ENCRYPTION TYPES AND KEY MANAGEMENT IN CLOUD STORAGE PROVIDERS

Abdullahi Osman [1], Yazeed Al Moaiad [2]

Al-Madinah International University, Malaysia

[1]cc604@lms.mediu.edu.my

[2]yazeed.alsayed@mediu.edu.my

Abstract: **The increase of data for individuals and businesses leads to be protected due to avoiding any unacceptable loss. Cloud storage services providers guarantee to give a solution to this difficulty. In current times, cloud storage service demand has increased a significant way. They give user-friendly interface, free storage or pay-as-you-go to store, manage, synchronize, share, automatically back up data and download. In addition, businesses and a part of individuals hesitate to utilize cloud storage services due to losing control over it. Many obvious attacks on cloud storage providers have annoyed these concerns. Cloud Storage aims to improve efficiency and productivity in terms of securing the data. The data stored on the cloud must be secure while transiting, sharing or resting at the data centers or servers. Securing includes that the cloud storage providers (insiders) cannot understand or read the stored data as plaintext. In this investigation, we have to examine the security mechanisms and key management of popular cloud storage services based on an online survey of how many users for each cloud storage provider: Google Drive, iCloud, Dropbox, OneDrive, Amazon Drive and Mega. The investigation will help the users to consider services.**

Keywords: **Cloud Storage Service Providers, Cloud Security, Encryption, Key.**

I. INTRODUCTION

Rajan (2012) state that cloud computing changes the current IT infrastructure; it has developed and managed by services providers in three service models: Infrastructure-as-a-Service (IaaS), Storage as a Service (StaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). It gives on-demand over the internet to access pools of flexible computing resources. The resources hosted and provided by cloud service providers as a service over the Internet network, the cloud-computing providers facilitate their resources to the customers.

Spoorthy et al. (2014) descried cloud data storage as a service known as Storage-as-a-Service (StaaS), which aids to facilitate cloud applications to scale, beyond their restricted servers. Cloud data storage service or StaaS enables the users to store and share their data on remote servers over the Internet by permitting the users to ac-cess the data anytime from anywhere.

Müller et al. (2017) mentioned that the cloud storage providers deliver an unlimited capacity of resources to their user's on-demand and pay-as-you-go over network access, including file synchronization and sharing functionality. The probably most examples of cloud storage providers are Dropbox and Amazon S3. However, Drop-box Microsoft and OneDrive.

Cloud security alliance (2012) characterized data stored on the cloud is referred to the data when it is stored, transmitted, or processed by a Cloud Service Provider. The data should be stored, shared, transmitted or pro-cessed securely. If the data is deleted from cloud storage servers, the providers must guarantee that it is purged in a proper approach and cannot be reached by anybody else in the future. Ant related records of the data, such as logs.

To understand cryptography and encryptions algorithms it is important to consider data security while transiting and at resting. In common, data while transit is secure due to implemented Transport Layer Security (TLS) protocols such as Hypertext Transfer Protocol Secure (HTTPS), the used key one-time keys for only that specific transmission. No, need for a holds the key, which assists to keep the data secure.

However, data stored in the servers or datacentres (data at rest) require using a different type of encryption method to generate a key used to decrypt the data.

Cloud Service Providers implement encryption techniques to secure and protect the data stored on their servers. For useful security, the encryption keys must be constructed, managed and protected accurately. This paper aims to examine the security mechanisms applied by Cloud Service Providers.

II. ENCRYPTION METHODS AND KEY MANAGEMENT OFFERED BY CLOUD STORAGE PROVIDERS

A. Encryption Methods And Key Management Offered By Cloud Storage Providers

The main purpose to implement encryption algorithms is to prevent the confidentiality of data from be-coming a data breach. Security methods and key management implemented to increase the level of data protec-tion while privileging access-level breaches.

The type of encryption method and key management may affected the level of security in cloud storage.

