Dr. K. Sunil Manohar Reddy, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 8, August- 2017, pg. 20-23 ISSN: 2321-8363
Impact Factor: 4.123

Eliminate Residue in Cloud System

Dr. K. Sunil Manohar Reddy
Assistant Professor, Department of CSE, Matrusri Engineering College, Hyderabad, sunil186@gmail.com

Abstract

Usually the client information's deduplication brings various problems of security, due to certain limitations of data possession. In this paper a novel client-side deduplication approach is introduced for sharing of outsourced information by using public cloud. The proposal ensures improved privacy towards unofficial users and secondly, by using integration of access rights within metadata file, an official user will decipher an encrypted file by means of his private key. This system of client-side data deduplication is on the basis of original usage of convergent encryption. The proposed solution is on the basis of cryptographic use of symmetric encryption utilized for enciphering data file as well as asymmetric encryption for Meta data files, because of maximum sensibility of the data towards various intrusions. It is moreover shown to be tough towards unofficial access towards data and for any data disclosure throughout sharing process, offering two levels of access control confirmation.

Keywords: Public cloud, Deduplication, Metadata, Access control, Convergent encryption, Intrusions.

1. Introduction

The usage of remote systems of storage is gaining attention, specifically services based on cloud storage, as it offers cost-reasonable models. These models manage transmission, storage in multi-tenant setting, and thorough computation of outsourced information in pay per usage model. In the recent times, several efforts were proposed in several representations of security known as proof of ownership systems [1]. These will permit storage server to confirm ownership of user data which is on basis of static in addition to short value. These protocols are considered to assurance various needs such as lightweight of verification and computation effectiveness. While existing proof of ownership systems have addressed several properties of security, we however need an important consideration of data leakage as well as poison attacks that target preservation of privacy plus revelation of data privacy. We introduce a novel client-side deduplication approach for sharing of outsourced information by means of public cloud [2][3]. A recognized secure channel was assumed among client and the cloud service provider which is secure channel supporting mutual authentication as well as data privacy besides integrity. Hence, after authentication by the provider of cloud service, cloud users will share the similar resources in multi-tenant setting. Hash functions are used in generation of enciphering data key thus we assume that cryptographic functions are collision resistant, since it is an inflexible problem to discover similar output for various data files. Our solution is moreover shown to be tough towards unofficial access towards data and for any data disclosure throughout sharing process, offering two levels of access control confirmation.

2. Existing System

Client side deduplication is used to remove the duplicate copies of data in the cloud storage system. This brings many security issues considerably due to the multi owner data possession challenges. For instance several attacks like bandwidth consumption or data confidentiality and privacy.
To solve these issues many efforts were proposed like proof of ownership, they allow the storage server storage check a user data ownership. And also they have used AES-256 CBC for data encryption and decryption.

©2017, IJCSMA All Rights Reserved, www.ijcsma.com

3. Proposed System

We are utilizing the previous technique POW (proof of ownership) and apply the Cryptographic techniques to that system and as well as Merkle based tree.

Merkle based tree is improving the data security in cloud storage systems and providing dynamic sharing between the users and ensuring efficiency data deduplication.

Apart from this in this proposed system we are also using Blowfish algorithm. So, that the encryption and decryption process can be done faster when compared with the existing one [4].

4. Methodology

The trend of leveraging cloud services in recent times for important content storage, processing and distribution are the important issues for public cloud. For consumption of saving resources in network bandwidth besides storage capacities, several cloud services will implement the method of client side-deduplication. This will remove storage of redundant data within cloud servers and decrease the usage of network bandwidth related to transmission of similar contents. Our work introduces a novel cryptographic technique for secured Proof of ownership that is on the basis of convergent encryption as well as Merkle-based Tree for improvisation of data security within cloud systems and offer active sharing among users and make sure of effective data deduplication. Proof of ownership is introduced by Halevi which is a protocol of challenge-response that permits a storage server to make sure of whether a requesting entity is the owner of data, on the basis of short value. While existing proof of ownership systems have addressed several properties of security, we however need an important consideration of data leakage as well as poison attacks that target preservation of privacy plus revelation of data privacy.

