Research Journal of Applied Sciences, Engineering and Technology 8(3): 354-357, 2014
DOI:10.19026/rjaset.8.980
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: February 22, 2014 Accepted: May 19, 2014 Published: July 15, 2014

Research Article

Enhancing Security in Cloud Computing for Third Party Auditor by Self-destruction Mechanism

Muzammil H. Mohammed
Department of Information Technology, College of Computers and Information Technology,
Taif University, Taif, Saudi Arabia

Abstract: The main aim study in cloud computing system, large amount of data can be maintained in the cloud storage system and it can be used for application based services for client. The bulk amount of data privacy will not be properly maintained by the cloud service provider. Without knowledge of authorized client, data can be viewed by another user with the permission of Cloud Service Provider (CSP). Many cryptography technique can be used for data privacy in the TPA (Third Party Auditor) which is the trusted authority to audit and verify the integrity in cloud. The cloud loaded data can be viewed by authorized user and copy of data can be in tag based data placed in TPA and data privacy can be affected in TPA system. In the proposed system, data privacy can be maintained in the TPA view by using self destruction mechanism to destroy the data after the view point of data for particular time and then the viewed data copy can be destruction in TPA. The cloud service provider can be securely loading the data in cloud via TPA Server. The main advantage of the self destruction mechanism security for the data in cloud via TPA server without the permission of the particular authenticated client other user cannot viewed the individual client data. Then data privacy can be perfectly maintained in the cloud service.

Keywords: Cloud service provider, self-destructing data, trusted third party auditor

INTRODUCTION

In the cloud computing, the application based service and the data storage service can be provided by the cloud service provider. In the application based service application can be viewed as per the user request (John *et al*., 2008). Then, particular worked data can be downloaded from the cloud server by the particular client. In cloud, data upload and download data speed will be decreased in the cloud service. Because, the copy of the data placed in the cloud server and the TPA server for the user point of view to view the placed data in TPA server. In the cloud, uploaded data can be categorized into public data and private data both the user individual data viewed can be viewed by the other user easily in the TPA server (Son *et al*., 2013). The policy can be maintained for each and every user aspect in the cloud provided policy.

The outsourced can be loaded from the cloud and the bulk amount of labeled data can be outsourced to the other user in cloud. The data transform from cloud to client and client to cloud. In this data copy can be produced in the networking cache memory. The user data leakages occur in cloud either by cloud service provider or the particular client loading time in the cloud (Devulapalli *et al*., 2009). However, data encryption and decryption can be used in the cloud for data privacy data can be leaked in the cloud system.

The data can be assured delete process can be performed. However the data can be deleting in the cloud. The backup copies in the server or the cloud data privacy can be leaked in intermediate server called trusted server third part auditor make the data copies in the particular sever. In this way particular data can be leaked in the cloud.

In recent years, FADE technique in the cloud for data assure deletion based on encryption and decryption of the key file management system in the intermediate server third party auditing service assure the data privacy, the data can be viewed by encrypt and decrypt based on the key file management system to manage the third party auditing service (Geambasu *et al*., 2009). In this system, policy based data deletion can be performed (Shamir, 1979). In this the user can be given the original key as input to view the particular data in the cloud. This is the biggest drawback in the cloud large data storage system. The client will know about the exact key to view the particular data in the TPA viewer otherwise the particular client cannot view the data. The client will having knowledge about the data key to view the data in the cloud (Zeng *et al*., 2010). This is the main drawback in the file assure deletion mechanism.

In this proposed system, data privacy can be maintained by the new technique called self destruction method. In this method data can be viewed using key management. In the key management, key can be

generated for the user data and the particular user views the data in cloud. For the loaded data in cloud having the particular information based on the data creation like data creation time and data creation date, data sending date and receiving date, sender name, receiver name. This kind of information can be used for fixing the data label name. In the data label name the particular data can be tagged in the TPA. In this way data can be securely shown to the particular user data only (Devulapalli *et al*., 2009). Once the particular data can be viewed by the particular user the data can be automatically destruction from the user point of view (Copy of the server data labeled in the TPA). The original data can be maintained in the main cloud server. In this way, the particular data privacy can be maintained securely (Wolchok *et al*., 2010). The client sending and receiving data in the cloud details can be maintained. Compared to the other method data leakage cannot be performed assuredly. In this system, data will be having security in the cloud.

In the SeDas prototype, the key distribution can be performed based on the following steps:

- In active storage framework SeDas is called the key storage server sedas. In this server key file can be chosen then only the particular user views the data in TPA server. In this server key can be created and divided to the entire client in the cloud to view her individual transformed data in the cloud.
- In this system, meets all data privacy and data processing can be performed with less time without any overhead in the user view the data in cloud server via the TPA.

