ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Protection Based Power Ability of User Information over Cloud

G.Kavi Nilavu[1.], S.Muthuraj, M.Tech[2]., Dr. R.Umamaheshwari, M.E.,Ph.D. [3]

Research Scholar, Dept. of Computer Science, Gnanamani College of Technology, Tamilnadu, India [1]

Assistant Professor, Dept. of Computer Science, Gnanamani College of Technology, Tamilnadu, India [2]

HOD (CS), Gnanamani College of Technology, Namakkal, Tamilnadu, India[3]

ABSTRACT: A cloud storage system, consisting of a set of storage servers, provides semi permanent storage services over the net. Storing knowledge during a third party's cloud system causes serious concern over knowledge confidentiality. General secret writing schemes shield knowledge confidentiality, however conjointly limit the practicality of the storage system as a result of a number of operations square measure supported over encrypted knowledge. Constructing a secure storage system that supports multiple functions is difficult once the storage system is distributed and has no central authority. We have a tendency to propose a threshold proxy re-encryption theme and integrate it with a suburbanized erasure code such a secure distributed storage system is developed. The distributed storage system not solely supports secure and study knowledge storage and retrieval, however conjointly lets a user forward his knowledge within the storage servers to a different user while not retrieving the information back. The most technical contribution is that the proxy re-encryption theme supports secret writing operations over encrypted messages yet as forwarding operations over encoded and encrypted messages. Our methodology absolutely integrates encrypting, encoding, and forwarding. We have a tendency to analyze and counsel appropriate parameters for variety of copies of a message sent to storage servers and also the number of storage servers queried by a key server. These parameters permit additional versatile adjustment between the amount of storage servers and hardiness.

KEYWORDS: Proxy re-encryption, Storage System, Erasure code

I. INTRODUCTION

Cloud computing is the use of computing resources that are delivered as a service over a network. For example, the email service is probably the most popular one. Cloud computing is a concept that treats the resources on the Internet as a unified entity, a cloud. Users just use services without being concerned about how computation is done and storage is managed. This paper focuses on designing a cloud storage system for robustness, confidentiality, and functionality. A cloud storage system is considered as a large scale distributed storage system that consists of many independent storage servers. Data robustness is a major requirement for storage systems. One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message. It is very robust because the message can be retrieved as long as one storage server survives. Another way is to encode a message of k symbols into a codeword of n symbols by erasure coding. To store a message, each of its codeword symbols is stored in a different storage server. A storage server failure corresponds to an erasure error of the codeword symbol. As long as the number of failure servers is under the tolerance threshold of the erasure code, the message can be recovered from the codeword symbols stored in the available storage servers by the decoding process. A decentralized erasure code is an erasure code that independently computes each codeword symbol for a message. A decentralized erasure code is suitable for use in a distributed storage system. After the message symbols are sent to storage servers, each storage server independently computes a codeword symbol for the received message symbols and stores it. This finishes the encoding and storing process.

Finally, besides data storing and retrieving, it is hard for storage servers to directly support other functions. This addresses the problem of forwarding data to another user by storage servers directly under the command of the

DOI: 10.15680/IJIRCCE.2018.0603063

data owner. We consider the system model that consists of distributed storage servers and key servers. Since storing cryptographic keys in a single device is risky, a user distributes his cryptographic key to key servers that shall perform cryptographic function on behalf of the user. These key servers are highly protected by security mechanisms. We use a new threshold proxy re-encryption scheme and integrate it with a secure decentralized code to form a secure distributed storage system. The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages. Our system meets the requirements that storage servers independently perform encoding and re-encryption.

II. RELATED WORK

Nowadays, the popularity of cloud storage has increased rapidly, and ordinary users as well as many large firms tend to outsource their data to CSP (Cloud Service Provider) . In cloud storage environment, the CSP should provide users with controllable, cross-domain and flexible data sharing service. Whereas, since CSP is widely considered a semi-trusted party, a user always tends to upload encrypted data (cipher texts) instead of original data (plaintexts) to cloud server for fear of data being disclosed. Thus, cloud data sharing means to share encrypted data stored in cloud servers, and it essentially involves a cryptographic access control problem. Nevertheless, traditional access control technologies which adopt access policies and privileges to control a group of users are plaintext oriented, and have weaknesses such as non-dead URL, unauthorized re-sharing, non-HTTPS shortened URL and sharing of trash files. These weaknesses widely exist in most popular cloud storage services like Dropbox, Google Drive and Microsoft SkyDrive . Obviously, such technologies are not suitable for cloud storage that aimed to share data with ungrouped individuals, because the CSP can easily get the plaintexts bypass the access policies and privileges limit. Therefore, researchers are seeking novel cryptographic access control technologies to support cloud data sharing to satisfy user’s requirements.