- Client-side encryption – users encrypt their own data, by their own key.
- Server-side encryption, keys held by server – users upload data to their cloud provider encrypt the data.
- Server-side encryption, keys held by client – users hold their own key but the server encrypt the data.
- End-to-End encryption, encrypted on the one end and decrypted on the other end, so only the sender and receiver can read it by using public/private keys.

Client-side encryption is a mechanism to encrypt the data using a secure key that is constructed using encryption algorithms at the end-user device. Applying encryption at the client-side converts plaintext information to Ciphertext, which means that the data is transmitted outside of the user's side securely (Seltzer, 2016).

Server-side encryption is a mechanism to encrypt the data using a secure key, which is constructed using encryption algorithms at the server but the key held by the users. Applying encryption at the server-side converts plaintext information to Ciphertext at rest (in the server), which means the data is transmitted outside of the user's side as plaintext.

Server-side encryption is a mechanism to encrypt the data using a secure key, which is constructed using encryption algorithms at the server but the key held by the server. Applying encryption at the server-side converts plaintext information to Ciphertext at rest (in the server), which means the data is transmitted outside of the user's side as plaintext.

End-to-end encryption defines as a method of communication between the sender and the intended recipient(s) securely and privately. In end-to-end encryption, the encryption is performed at the device level; the keys are stored with the participants' devices. The data is encrypted before it transmits the end-user device and decrypted when reaches its destination Preveil (2018). Different security mechanisms can make a huge difference in the level of security provided (see figure1)

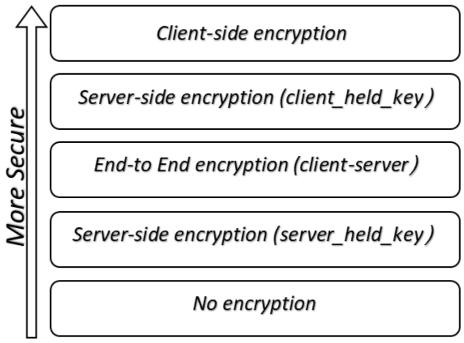
Client-side encryption
Server-side encryption (client_held_key)
End-to End encryption (client-server)
Server-side encryption (server_held_key)
No encryption
More Secure

FIGURE 1: TYPES OF SECURITY MECHANISMS OFFERED BY CLOUD STORAGE PROVIDERS

B. Types of attacks in Cloud storage

Implementing encryption will protect data from three sets of parties:

- First party – malicious insider
- Second-party – the cloud provider
- Third-party – hackers/cybercriminals

III. RESULT AND DISCUSSION

A. Analysis of the different types of attacks associated with security methods

Cloud storage suffers from several attacks and unauthorized access due to the services are available on the public internet. Therefore, in this part we will focus on the different types of attacks that are typically related to specific security methods

- No encryption (level 0): It costs nothing and provides zero protection.
- Server-side encryption (levels 1): It is simple, convenient and gives limited protection from outside attacks.
- End-to-end encryption (level 2): It is much secure especially while transmitting the data and gives protection against cybercriminals
- Server-side encryption (levels 3): It is extremely secure but it seems impractical due to the key generate at the client-side and the trade-off of the key may be failed. It protects against a wide range of attacks.
- Server-side encryption (levels 4): It is the most secure and sufficiently gives total protection most time.

Table 1 will explain how different data breach attacks affect the security methods in cloud storage.

TABLE 1: ANALYSIS DATA BREACH ATTACKS AFFECT THE SECURITY METHODS.

Providers	Server-side encryption (server held the key)	End-to-end encryption (Two keys)	Server-side encryption (client held the key)	Client-side encryption (client held the key)
Google Drive	✔		✔	
iCloud	✔	✔		
Dropbox	✔			
OneDrive	✔			
Amazon Drive	✔		✔	
Mega nz		✔		✔

***Note*. Adapted from eeNews Europe website, by Chang, L. (2018)**

B. A comparison between cloud storage providers in term encryption techniques and key management

Cloud storage services providers try to secure the user data with different levels of encryption, in this part; we will see the comparison between some providers in terms of encryption side and key management.