We introduce a novel client-side deduplication approach for sharing of outsourced information by means of public cloud. Our system of client-side data deduplication is on the basis of original usage of convergent encryption. Our proposal is on the basis of cryptographic use of symmetric encryption utilized for enciphering data file as well as asymmetric encryption for meta data files, because of maximum sensibility of the data towards various intrusions. Our introduced proposal is of twofold that is, it ensures improved privacy towards unofficial users and secondly, by means of integration of access rights within metadata file, an official user will decipher an encrypted file simply by means of his private key [5]. Our solution is tough towards unofficial access towards data and for any data disclosure throughout sharing process, offering two levels of access control confirmation. Our notion includes usage of Merkle-based Tree on encrypted information, to obtain an exceptional identifier regarding the outsourced information. This identifier will make sure of the availability of same data in secluded cloud servers and moreover it is used to make sure of effective access control in active sharing situations. To prevent data leak, Halevi etal have introduced proof of ownership concept while introducing three various constructions regarding security as well as performances. These schemes will consider the server challenging client to provide accurate sibling paths for the subset of Merkle tree leave.

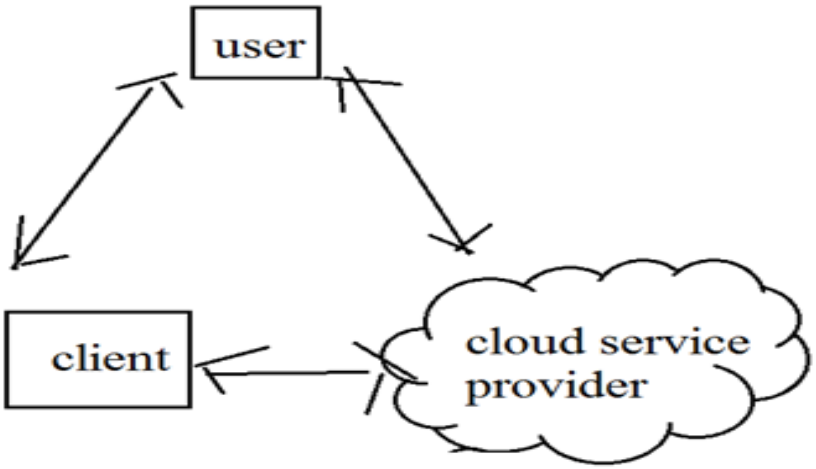

Figure 1: An overview of cloud data storage

©2017, IJCSMA All Rights Reserved, www.ijcsma.com

5. An Overview of Proposed System

Requirement for secured services of cloud storage and the properties of convergent cryptography will lead us to group them, hence, describing a pioneering solution towards the security issues of data outsourcing. Several efforts were proposed in several representations of security known as proof of ownership systems which permit storage server to confirm ownership of user data which is on basis of static in addition to short value. These are considered to assurance various needs such as lightweight of verification and computation effectiveness. We introduce a novel client-side deduplication approach for sharing of outsourced information by means of public cloud. Our solution makes several considerations [6]. We assume a recognized secure channel among client and the cloud service provider which is secure channel supporting mutual authentication as well as data privacy besides integrity. Hence, after authentication by the provider of cloud service, cloud users will share the similar resources in multi-tenant setting. Our solution will make use of hash functions in generating enciphering data key thus we assume that cryptographic functions are collision resistant, since it is an inflexible problem to discover similar output for various data files. Our solution is on the basis of cryptographic use of symmetric encryption utilized for enciphering data file as well as asymmetric encryption for meta data files, because of maximum sensibility of the data towards various intrusions. Our solution is moreover shown to be tough towards unofficial access towards data and for any data disclosure throughout sharing process, offering two levels of access control confirmation. Our introduced proposal is of twofold that is, it ensures improved privacy towards unofficial users and secondly, by means of integration of access rights within metadata file, an official user will decipher an encrypted file simply by means of his private key. Our secured system of client-side data deduplication is on the basis of original usage of convergent encryption. When the data owner desires to store up a novel enciphered data file in distant storage servers, initially generation of enciphering key is required. This data encryption key is derived by means of application of one-way hash function on the content of data and after encryption of file data, client has to create data identifier of enciphered information, to make sure of its distinctiveness within cloud database, prior to uploading of claimed file. This data identifier is estimated by means of Merkle hash tree, above encrypted contents. For the later data outsourcing, client is not mandatory to show similar encrypted data. But, he has to substitute client- server interactive proof system to verify his ownership. To defend data within public cloud servers from unofficial entities, client has to confirm that simply approved users are capable to attain decrypting keys. The data owner needs to encrypt data deciphering key, by means of public key of recipient user. This key is integrated by data owner in user metadata to make sure of data privacy against malicious users, in addition to flexible policies of access control [7].

