ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

PRIVACY PRESERVING ADVANCED SECURITY ON UNTRUSTED CLOUD WITH SELF BACKUP PROCESS

Sadeer Dheyaa Abdulameer [*1]
[*1] Faculty of Computer Science, Cihan University, Sulaimaniya, Kurdistan, Iraq

DOI: https://doi.org/10.5281/zenodo.570184

Abstract

Cloud Storage service are frequently required for many corporate and government organizations. Most of cloud storage service providers are un-trusted, so it is not safe to keep the data in cloud for long period. Many are using cloud storage for data sharing that means it is not possible to send a big file in email, maximum 25 GB are allowed, for big files, files are uploaded in cloud storage and link is given to the data consumer. After Data consumer download the file, Data owner has to delete the file from the cloud for the security reasons, but most of time Data Owner forget to delete the file. To overcome this problem data self-destruction is proposed in many papers and now proposed system has Self-Destruction cum Self-Backup Process, which help the file to stay in the public cloud for certain period of times and it will be removed from the cloud storage and securely stored in another storage. To verify the integrity of the file HMAC is created while file is uploaded and Data Consumer can able to download the file and generate the HMAC, check the integrity of the file.

Keywords: Cloud Storage; Data Self-Destruction; Self-Backup; HMAC - Hash Message Authentication Code.

Cite This Article: Sadeer Dheyaa Abdulameer. (2017). "PRIVACY PRESERVING ADVANCED SECURITY ON UNTRUSTED CLOUD WITH SELF BACKUP PROCESS." *International Journal of Research - Granthaalayah*, 5(4), 176-181. https://doi.org/10.5281/zenodo.570184.

1. Introduction

Public Cloud file storage and retrieval system have gained increasing popularity to support various cloud services. To provide services efficiently, Cloud service providers are inventing new ideas by keeping in mind how to give additional security to the user's sensitive data. They also have a big risk to user data since the cloud large storage networks are usually not secure and experience with software / hardware faults. Cloud Storage data always contain user's privacy & secrets; the responsibility is very high for the cloud service provider (CSPs) to ensure the data

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

privacy and security protection for the users. However, achieving these aim are big challenge especially when considering cloud environment.

In this paper, to provide security to the user's sensitive data secure self-backup process is introduce with self-destruction system. Another name for self-destruction is SafeVanish which means the data in the cloud storage will be deleted automatically at certain time interval. This system has the Secure Self Backup process which will provide additional features the user. When the user needs the uploaded data after the self-destruction process, in this system he can able to retrieve by Request System. Request System is developed to help the user when the user want the data which he uploaded and which is not available now, to send the request to the Admin and get it back.

Another feature in this system is the use of Hash Message Authentication Code (HMAC), which ensures the data integrity. HMAC is a message authentication code calculated by a secure hash function combined with a key. Only the key holder can calculate and verify HMAC.

2. Proposed System

In proposed system user as to provide Time to Live (TTL) for each and every file which is uploading into the cloud storage. While file is uploading Hash Message Authentication code (HMAC) for the file content is generated and stored in database for integrity check.

Self-backup process is running in cloud which has to check files in the cloud storage whether the Time to Live (TTL) is expired or not in periodic interval. The files which are expired as to be removed from cloud storage and it has to encrypted and stores it in self backup storage.

When the user who uploaded the file into the cloud and he had the requirement to get it back, in this situation the required file is not in cloud storage then he as to send request to admin to ask him to restore the required file to cloud storage. It is the responsibility of admin to verify the user request and trigger the operation of restoring process which will pick the file from backup storage and decrypt it then restore in cloud storage. While user is downloaded the file with the help of HMAC integrity test is conducted and result shown to the user.

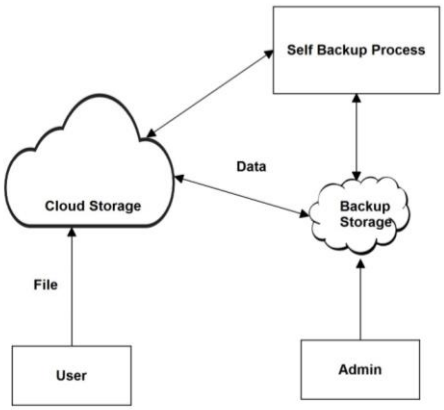


Figure 1: System Architecture

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

3. Self-Backup Process

Let there are N number of files in cloud storage. This self-backup process has to check each and every file in cloud storage in certain time interval for the expiry of Time to Live (TTL) of the file. The self-backup process clearly showed in Fig 2. Where UT is Uploaded Time, CT is Current System Time, consider a file F. uploaded at time 5:00 and user set TTL as 6 hours.

