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 2, February 2018

Attribute Based Intelligent Data Management Scheme over Cloud with Duplication-Free Data Logic

K.Priya[1], P.Ponvasan[2]

M.E. Computer Science and Engineering, Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Amaravathipudur, Karaikudi, TamilNadu, India.

Assistant Professor, Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Amaravathipudur, Karaikudi, TamilNadu, India.

ABSTRACT: The main objective of this system is to introduce duplication free cloud server with powerful encryption and decryption data logics such as Attribute Based Encryption (ABE). More and more clients would like to store their data into cloud servers along with the rapid development of cloud computing. New security problems have to be solved in order to help more clients process their data in public cloud. All the cloud having certain space maintenance problems, so that a new mechanism is required in proposed system, which provides duplication free data services over cloud environment. Security is the main constraint in cloud computing environment, which depicts the nature of the surveillance mechanisms in remote server based data maintenance scheme. In this system we follow the maximum security utility maximization with powerful Attribute Based Encryption (ABE), which process the data with 256-bit unbreakable encryption mechanism.

KEYWORDS: Data Deduplication, Cloud Computing, Access Control, Storage Management

I. INTRODUCTION

Cloud computing allows centralized data storage and online access to computer services or resources. It offers a new way of Information Technology (IT) services by re-arranging various resources and providing them to users based on their demands. Cloud computing has greatly enriched pervasive services and become a promising service platform due to a number of desirable properties, such as scalability, elasticity, fault-tolerance, and pay-per-use. Data storage service is one of the most widely consumed cloud services.

Cloud users have greatly benefited from cloud storage since they can store huge volume of data without upgrading their devices and access them at any time and in any place. However, cloud data storage offered by Cloud Service Providers (CSPs) still incurs some problems. First of all, various data stored at the cloud may request different ways of protection due to different data sensitivity. The data stored at the cloud include sensitive personal information, publicly shared data, data shared within a group, and so on.

Obviously, crucial data should be protected at the cloud to prevent from any access of unauthorized parties. Some unimportant data, however, have no such a requirement. As outsourced data could disclose personal or even sensitive information, data owners sometimes would like to control their data by themselves, while on some occasion, they prefer to delegate their control to a third party since they cannot be always online or have no idea how to perform such a control. How to make cloud data access control adapt to various scenarios and satisfy different user demands becomes a practically important issue. Access control on encrypted data has been widely studied in the literature.

However, few of them can flexibly support various requirements on cloud data protection in a uniform way, especially with economic deduplication management. Second, flexible cloud data deduplication with data access control is still an open issue. Duplicated data could be stored at the cloud in an encrypted form by the same or different

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 2, February 2018

users, in the same or different CSPs. From the standpoint of compatibility, it is highly expected that data deduplication can cooperate well with data access control. That is the same data (either encrypted or not) are only stored once at the cloud, but can be accessed by different users based on the policies of data owners or data holders (i.e., the eligible data users who hold original data).

Although cloud storage space is huge, duplicated data storage could greatly waste networking resources, consume plenty of power energy, increase operation costs, and make data management complicated. Economic storage will greatly benefit CSPs by decreasing their operation costs and reversely benefit cloud users with reduced service fees. Obviously, cloud data deduplication is particularly significant for big data storage and management. However, the literature still lacks studies on flexible cloud data deduplication across multiple CSPs. Existing work cannot offer a generic solution to support both deduplication and access control in a flexible and uniform way over the cloud.