6. Results

In order to evaluate the time consumption at client side, we have conducted data encryption and decryption of data.

Table 1: Average time to upload and download file of size from 10 to 104 bytes, encrypted by AES-256-CBC

Average time in seconds		
Size in bytes	*Upload*	*Download*
10	5.48	4.32
10^2	5.68	4.52
10^3	6.02	4.58
10^4	6.45	5.02

7. Conclusion

In the recent times, the increase of digital contents will continue to increase the demand for network capacities, along by an increasing necessity for commercial usage of storage besides network bandwidth for transferring of data. We introduce a client-side deduplication approach for sharing of outsourced information by means of public cloud which is of twofold that is, it ensures improved privacy towards unofficial users and secondly, by

©2017, IJCSMA All Rights Reserved, www.ijcsma.com

means of integration of access rights within metadata file, an official user will decipher an encrypted file simply by means of his private key.

A novel cryptographic technique for secured Proof of ownership was introduced which is on the basis of convergent encryption as well as Merkle-based Tree for improvisation of data security within cloud systems, and offer active sharing among users and make sure of effective data deduplication. It is moreover shown to be tough towards unofficial access towards data and for any data disclosure throughout sharing process, offering two levels of access control confirmation. The proposed approach is on the basis of cryptographic use of symmetric encryption utilized for enciphering data file as well as asymmetric encryption for meta data files, because of maximum sensibility of the data towards various intrusions. Our proposed system of client-side data deduplication is on the basis of original usage of convergent encryption.

References

[1] O. Goldreich. Foundations of Cryptography: Basic Tools. Cambridge University Press, New York, NY, USA, 2000.
[2] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman- Peleg. Proofs of ownership in remote storage systems. In Proceedings of the 18th ACM conference on Computer and communications security, CCS '11, pages 491–500, New York, NY, USA, 2011. ACM.
[3] D. Hankerson, A. J. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer- Verlag New York, Inc., Secaucus, NJ, USA, 2003.
[4] Performance Analysis of Data Encryption Algorithms. Abdel-karim AI Tamimi, aa7@wustl.edu.
[5] W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols in cloud storage. In Proceedings of the 27th Annual ACM Symposium on Applied Computing, SAC '12, pages 441–446, New York, NY, USA, 2012. ACM.
[6] M. W. Storer, K. Greenan, D. D. Long, and E. L. Miller. Secure data deduplication. In Proceedings of the 4th ACM International Workshop on Storage Security and Survivability, StorageSS '08, pages 1– 10, New York, NY, USA, 2008. ACM.
[7] C. Wang, Z. guang Qin, J. Peng, and J. Wang. A novel encryption scheme for data deduplication system. In Communications, Circuits and Systems (ICCCAS), 2010 International Conference on, pages 265–269, 2010.

A Brief Author Biography

Dr. K. Sunil Manohar Reddy – Dr. K. Sunil Manohar Reddy is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Matrusri Engineering College, Hyderabad, India. His areas of interest are Neural Networks, Artificial Intelligence, Software Engineering, Cloud Computing, Computer Graphics and Data Warehousing and Data Mining. He has published and presented about 30 papers in National and International Conferences and Journals.

©2017, IJCSMA All Rights Reserved, www.ijcsma.com