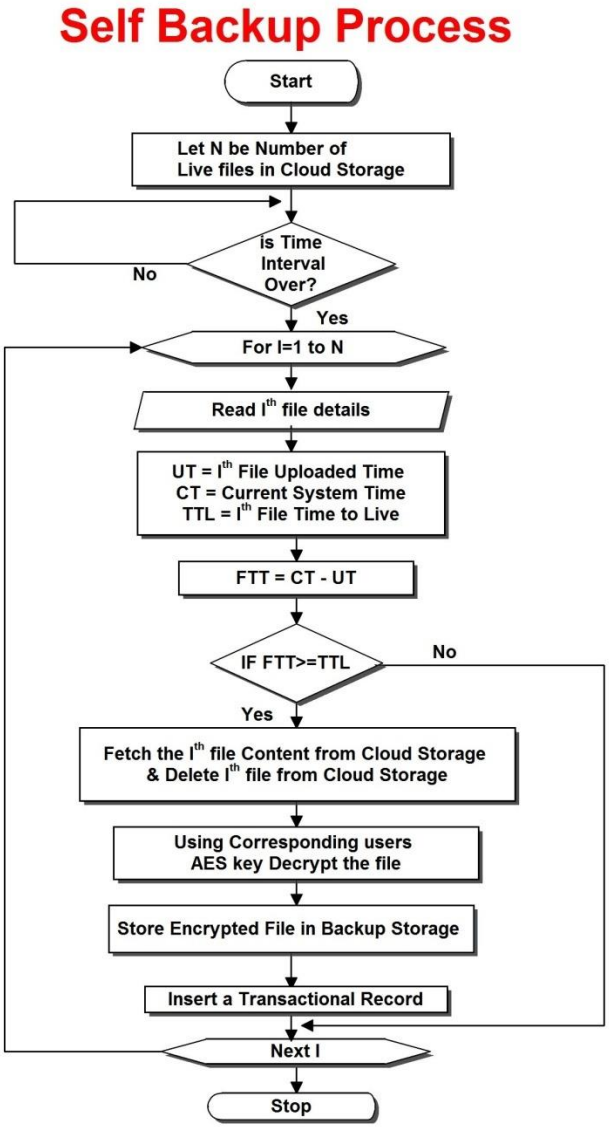


Figure 2: Secure Self Backup Process

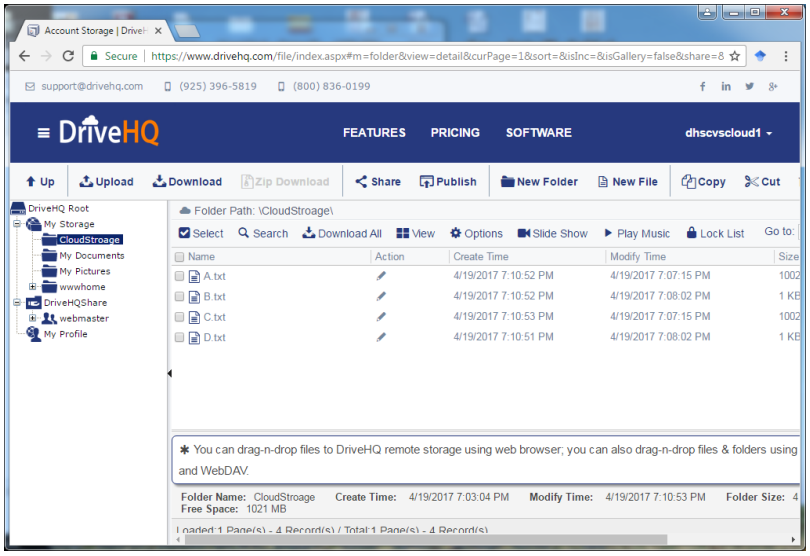
When Secure Self Backup Process is triggered, process has to get CT (Current System Time) it has to calculate FTT (File Terminating Time) by calculating CT-UT consider now system time is 11:05 then for the file F, ***FTT = 11:05 - 5:00*** and the result is 6:05, then it has to check the condition ***FTT >= TTL*** that is in this case ***0.65 >= 6***, which is true here. Then self backup process has to remove F from cloud storage and encrypt the file F and store it in self backup storage. This process is explained clearly in **Fig 2**.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