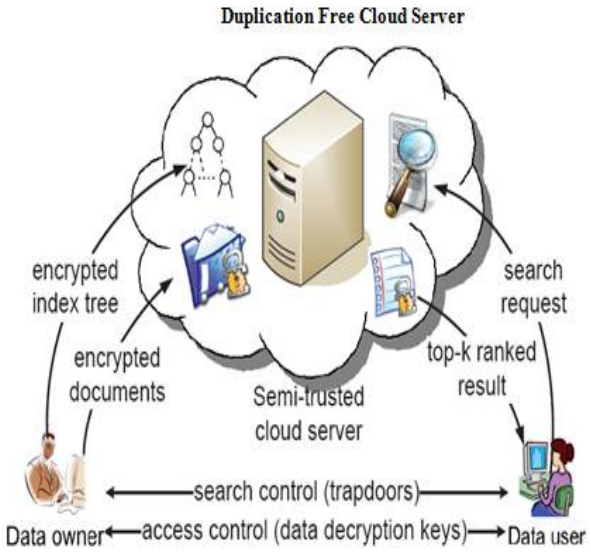

Fig.1 Proposed System Archietctural Design

In this system, we propose a holistic and heterogeneous data storage management scheme in order to solve the above problems. The proposed scheme is compatible with the access control scheme proposed earlier. It further realizes flexible cloud storage management with both data deduplication and access control that can be operated by either the data owner or a trusted third party or both or none of them. Moreover, the proposed scheme can satisfy miscellaneous data security demands and at the same time save storage spaces with deduplication across multiple CSPs. Thus it can fit into various data storage scenarios. Our scheme is original and different from the existing work. It is a generic scheme to realize encrypted cloud data deduplication with access control, which supports the cooperation between multiple CSPs. Specifically, the contributions of this paper are: We motivate to save cloud storage across multiple CSPs and preserve data security and privacy by managing encrypted data storage with deduplication in various situations. We propose a heterogeneous data management scheme to support both deduplication and access control according to the demands of data owners, which can adapt to different application scenarios. Our scheme can support data sharing among eligible users in a flexible way, which can be controlled by either the data owners or other trusted parties or both of them. We justify the performance of the proposed scheme through security analysis, comparison with existing work and implementation based performance evaluation. The results show its security, advantages, efficiency and potential applicability.

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 2, February 2018

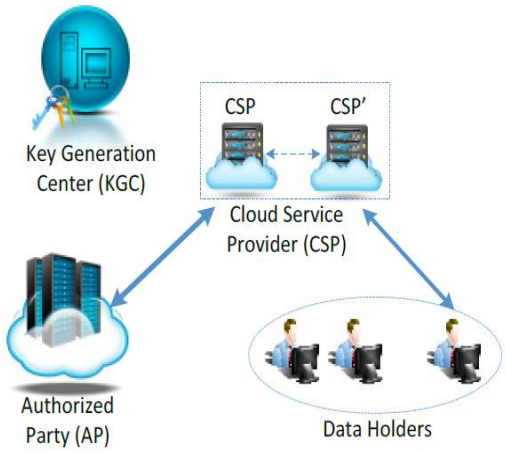

Fig.2 Proposed System Replication

II. EXISTING APPROACHES – A SUMMARY

Data Storage service is one of the most widely consumed cloud services. Cloud users have greatly benefited from cloud storage since they can store huge volume of data without upgrading their devices and access them at any time and in any place. However, cloud data storage offered by Cloud Service Providers [CSPs] still incurs some problems. First of all, various data stored at the cloud may request different ways of protection due to different data sensitivity. The data stored at the cloud include sensitive personal information, publicly shared data, data shared within a group, and so on. As outsourced data could disclose personal or even sensitive information of users, so, they have no idea to provide sensitive information over cloud environment. The existing system has several disadvantages, some of them are listed below: (a) Encrypted Data could incur much waste of cloud storage and complicate data sharing among authorized users and (b) We are still facing challenges on encrypted data storage and management with deduplication.

III. PROPOSED SYSTEM

In the proposed system of development the following things are concentrated more and they are describes as below: We motivate to save cloud storage across multiple CSPs and privacy by managing and preserve data security and privacy by managing encrypted data storage with deduplication in various situations. We propose a heterogeneous data management scheme to support both deduplication and access control according to the demands of data owners, which can adapt to different application scenarios. Our scheme can support data sharing among eligible users in a flexible way, which can be controlled by either the data owners or other trusted parties or both of them. We justify the performance of the proposed scheme through security analysis, comparison with existing work and implementation based performance evaluation.

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 2, February 2018

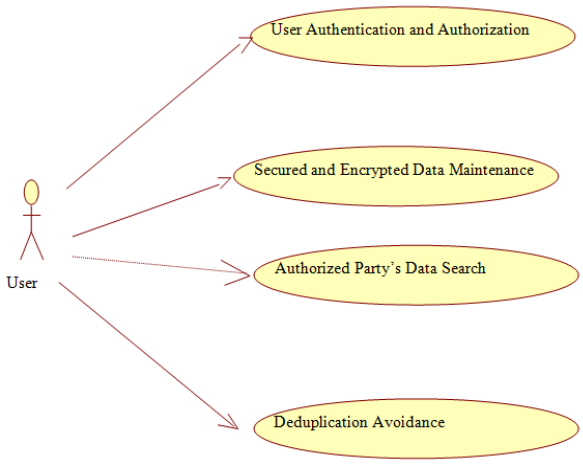

Fig.3 System Usecase Diagram

The proposed system has several advantages; some of them are listed below: (a) Flexible Cloud Data Deduplication with proper Access Control facilities and (b) The proposed scheme is more secured, advanced and efficient.