The first public key broadcast encryption scheme was proposed by Dodis and Fazio in 2002. However, Dodis and Fazio’s scheme has the weakness of too big size of encryption keys. In addition, from perspective of cloud storage users, in order to share data to unforeseeable individuals dispersing on the Internet, the broadcast encryption technology must support dynamically adding a user to the sharing group without changing the encryption public key. For this purpose, Delerablee et al. proposed the first dynamic broadcast encryption scheme that allows users join the broadcast system at any point. Thereafter, many broadcast schemes are proposed in succession. On the other hand, although broadcast encryption which naturally has the “broadcast distribution” feature can easily support broadcast sharing, it is inefficient when used in a secure cloud storage platform, because data are not stored in its owner’s devices but in the cloud devices held by semi-trusted CSP. If directly using broadcast encryption technology to share cloud data, the data owner must first download his encrypted data, then decrypt it, and then encrypt it with new key, and subsequently upload to cloud server for target users to download. These procedures inevitably increase the network load and lower the efficiency. For this, combining broadcast encryption and proxy re-encryption (PRE) becomes a good choice to realize broadcast sharing in secure cloud storage. Proxy re-encryption enables a semi-trusted proxy to transform a cipher text encrypted with A’s public key to a cipher text encrypted with B’s public key without disclosing plaintext to the proxy. Nowadays, with the popularity of cloud computing, conditional PRE that enables clients to limit the proxy by only diverting the cipher text meeting a specified condition is put forward to improve practicability. Based on the idea of broadcast encryption and conditional proxy re-encryption, Chu et al. first proposed the idea of CPBRE (Conditional Proxy Broadcast Re-Encryption), and put forward a CPBRE scheme. Recently, Sun et al. put forward a similar scheme which attempts to deal with cloud data sharing. In this paper, we have the following main contributions:

We propose an efficient encrypted data sharing scheme for secure cloud storage based on conditional proxy broadcast re-encryption. The proposed scheme (named as CPBRE-DS) not only inherits the support of user dynamics but also enables the proxy directly re-encrypts sharing data in the cloud without disclosing the data to any party including the proxy.

We give a security analysis of the proposed scheme, which shows that it is secure against the semi-trusted CSP.

We analyze theoretically and test experimentally the performance of the proposed scheme, and the results show that our scheme is efficient.

DOI: 10.15680/IJIRCCE.2018.0603063

III. EXISTING SYSTEM

Data access control has becoming a challenging issue in cloud storage systems. Some techniques have been proposed to achieve the secure data access control in a semi trusted cloud storage system. Recently, K. Yang et al. proposed a basic data access control scheme for multi authority cloud storage system (DAC-MACS) and an extensive data access control scheme (EDAC-MACS). They claimed that the DAC-MACS could achieve efficient decryption and immediate revocation and the EDAC-MACS could also achieve these goals even though non revoked users reveal their Key Update Keys to the revoked user. However, through our cryptanalysis, the revocation security of both schemes cannot be guaranteed. In this paper, we first give two attacks on the two schemes. By the first attack, the revoked user can eavesdrop to obtain other users' Key Update Keys to update its Secret Key, and then it can obtain proper Token to decrypt any secret information as a non revoked user. In addition, by the second attack, the revoked user can intercept Cipher text Update Key to retrieve its ability to decrypt any secret information as a non revoked user. Secondly, we propose a new extensive DAC-MACS scheme (NEDAC-MACS) to withstand the above two attacks so as to guarantee more secure attribute revocation. Then, formal cryptanalysis of NEDAC-MACS is presented to prove the security goals of the scheme. Finally, the performance comparison among NEDAC-MACS and related schemes is given to demonstrate that the performance of NEDAC-MACS is superior to that of DACC, and relatively same as that of DAC-MACS.

Disadvantages

- General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data.
- Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority.
- Data robustness is a major requirement for storage systems.

IV. PROPOSED SYSTEM

We have a tendency to propose a threshold proxy re-encryption theme and integrate it with a suburbanized erasure code such a secure distributed storage system is developed. The distributed storage system not solely supports secure and sturdy knowledge storage and retrieval, however conjointly lets a user forward his knowledge within the storage servers to a different user while not retrieving the information back. The most technical contribution is that the proxy re-encryption theme supports secret writing operations over encrypted messages yet as forwarding operations over encoded and encrypted messages. Our methodology absolutely integrates encrypting, encoding, and forwarding. We have a tendency to analyze and counsel appropriate parameters for variety of copies of a message sent to storage servers and also the number of storage servers queried by a key server. These parameters permit additional versatile adjustment between the amount of storage servers and hardiness.

Advantages

- The proposed method integrating the data encryption, encoding and data forwarding functions.
- The cloud storage system supports multi authority functions.
- Data centralized system has been utilized by this proposed method.
- In proposed method, user can easily maintains the data access control.

V. METHODOLOGIES

- Data Owner Module
- Construction of secure cloud storage Module
- Proxy re-encryption
- Secure Forwarding
- Data Retrieval Module

Data Owner Module:

Each cloud service provider as a owner. Data outsourcing to cloud storage servers is raising trend among many firms and users owing to its economic advantages. This essentially means that the owner (client) of the data moves its data to a third party cloud storage server which is supposed to presumably for a fee faithfully store the data with it and provide it back to the owner whenever required.

