides most protected mechanism. Every cloud service provider considered in this paper uses symmetric encryption AES-128 and AES-256. Azure and AWS has more complicated access control policies as compared to other cloud providers which would be better for users with complex requirements. Google drive has very simple access control policy and hence users with complex requirements should avoid it. Microsoft Onedrive has simple data recovery mechanism, whereas versioning allows AWS and dropbox to recover data from previous versions. If a user is storing very confidential data then they must take into consideration that in AWS and Azure deleted data still exists on the cloud physical storage.

REFERENCES

[1] Amazon Web Service .AWS Security Best Practices(Whitepaper)2016. Print.
[2] Amazon Web Service .Overview of AWS Security - Storage Services(Whitepaper)2016. Print.
[3] Google Cloud. G Suite Encryption Whitepaper. Print.
[4] Google cloud. Google Cloud Security and Compliance Whitepaper 2018. Print.
[5] Microsoft. Microsoft Azure Detail(Whitepaper)2018. Print.
[6] TCS- Windows Azure The Cloud Computing Platform TCS Perspectives(whitepaper)2018. Print.
[7] Microsoft .File security in Microsoft SharePoint and OneDrive for Business(Whitepaper)2016. Print.
[8] Dropbox. Privacy and Data Protection(Dropbox Business whitepaper) 2018 v2018.03.Print.
[9] Dropbox. Dropbox Business Security(Dropbox whitepaper)2018. Print