International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 26th Jul 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-07

Title **STORAGE SUPPORTING SECURE DEDUPLICATION OF ENCRYPTED DATA BASED ON ATTRIBUTE-BASED STORAGE**

Volume 08, Issue 07, Pages: 336–342.

Paper Authors

SK. AAKHILA BEGUM, MD.JOHN SAIDA

Eswar College of Engineering, Narasaraopet

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

STORAGE SUPPORTING SECURE DEDUPLICATION OF ENCRYPTED DATA BASED ON ATTRIBUTE-BASED STORAGE

SK. AAKHILA BEGUM[1], MD.JOHN SAIDA[2]

[1] PG Student, Eswar College of Engineering, Narasaraopet
[2] Asst.Professor, Eswar College of Engineering, Narasaraopet

ABSTRACT: Attribute-based encryption (ABE) has been widely used in cloud computing where a data provider outsources his/her encrypted data to a cloud service provider, and can share the data with users possessing specific credentials (or attributes). However, the standard ABE system does not support secure deduplication, which is crucial for eliminating duplicate copies of identical data in order to save storage space and network bandwidth. In this paper, we present an attribute-based storage system with secure deduplication in a hybrid cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage. Compared with the prior data deduplication systems, our system has two advantages. Firstly, it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. Secondly, it achieves the standard notion of semantic security for data confidentiality while existing systems only achieve it by defining a weaker security notion. In addition, we put forth a methodology to modify a cipher text over one access policy into cipher texts of the same plaintext but under other access policies without revealing the underlying plaintext.

1. INTRODUCTION

Cloud computing greatly facilitates data providers who want to outsource their data to the cloud without disclosing their sensitive data to external parties and would like users with certain credentials to be able to access the data. This requires data to be stored in encrypted forms with access control policies such that no one except users with attributes (or credentials) of specific forms can decrypt the encrypted data. An encryption technique that meets this requirement is called attribute-based encryption(ABE), where a user's private key is associated with an attribute set, a message is encrypted under an access policy (or access structure) over a set of attributes, and a user can decrypt a cipher text with his/her private key if his/her set of attributes satisfies the access policy associated with this cipher text. However, the standard ABE system fails to achieve secure deduplication, which is a technique to save storage space and network bandwidth by eliminating redundant copies of the encrypted data stored in the cloud. On the other hand, to the best of our knowledge, existing constructions for secure deduplication are not built on attribute-based encryption. Nevertheless, since ABE and secure deduplication have been widely applied in

cloud computing, it would be desirable to design a cloud storage system possessing both properties. We consider the following scenario in the design of an attribute-based storage system supporting secure deduplication of encrypted data in the cloud, in which the cloud will not store a file more than once even though it may receive multiple copies of the same file encrypted under different access policies. A data provider, Bob, intends to upload a file M to the cloud, and share M with users having certain credentials. In order to do so, Bob encrypts M under an access policy over a set of attributes, and uploads the corresponding cipher text to the cloud, such that only users whose sets of attributes satisfying the access policy can decrypt the cipher text. Later, another data provider, Alice, uploads a cipher text for the same underlying file M but ascribed to a different access policy `. Since the file is uploaded in an encrypted form, the cloud is not able to discern that the plaintext corresponding to Alice's cipher text is the same as that corresponding to Bob's, and will store M twice. Obviously, such duplicated storage wastes storage space and communication bandwidth. We present an attribute-based storage system which employs ciphertext-policy attribute-based encryption (CP-ABE) and supports secure deduplication. Our main contributions can be summarized as follows.•Firstly, the system is the first that achieves the standard notion of semantic security for data confidentiality in attribute-based deduplication systems by resorting to the hybrid cloud architecture. •Secondly, we put forth a methodology to modify a cipher text over one access policy into cipher texts of the same plaintext but under any other access policies without revealing the underlying plaintext. This technique might be of independent interest in addition to the application in the proposed storage system. •Thirdly,we propose an approach based on two cryptographic primitives, including a zero-knowledge proof of knowledge and a commitment scheme, to achieve data consistency in the system

2. LITERATURE SURVEY

Distributed computing, an advantageous method for getting to administrations, assets and applications over the Internet, moves the focal point of ventures and associations from the sending and dayto-day running of their IT offices by giving an on-request, self-administration, and pay-as-you-go plan of action. It is, in this way, obvious that distributed computing has kept on expanding in fame lately. While distributed computing gives different advantages to clients, there are hidden security and protection dangers. For instance, multi-tenure, asset pooling and shareability highlights can be misused by cybercriminals and anyonewith amalicious expectation, to the disservice of both cloud clients and cloud specialist co-ops. It is obvious, at that point, that distributed computing has risen as a notable region of request for security scientists. For instance, when client information (for example reports, recordings and photographs) are transferred or put away in a distributed computing administration, the information proprietors are probably not going to know the way of the transmitted information or whether the information are being gathered and dissected by an outsider, including an administration organization

Contingent intermediary re-encryption (CPRE) empowers fine-grained designation of decoding rights, and has some genuine applications. In this paper, we present a ciphertext-approach property based CPRE conspire, together with a formalization of the crude and its security examination. We exhibit the utility of the plan in a cloud sending, which accomplishes fine-grained information sharing. This application executes cloud server-empowered client repudiation, offering an option yet progressively productive answer for the client denial issue with regards to fine-grained encryption of cloud information. High client side productivity is another conspicuous component of the application, which makes it feasible for clients to utilize asset compelled gadgets, e.g., cell phones, to access cloud information. Our assessments show promising outcomes on the presentation of the proposed plan.