Construction of Cloud Data Storage Module

In Admin Module the admin can login to give his username and password. Then the server setup method can be opened. In server setup process the admin first set the remote servers Ip-address for send that Ip-address to the receiver. Then the server can skip the process to activate or Disactivate the process. For activating the process the storage server can display the Ip-address. For Disactivating the process the storage server cannot display the Ip-address. These details can be viewed by clicking the key server. The activated Ip-addresses are stored in available storage server. By clicking the available storage server button we can view the currently available Ip-addresses.

Data Encryption Module

In cloud login module the user can login his own details. If the user cannot have the account for that cloud system first the user can register his details for using and entering into the cloud system. The Registration process details are Username, E- mail, password, confirm password, date of birth, gender and also the location. After entering the registration process the details can be stored in database of the cloud system. Then the user has to login to give his corrected username and password the code has to be send his/her E-mail. Then the user will go to open his account and view the code that can be generated from the cloud system.

Data Forwarding Module

In forward module first we can see the storage details for the uploaded files. When click the storage details option we can see the file name, question, answer, folder name, forward value (true or false), forward E-mail. If the forward column display the forwarded value is true the user cannot forward to another person. If the forward column display the forwarded value is false the user can forward the file into another person. In file forward processes contains the selected file name, E- mail address of the forwarder and enter the code to the forwarder. Now, another user can check his account properly and view the code forwarded from the previous user. Then the current user has login to the cloud system and to check the receive details. In receive details the forwarded file is present then the user will go to the download process.

Data Retrieval Module

In Download module contains the following details. There are username and file name. First, the server process can be run which means the server can be connected with its particular client. Now, the client has to download the file to download the file key. In file key downloading process the fields are username, filename, question, answer and the code. Now clicking the download option the client can view the encrypted key. Then using that key the client can view the file and use that file appropriately.

VI. CONCLUSION AND FUTURE WORK

We consider a cloud storage system that consists of storage servers and key servers. Our system provides both the storage service and key management service. A secure cloud storage system is constructed using the threshold proxy re-encryption scheme that provides secure data storage and secure data forwarding functionality in a decentralized structure. The threshold proxy re-encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way. Our construction is fully decentralized with storage server performing encoding and re-encryption process and each key server perform partial decryption. Our storage servers act as storage nodes in a content addressable storage system for storing content addressable blocks. Our key servers act as access nodes for providing a front-end layer such as a traditional file system interface.

REFERENCES

[1] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,”*J. Network and Computer Applications*,vol. 34, no. 1, pp. 1-11, Jul. 2010
[2] K. Yang, X. Jia, and K. Ren, “DAC-MACS: Effective data access control for multiauthority cloud storage systems,” *IEEE Trans. Information Forensics and Security*,vol. 8, no. 11, pp. 1790-1801, Nov. 2013
[3] Kan Yang and Xiaohua Jia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage," *IEEE Trans.Parallel and Distributed Systems*,vol.25, no.7, pp.1735-1744, July 2014
[4] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” *Proc. EU-ROCRYPT’ 05*, pp. 457-473, 2005
[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryp-tion for Fine-Grained Access Control of Encrypted Data,” *Proc. ACM Conf. Computer and Comm.*Security, pp. 89-98, 2006
[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” *Proc.IEEE Symp.Security &Privacy*, pp. 321-334, 2007
[7] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-Based Encryption with Non-Monotonic Access Structures,” *Proc. ACM Conf. Computer and Comm.*Security, pp. 195-203, 2007
[8] L. Cheung and C. C. Newport, “Provably secure ciphertext policy ABE,”*Proc. ACM Conf. Computer &Communications Security*, pp. 456-465, 2007
[9] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: distributed access control in clouds,” *Proc. TrustCom’11*, pp. 91-98, IEEE, 2011
[10] Zhiguo Wan, Jun'eLiu, and Deng, R.H., "HASBE: A Hierarchical At-tribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing," *IEEE Trans.Information Forensics and Security*, vol.7, no.2, pp. 743-754, April 2012
[11] Junzuo Lai,Deng, R.H.,Chaowen Guan, andJian Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption," *IEEE Trans.Information Forensics and Security*, vol.8, no.8, pp. 1343-1354, Aug. 2013
[12] J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 7, pp.1214-1221, Jul.2011
[13] J. Hur, “Improving security and efficiency in attribute-based data shar-ing,” *IEEE Trans.Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2271-2282, Oct. 2013
[14] M. Chase and S. S. M. Chow, “Improving privacy and security in mul-tiauthority attribute-based encryption,” *Proc. CCS’09*, pp.121-130, 2009
[15] M. Chase, “Multiauthority attribute-based encryption,” *Proc.TCC’07*, pp. 515-534, Springer, 2007

DOI: 10.15680/IJIRCCE.2018.0603063