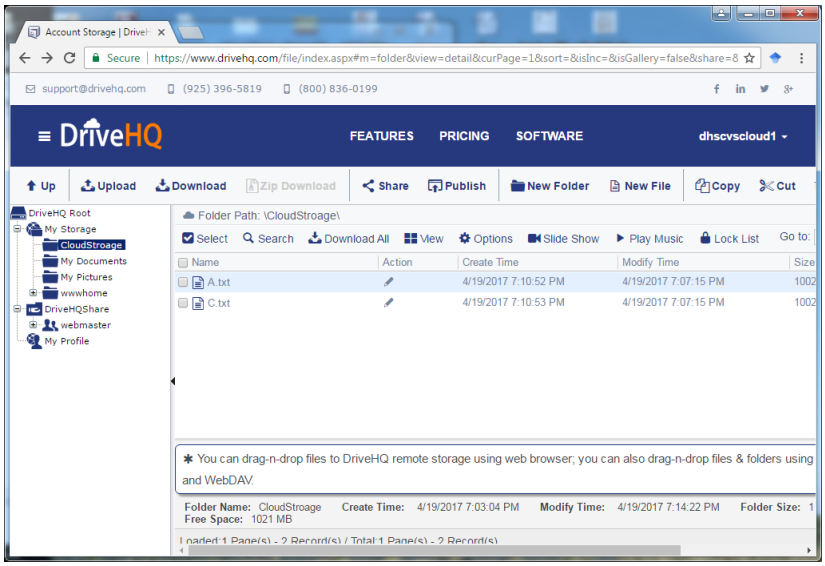
4. Experimental Process

The following three output screen shows the experimental result of this system clearly, a user uploaded four files A, B, C, D in cloud storage at 7:10 PM and set time to leave for file B, D 5 minutes and for A, D 60 minutes.

When Secure Self Backup process happen it removes files B, D from cloud storage and encrypt the file place it in self backup cloud storage which is showed in below screen shots.

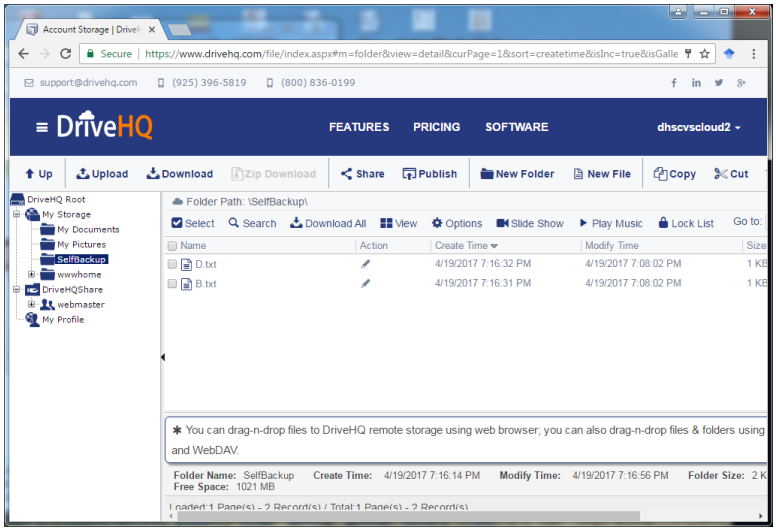


Screen Shot 1: After File Upload (Cloud Storage)



Screen Shot 2: After Backup Process (Cloud Storage)

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86



Screen Shot 3: After Backup Process (Self Backup Storage)

5. Conclusion

This paper introduced Secure Self Backup Process on Untrusted Cloud Storage, which has an automatic time interval based self-destruction system and Secure Self-backup and authentication based restore system. The new invention in this system is a user can able to retrieve the data which is uploaded in cloud and which is deleted based on SafeVanish process. For the security purpose the backup data are encrypted and store in Self Backup Cloud Storage. For data integrity check HMAC is used. This system is tested with experimental data and it meets all the functional requirement of the system.

We demonstrated the feasibility of Secure Self Backup Process by implementing a proof-of-concept prototype, which has the function to destruct the user's sensitive information without any user's interactions and the deleted data in cloud storage is encrypted and stored in self backup storage for future use.

References

[1] L Zeng, S Chen, Q Wei, D Feng - APMRC, "SeDas: A self-destructing data system based on active storage framework," APMRC, 2012 Digest, 2012.
[2] Y. Zhang and D. Feng, "An active storage system for high perfor-mance computing," inProc. 22nd Int. Conf. Advanced Information Networking and Applications (AINA), 2008, pp. 644–651.
[3] M Li, S Yu, Y Zheng, K Ren," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", in IEEE Transactions on Parallel and Distributed Systems 2013 .
[4] Y Zhou, D Feng, W Xia, M Fu, F Huang," SecDep: A User-Aware Efficient Fine-Grained Secure Deduplication Scheme with Multi-Level Key Management", in Mass Storage Systems and Technologies (MSST) 2015.
[5] J. Li, X. Chen, M. Li, J. Li, P. P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 6, pp. 1615–1625, 2014.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

[6] J Wei, W Liu, X Hu," Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption, in IEEE Transactions on Cloud Computing 2016.
[7] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.
[8] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.
[9] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," inthe Proceedings of IEEE INFOCOM 2012,2012, pp. 693–701.
[10] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, andQ. Zhou, "Feacs: A flexible and efficient access control scheme for cloud computing," in Trust, Security and Privacy in Computing and Communications, 2014 IEEE 13th International Conference on, Sept 2014, pp. 310–319.

*Corresponding author.
E-mail address: sadeer.alatter@gmail.com