Plate based deduplication stockpiling has developed as the new-age stockpiling framework for big business information security to supplant tape libraries. Deduplication expels excess information sections to pack information into a very conservative structure and makes it prudent to store reinforcements on plate rather than tape. A critical necessity for big business information assurance is high throughput, regularly more than 100 MB/sec, which empowers reinforcements to finish rapidly. A noteworthy test is to recognize and take out copy information fragments in light of present conditions on a minimal effort framework that can't bear the cost of enough RAM to store a list of the put away portions and might be compelled to get to an on-plate list for each information section. This paper portrays three procedures utilized in the generation Data Domain deduplication document framework to soothe the circle bottleneck. These strategies include: (1) the Summary Vector, a conservative in-memory information structure for distinguishing new sections; (2) Stream-Informed Segment Layout, an information format strategy to enhance plate area for consecutively gotten to fragments; and (3) Locality Preserved Caching, which keeps up the region of the fingerprints of copy portions to accomplish high store hit proportions. Together, they can evacuate 99% of the plate gets to for deduplication of true outstanding tasks at hand. These procedures empower an advanced two-attachment double center framework to keep running at 90% CPU usage with just a single rack of 15 circles and accomplish 100 MB/sec for single-stream throughput and 210 MB/sec for multi-stream throughput.

3. EXISTING SYSTEM

When a user uploads data that already exist in the cloud storage, the user should be deterred from accessing the data that were stored before he obtained the ownership by uploading it (backward secrecy)2. These dynamic ownership changes may occur very frequently in a practical cloud system, and thus, it should be properly managed in order to avoid the security degradation of the cloud service. In the former approach, most of the existing schemes have been proposed in order to perform a PoW process in an efficient and robust manner, since the hash of the file, which is treated as a “proof” for the entire file, is vulnerable to being leaked to outside adversaries because of its

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

relatively small size. a data owner uploads data that do not already exist in the cloud storage, he is called an initial uploader; if the data already exist, called a subsequent uploader since this implies that other owners may have uploaded the same data previously, he is called a subsequent uploader.

User deduplication on the client-side, cannot generate a new tag when they update the file. In this situation, the dynamic Ownerships would fail. As a summary, existing dynamic Ownerships cannot be extended to the multi-user environment. Whenever data is transformed, concerns arise about potential loss of data. By definition, data deduplication systems store data differently from how it was written. As a result, users are concerned with the integrity of their data. One method for deduplicating data relies on the use of cryptographic hash functions to identify duplicate segments of data. If two different pieces of information generate the same hash value, this is known as a collision. The probability of a collision depends upon the hash function used, and although the probabilities are small, they are always non zero.

4. PROPOSED SYSTEM

This Project the goal of saving storage space for cloud storage services also is used for secure deduplication .but several process have been this same concept for deduplication. however this project flow some different modules in there . In this case, if two users upload the same file, the cloud server can discern the equal ciphertexts and store. only one copy of them. This process some authentication available in some issue for security purpose . through this process for ensure secured deduplication. A owner wants to outsource data to the cloud and share it with users possessing certain credentials. The Attribute Authority issues every user a decryption key associated with users set of attributes. which is considered to be the most important challenge for efficient and secure cloud storage services in the environment where ownership changes dynamically. Every time data provider upload file checking from cloud for save storage purpose . Most of the schemes have been proposed to provide data encryption, while still benefiting from a deduplication technique. every user get secured key form admin for security purpose .user can not take any key he can not download chipertext file .they can download only encrypted data. every details manage and maintain by Attribute authority.

System has two advantages. Firstly, it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. Secondly, it achieves the standard notion of semantic security for data confidentiality while existing systems only achieve it by defining a weaker security notion. In addition, we put forth a methodology to modify a ciphertext over one access policy into ciphertexts of the same plaintext but under other access policies without revealing the underlying plaintext.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

5. SYSTEM ARCHITECTURE:

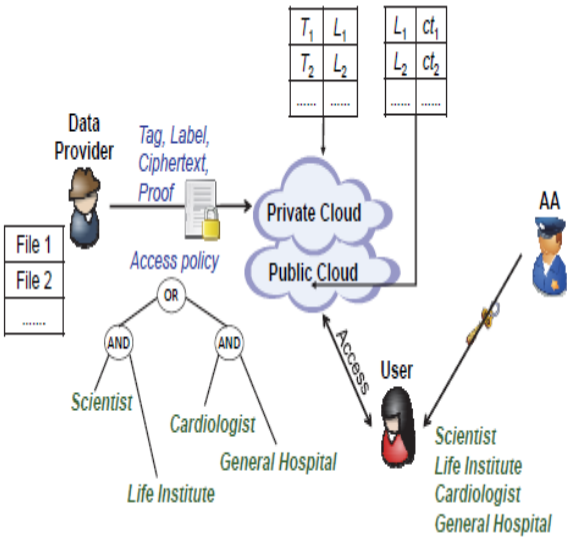

Fig 1 System Architecture

6. IMPLEMENTATION

Data Provider:-

Data provider uploading file to cloud with tag , label and security key , the proposed scheme guarantees data integrity against any tag inconsistency attack. Thus, security is enhanced in the proposed scheme.