METHODOLOGY

Basic data upload/download in cloud: In the cloud data upload or download in the based on data storage system in cloud based on some policies. Either the particular data can be associated with single policy or the multiple policies in the cloud then the particular user request the data from the cloud server and particular tag labeled data can be viewed in the TPA server based on key management. In the key file management data can be viewed in the TPA server.

Data upload: In the data upload the data can be uploaded in the name of file information like data creation, data sender, receiver, sending time and the data modified time all the information can be named as the user uploaded data in the cloud.

Data download: In the data download data can be downloaded based on the user chosen the key in the key storage system SeDas called active storage framework. In this key storage server key can be created for the particular user and then user select the key file then the data viewed file can be chosen the particular data can be automatically destructed in the TPA server.

Active storage framework-SeDas: In the SeDas system, the data can view by the key file and the data file in the TPA view can be destroyed based on the TTL (Time to Live) data can be viewed time can be calculated. When data view time can be finished in TPA server and labeled copy of data can be automatically destructed. The latency of the data increased by 60% upload and download speed and the acceptability of the data in the cloud taken by less than 72% without using SeDas prototype. In this system, object based interface can be used to store and manage the key in SEDAS sever. Object based interface can be found between application server and the SeDas key storage server.

Self data manipulation: In the self data manipulation, third party auditor storing the data. The temporary labeled data no need to modify the data in TPA. Copies of the data can be stored temporary in the TPA server. Self-destructing data cannot affect the normal storage data in the cloud.

Time interval for secret key data in TPA: Time interval for the availability of labeled data in the TPA can be viewed in particular amount of user access time in the cloud. Once the data can be viewed by the user at the particular view point of time the temporary storage data can be automatically in the cloud. After the period of time the particular data can be automatically destructed in the labeled data.

Key generation: The key distribution can be performed randomly and the key file can be created when the data can be uploaded to the cloud server via TPA server. Then particular user choose key file and it can be allocated for all the user loaded data in cloud server. Once the key file can be chosen in SeDas server and the user viewed data can be of data automatically destructed in the TPA server label data. The normal stored data in the cloud server cannot be modifying in the cloud. The privacy of the data can be perfectly maintained in the cloud.

Attack prevention: In the cloud data storage system, many attacks can be found during data transmission like sniffing attack, shoulder attack can be found, (Shamir, 1979) this type of non privacy can be completely preserved and provide the efficient service in the cloud (Fig. 1).

RESULTS AND DISCUSSION

In result Fig. 2 and 3 shows the throughput for upload. X axis represents the throughput Y axis