IV. SYSTEM IMPLEMENTATION

The proposed system is implemented with the help of following modules; all of them are described in detail below:

A. User Authorization and Authentication

Proxy defines the security by means of user authorization and authentication. Proxy signature is a signature scheme, in which an original signer can delegate his/her signing capability to a proxy signer, and then the proxy signer generates a signature on behalf of the original signer. From a proxy signature, a verifier can be convinced of the original signer's agreement on the signed message. Researchers have proposed 3 kinds of proxy signature algorithms: full delegation, partial delegation and partial delegation by warrant. The former two are eliminated by partial delegation with warrant which is proved to be more secure and practical, so we also use partial delegation with warrant in our protocol design. Let A be an original signer who has an authentic key pair (PrKA and PuKA), and B be a proxy signer who has an authentic key pair (PrKB and PuKB). Let mw be A's warrant information for the delegation, which has semantic means including the original signer's identity, some information about the proxy signer (for example the identity), period of delegation validity, the qualification of messages on which the proxy signer can sign, etc.

B. Secured and Encrypted Data Maintenance

This Secured and Encrypted Data Maintenance module describes the unencrypted dynamic and ranked search scheme which is constructed on the basis of vector space model and KBB tree. Based on the above mentioned scheme, two secure search schemes are constructed such as Keyword based search and content based search against two threat models, respectively. This system fully involves in the context of generating efficient hint texts against the given data.

In this module, we just consider the cloud provider is semi-trusted: honest but curious, which means that cloud servers would follow our proposed protocol in general, but would try to find out as much secret information as possible based on each group member's inputs. In general, we assume cloud servers are interested in data contents and group member's security information rather than other secret information. Cloud servers might collude with some malicious members for the purpose of getting data contents and group members' private information. Our scheme should satisfy

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 2, February 2018

the security requirements of backward secrecy and forward secrecy. The former one ensures that the revoked user cannot decrypt new cipher texts. The later one ensures that the newly joined user can also access and decrypt the previously published data. This two security requirements are usually used in some cloud based data sharing scenarios.

A potential adversary may be a former group member or any one out of the group. We assume that an adversary can be a passive attacker who could be a man-in-the-middle to monitor the communications among the group members and cloud servers. A former group member can collude with cloud servers and try to access data contents shared in his/her former group.

An active adversary is able to impersonate an legitimate group member to gain some right. In general, we say that our scheme is secure if no adversary can succeed with any possible attacks mentioned above.

C. Authorized Party Data Search

The Authorized Party Data Search module alloes the Authorized Party to search for the data based on the content presented into it, which eliminates the problem of unwanted confusions and problems over data mining scenario, which is achieved by means of structured data maintenance module. The structured data storage scheme fully describes about the flow of data structure maintenance and the concept of implicit data mining and document maintenance schema. Once the Data Holder uploads the respective document it checks for the reference schema of the existing document for reference, if the document is presented in the database server then the following document is sequenced under the existing document otherwise it creates a new schema for the following document, so that the data into the database server is maintained in the structured manner. All the data into the server is based on the cluster format and provides the frequent access for the AP search between the server and the client.

D. Page Ranking Scenario

The PageRank model is a ranking methodology used by Search engines to rank the resulting in their search results. PageRank is a way of measuring the importance of website pages. According to Google: PageRank works by counting the number and quality of links to a page to determine a rough estimate of how important the website is. The underlying assumption is that more important websites are likely to receive more links from other websites. It is not the only algorithm used by Google to order search engine results, but it is the first algorithm that was used by the company, and it is the best-known.