Table 2 will explain how different cloud storage provider's encryption techniques and key management storage services providers try to secure the user data with different levels of encryption, in this part; we will see the comparison between some providers in terms of encryption side and key management.

TABLE 2. ANALYSIS ENCRYPTION TECHNIQUES AND KEY MANAGEMENT AFFECTED BY BREACH ATTACKS AFFECTED.

Factors	**First Party (malicious insider)**	**Second-party (cloud provider)**	**Third-party (hackers/cybercriminals)**
Client-side encryption (levels 4)	**High**	**High**	**High**
Server-side encryption (levels 3)	**Low**	**Medium**	**High**

End-to-end encryption (level 2)	**Low**	**Medium**	**High**
Server-side encryption (levels 1)	**None**	**Low**	**None**
No encryption (level 0)	**None**	**None**	**None**

Note. Adapted from (Apple, 2019; Dropbox, 2020; Google Cloud, 2020; Microsoft, 2020; Mega, 2020)

IV. CONCLUSION

The experiments conducted show that using different levels of encryption techniques and key management in cloud storage services will affect system security in terms of confidentiality and privacy. This will influence user reliability and selecting cloud service providers. The paper aims to help users to select the best service provider with understanding their requirements of security to protect their data against any possibility of breach data.

Future works will be more comprehensive and take into account the encryption algorithms and data integrity, which gives high trust security. It also helps the users to protect their privacy by selecting the best providers that provided a high level of security with various priorities of services.

REFERENCES

[1] Apple. (2019, July 3). ICloud security overview. Retrieved from Apple Support website: https://support.apple.com/en-us/HT202303

[2] Chang, L. (2018, May 14). Client-side vs server-side encryption – who holds the key? R trieved April 15, 2020, from eeNews Europe website: https://www.enewseurope.com/design-center/client-side-vs-server-side-encryption-who-holds-key/page/0/1

[3] Cloud security alliance. (2012). Retrieved from https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_8_Encryption_Implementation_Guidance.pdf

[4] Dropbox Business. (n.d.). Secure, scalable infrastructure. Retrieved from www.dropbox.com website: https://www.dropbox.com/business/trust/security/architecture

[5] Google Cloud. (2020a). Data encryption options | Cloud Storage. Retrieved April 15, 2020, from Google Cloud website: https://cloud.google.com/storage/docs/encryption/?hl=ar

[6] Mega. (2020b). MEGA help. Retrieved April 15, 2020, from help.mega.nz website: https://help.mega.nz/webclient/security-and-privacy.html#how-does-the-encryption-work

[7] Microsoft. (2020c). How onedrive safeguards your data in the cloud. Retrieved from Office.com website: https://support.office.com/en-us/article/How-OneDrive-safeguards-your-data-in-the-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1

[8] Müller, S., Pallas, F., & Balaban, S. (2017). ON THE SECURITY OF PUBLIC CLOUD STORAGE. Retrieved from http://www.ise.tu-berlin.de/fileadmin/fg308/publications/2015/Mueller_Pallas_Balaban_Security_of_Public_Cloud_Storage.pdf

[9] Preveil. (2018). End-to-end encryption at entperprise scale. Retrieved April 15, 2020, from PreVeil website: https://www.preveil.com/end-to-end-encryption/

[10] Rajan, R. A. P. (2012). Evolution of cloud storage as cloud computing infrastructure service. IOSR Journal of Computer Engineer-ing, 1(1), 38–45. https://doi.org/10.9790/0661-0113845

[11] Seltzer, M. (2016). Security Final Paper Client Side Encryption in the Web Browser Mentor: Ming Chow. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2015/mseltzer.pdf

[12] Spoorthy, V., Mamatha, M., & Santhosh Kumar, B. (2014). A survey on data storage and security in cloud computing. International Journal of Computer Science and Mobile Computing, 3(6), 306–313. Retrieved from https://www.ijcsmc.com/docs/papers/June2014/V3I6201444.pdf