Cloud Storage:-

Secure Deduplication with the goal of saving storage spacefor cloud storage services, Douceur et al the first solution for balancing confidentiality and efficiency in performing deduplication called convergent encryption, where a message is encrypted under a message-derived key so that identical plaintexts are encrypted to the same ciphertexts. In this case, if two users upload the same file, the cloud server can discern the equal ciphertexts and store only one copy of them. which may violate the privacy of the data if the cloud server cannot be fully trusted . This is a client who owns data, and wishes to upload it into the cloud storage to save costs. A data owner encrypts the data and outsources it to the cloud storage with its index information, that is, a tag.

Deduplication:-

Data deduplication is a specialized data compression technique for eliminating duplicate copies of repeating data. Related and somewhat synonymous terms are intelligent (data) compression and single-instance (data) storage. This technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. In the deduplication process, unique chunks of data, or byte patterns, are identified and stored during a process of analysis. Deduplication techniques take advantage of data similarity to identify the same data and reduce the storage space. In contrast, encryption algorithms randomize the encrypted files in order to make ciphertext indistinguishable from theoretically random data.

Attribute Authority:

The AA issues every user a decryption keyassociated with user set of attributes At the user side, each user can download an item, and decrypt the ciphertext with the attribute-based private key generated by the AA if this user's attribute set satisfies the access structure.

7. CONCULUTION

Attribute-based encryption (ABE) has been widely used in cloud computing where a data provider outsources his/her encrypted data to a cloud service provider, and can share the data with users possessing specific credentials (or attributes). However, the standard ABE system does not support secure deduplication, which is crucial for

eliminating duplicate copies of identical data inorder to save storage space and network bandwidth. In this paper, we present an attribute-based storage system with secure deduplication in a hybrid cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage. That can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. In addition, we put forth a methodology to modify a ciphertext over one access policy into ciphertexts of the same plaintext but under other access policies without revealing the underlying plaintext.

BIBILOGRAPHY

[1] M. A. Beyer and D. Laney, "The importance of big data: a definition," Stamford, CT: Gartner, 2012.

[2] V. Marx, "Biology: The big challenges of big data," Nature, vol. 498, no. 7453, pp. 255–260, 2013.

[3] G. P. Consortium et al., "A map of human genome variation from population-scale sequencing," Nature, vol. 467, no. 7319, pp. 1061–1073, 2010.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT 2005, pp. 457–473, 2005.

[5] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.

[6] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94– 107, 2016.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 89–98.

[8] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," Public Key Cryptography– PKC 2011, pp. 53–70, 2011.

[9] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," IEEE journal on selected areas in communications, vol. 31, no. 9, pp. 37–46, 2013.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT 2011, pp. 568–588, 2011.

[11] C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, "An attributebased signcryption scheme to secure attribute-defined multicast communications," in SecureComm 2015. Springer, 2015, pp. 418–435.

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.

[13] M. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multisecret sharing," Computer Standards & Interfaces, vol. 30, no. 3, pp. 187–190, 2008.

[14] Z. Eslami and J. Z. Ahmadabadi, "A verifiable multi-secret sharing scheme based on cellular automata," Information Sciences, vol. 180, no. 15, pp. 2889–2894, 2010.
[15] M. H. Dehkordi and S. Mashhadi, "New efficient and practical verifiable multi-secret sharing schemes," Information Sciences, vol. 178, no. 9, pp. 2262–2274, 2008.
[16] J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," Computer Standards & Interfaces, vol. 29, no. 1, pp. 138–141, 2007.
[17] C. Hu, X. Liao, and X. Cheng, "Verifiable multi-secret sharing based on LFSR sequences," Theoretical Computer Science, vol. 445, 2012.
[18] C. Hu, X. Liao, and D. Xiao, "Secret image sharing based on chaotic map and chinese remainder theorem," International Journal of Wavelets, Multiresolution and Information Processing, vol. 10, no. 03, 2012.
[19] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dac-macs: Effective data access control for multiauthority cloud storage systems," Information Forensics and Security, IEEE Transactions on, vol. 8, no. 11, pp. 1790– 1801, 2013.
[20] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 7, pp. 1735–1744, 2014.

AUTHORS PROFILE

Sk. Aakhila Begum is a student pursuing MTech(CSE) in Eswar college Of Engineering, Narasaraopet, Guntur.

MD.Jhon Saida M.Tech in Computer Science & Engineering. He is currently working as an Asst Professor in Eswar College of Engineering, Narasaraopet, Guntur, India. He is having about 10 years of teaching experience in different Engineering Colleges.