V. LITERATURE SURVEY

In the year of 2004, the authors "D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano" proposed a paper titled "Public key encryption with keyword search", in that they described such as: the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

In the year of 2005, the authors "L. Ballard, S. Kamara, and F. Monrose" proposed a paper titled "Achieving efficient conjunctive keyword searches over encrypted data", in that they described such as: two provably secure and efficient schemes are proposed for performing conjunctive keyword searches over symmetrically encrypted data. Our first scheme is based on Shamir Secret Sharing and provides the most efficient search technique in this context to date. Although the size of its trapdoors is linear in the number of documents being searched, we empirically show that this overhead remains reasonable in practice. Nonetheless, to address this limitation we provide an alternative based on bilinear pairings that yields constant size trapdoors. This latter construction is not only asymptotically more efficient than previous secure conjunctive keyword search schemes in the symmetric setting, but incurs significantly less storage overhead. Additionally, unlike most previous work, our constructions are proven secure in the standard model.

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 2, February 2018

In the year of 2007, the authors "D. Boneh and B. Waters" proposed a paper titled "Conjunctive, Subset, and Range Queries on Encrypted Data", in that they described such as: we construct public-key systems that support comparison queries ($x \geq a$) on encrypted data as well as more general queries such as subset queries ($x \in S$). Furthermore, these systems support arbitrary conjunctive queries ($P\ 1 \wedge \cdots \wedge P\ \ell$) without leaking information on individual conjuncts. We present a general framework for constructing and analyzing public-key systems supporting queries on encrypted data.

VI. CONCLUSION

Data deduplication is important and significant in the practice of cloud data storage, especially for big data storage management. In this system, we proposed a heterogeneous data storage management scheme, which offers flexible cloud data deduplication and access control. Our scheme can adapt to various application scenarios and demands and offer economic big data storage management across multiple CSPs. It can achieve data deduplication and access control with different security requirements. Security analysis, comparison with existing work and implementation based performance evaluation showed that our scheme is secure, advanced and efficient.

REFERENCES

[1]R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in Proc. 2009 ACM Workshop Cloud Comput. Secur., pp. 85-90, 2009.
[2]S. Kamara, and K. Lauter, "Cryptographic cloud storage," Financ. Crypto. Data Secur., pp. 136-149, Springer, 2010.
[3]Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Efficient information retrieval for ranked queries in cost-effective cloud environments," in Proc. 2012 IEEE INFOCOM, pp. 2581-2585, 2012.
[4]M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., pp. 29–42, 2003.
[5]E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "SiRiUS: securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Secur. Symp., pp. 131-145, 2003.
[6]J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. of IEEE Symp. Secur. Privacy (SP'07), pp. 321-334, 2007.
[7]V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", in Proc. of 13th ACM Comput. Commun. Secur., pp. 89–98, 2006.
[8]S. Muller, S. Katzenbeisser, and C. Eckert, "Distributed attribute-based encryption," in Proc. of 11th Annual Int. Conf. Inf. Secur. Crypto., pp. 20–36, 2008.
[9]A. Sahai, and B. Waters, "Fuzzy identity-based encryption," in Proc. of 24th Int. Conf. Theory App. Cryptographic Tech., pp. 457– 473, 2005.
[10]S. C. Yu, C. Wang, K. Ren, and W. J. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. of IEEE INFOCOM, pp. 534–542, 2010.
[11]G. J. Wang, Q. Liu, J. Wu, and M. Y. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Comput. Secur., vol. 30, no. 5, pp. 320–331, 2011.
[12]S. C. Yu, C. Wang, K. Ren, and W. J. Lou, "Attribute based data sharing with attribute revocation," in Proc. ACM Asia Conf. Comput. Commun. Secur., pp. 261–270, 2010.
[13]G. J. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. of 17th ACM Comput. Commun. Secur., pp. 735-737, 2010.
[14]M. Zhou, Y. Mu, W. Susilo, M. H. Au, and J. Yan, "Privacy-preserved access control for cloud computing," in Proc. of IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun., pp. 83-90, 2011.
[15]Z. G. Wan, J. E. Liu, and R. H. Deng, "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 2, pp. 743-754, 2012.
[16]Z. Yan, Trust Management in Mobile Environments – Usable and Autonomic Models, IGI Global, Hershey, Pennsylvania, 2013.
[17]Y. Tang, P. P. Lee, J. C. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 903-916, 2012.
[18]M. Bellare, S. Keelveedhi, and T. Ristenpart, "DupLESS: server aided encryption for deduplicated storage," in Proc. of 22nd USENIX Conf. Secur., pp. 179-194, 2013.
[19]Dropbox, "A file-storage and sharing service," http://www.dropbox.com/.
[20]Google Drive. http://drive.google.com.