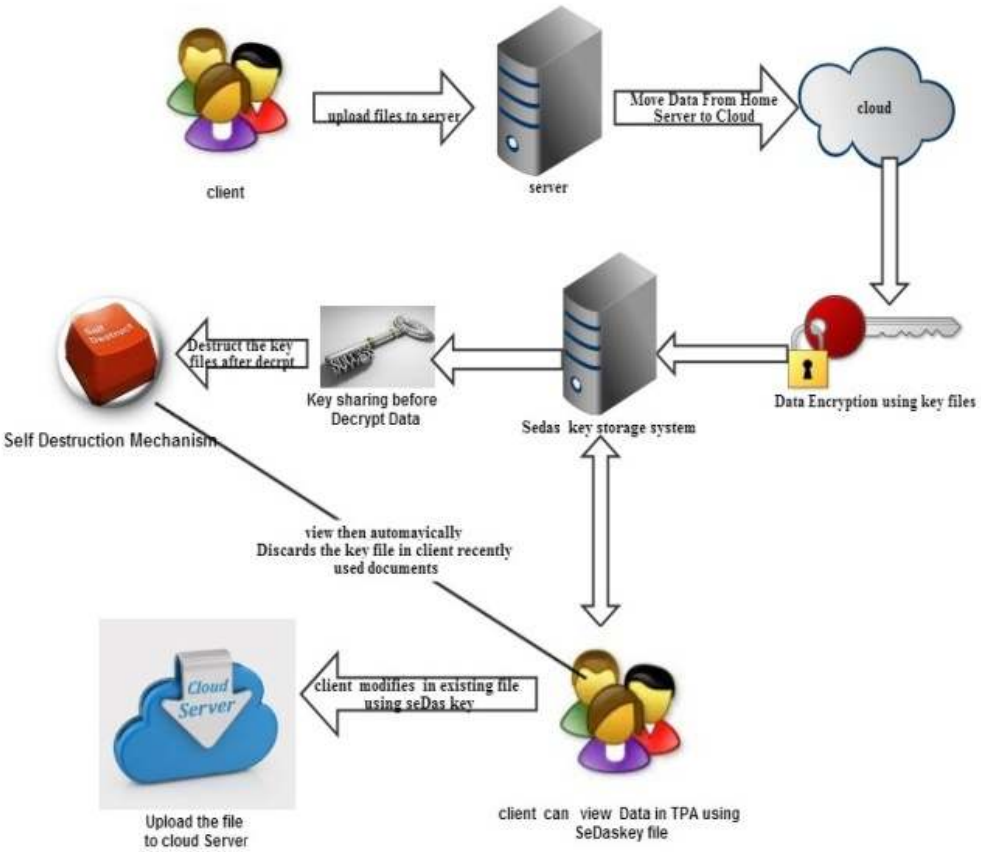

Fig. 1: System architecture

Fig. 2: Throughput for upload

Fig. 3: Throughput for download

represents the file size. Throughput is how much mb is calculated in 1 sec. In existing system, 16 mb was uploaded in 50 sec, where as in proposed system it takes 10 sec to upload a 16 mb file. Compare to the existing system the performance of proposed system is higher. This graph clearly shows the proposed system reduces the throughput over the existing system by an average of 15.5% and up to 55% for the uploading.

In Result Fig. 2 shows the throughput for download. X axis represents the throughput Y axis represents the file size. In existing system, 16 mb was downloaded in 50 sec, where as in proposed system it takes 18 sec to download a 16 mb file. Compare to the existing system the performance of proposed system is higher. Figure 4 shows that proposed system reduces the throughput over the existing system by an average of 18% and up to 50.75% for the downloading. Figure 2 and 3 shows the throughput results for the different schemes. The throughput decreases because upload/download processes require much more CPU computation and finishing encryption/decryption processes in the proposed system, compared with the existing system.

CONCLUSION

Data security is important in the cloud environment. This study introduced a new approach for defending data privacy in cloud computing. Self-destructing data mainly aims at protecting the user data's confidentiality. In this project SeDas concept is used for data privacy. The functionality and security is properly maintained by using SeDas prototype. SeDas uses object based storage technique. It will be used for object based storage design for cloud services. Here the key file is used for accessing the uploaded file on the cloud by the server. SeDas have self destruct method for deleting the important information such as password and account number. If the client once downloads the file from cloud the important information of the particular client will be deleted from the cache memory and the original memory. Using the Rijindael algorithm, the security and performance in this process is improved.

In the existing system time complexity arrived at file upload and download due to insufficiency of network. In future first the best network for file transmission is analyzed the time consumption is also avoided. It is used to reduce the computational cost (Zhang and Feng, 2008).

In the future work the client can download file using the SeDas concept and the dynamic data operation can be maintained by the auditing process in the cloud environment.

REFERENCES

Devulapalli, A., I.T. Murugandi, D. Xu and P. Wyckoff, 2009. Design of an Intelligent Object-Based Storage Device [Online]. Retrieved form: http://www.osc.edu/research/network_file/projects/object/ papers/istor-tr.pdf.

Geambasu, R., T. Kohno, A.A. Levy and H.M. Levy, 2009. Vanish: Increasing data privacy with self-destructing data. Proceeding of the 18th Conference on USENIX Security Symposium, pp: 299-316.

John, T.M., A.T. Ramani and J.A. Chandy, 2008. Active storage using object-based devices. Proceeding of IEEE International Conference on Cluster Computing, pp: 472-478.

Shamir, A., 1979. How to share a secret. Commun. ACM, 22(11): 612-613.

Son, S.W., S. Lang, P. Carns, R. Ross, R. Thakur, B. Ozisikyilmaz, W.K. Liao and A. Choudhary, 2013. Enabling active storage on parallel I/O software stacks. Proceeding of IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST'2010), pp: 1-12.

Wolchok, S., O.S. Hofmann, N. Heninger, E.W. Felten, J.A. Halderman, C.J. Rossbach, B. Waters and E. Witchel, 2010. Defeating Vanish with Low-Cost Sybil Attacks against Large DHEs. Retrieved form: http://z.cs.utexas.edu/users/osa/unvanish/.

Zeng, L., Z. Shi, S. Xu and D. Feng, 2010. Safe vanish: An improved data self-destruction for protecting data privacy. Proceeding of 2nd International Conference on Cloud Computing Technology and Science (CloudCom). Indianapolis, IN, USA, pp: 521-528.

Zhang, Y. and D. Feng, 2008. An active storage system for high performance computing. Proceeding of 22nd International Conference on Advanced Information Networking and Applications (AINA, 2008), pp: 644-651.