Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 6, Issue 4, April-2019

Efficient Client-Side Deduplication of Encrypted Data in Cloud Storage

Tejaswini Kailuke[1], Vikas Singh[2], Raj Waykos[3],Swati Jadhav[4] , Tejaswini Joshi[5]

[1]*Department of Information Technology,PCCOE Pune, Maharashtra, India*
[2]*Department of Information Technology, PCCOE, Pune, Maharashtra, India*
[3]*Department of Information Technology, PCCOE, Pune, Maharashtra, India*
[4]*Department of InformationTechnology, PCCOE, Pune, Maharashtra, India*
[5]*Department of InformationTechnology, PCCOE, Pune, Maharashtra, India*

Abstract — Attribute-based secret writing (ABE) has been wide employed in cloud computing wherever knowledge|a knowledge|an information} supplier outsources his/her encrypted data to a cloud service supplier, and may share the info with users possessing specific credentials (or attributes). However, the quality ABE system doesn't support secure de duplication, that is crucial for eliminating duplicate copies of identical information so as to save lots of space for storing and network information measure. during this paper, we have a tendency to gift associate attribute-based storage system with secure deduplication during a hybrid cloud setting, wherever a personal cloud is liable for duplicate detection and a public cloud manages the storage. Compared with the previous information deduplication systems, our system has 2 blessings. Firstly, it are often wont to confidentially share information with users by specifying access policies instead of sharing secret writing keys. Secondly, it come throughs the quality notion of linguistics security for information confidentiality whereas existing systems solely achieve it by shaping a weaker security notion. additionally, we have a tendency to place forth a technique to switch a ciphertext over one access policy into ciphertexts of identical plaintext however beneath different access policies while not revealing the underlying plaintext.

Keywords - Attribute-based encryption, access control, audit logs, broadcast encryption, delegation, hierarchical identitybased encryption.

INTRODUCTION

Cloud computing greatly facilitates information suppliers World Health Organization ought to supply their information to the cloud whereas not revealing their sensitive information to external parties and would love users with sure credentials to be able to access the data. this desires information to be hold on in encrypted forms with access management policies such no one except users with attributes (or credentials) of specific forms can decipher the encrypted information. degree cryptography technique that meets this demand is termed attribute-based cryptography (ABE), where a user's personal secret's associated with degree attribute set, a message is encrypted below degree access policy (or access structure) over a bunch of attributes, and a user can decipher a ciphertext with his/her personal key if his/her set of attributes satisfies the access policy associated with this ciphertext. However, the standard ABE system fails to appreciate secure deduplication, which will be a method to avoid wasting area for storing and network system of measurement by eliminating redundant copies of the encrypted information hold on among the cloud. On the alternative hand, to the foremost effective of our data, existing constructions for secure deduplication are not built on attribute-based cryptography. however, since ABE and secure deduplication area unit wide applied in cloud computing, it would be fascinating to vogue a cloud storage system possessing every properties.

LITERATURE REVIEW

1.**Paper name:**Cloud Cryptography: Theory, apply and Future analysis Directions
Author: Elsevier B.V.
Cloud computing, a convenient manner of accessing services,resources and applications over the net, shifts the main target of industries ANd organizations faraway from the preparation and day-after-day running of their IT facilities by providing an on-demand,self-service, and pay-as-you-go business model. It is, therefore,unsurprising that cloud computing has continuing to extend in quality in recent times.

2.Paper name:Cloud primarily based information sharing with fine-grained proxy re-encryption
Author: Yanjiang rule a , Haiyan Zhu , Haibing Lu , Jian Weng , Youcheng Zhang ,
Kim-Kwang Raymond Choo.
Conditional proxy re-encryption (CPRE) allows fine-grained delegation of secret writing rights, and has several real-world applications. during this paper, we tend to gift a ciphertext-policy attributebased CPRE scheme,together with a formalization of the primitive an dits security analysis. we tend to demonstrate the utility of the theme during a cloud preparation, that achieves fine-grained information sharing. This application implements cloud server-enabled user revocation, providing another nevertheless additional economical answer to the user revocation downside in the context of fine-grained encoding of cloud information. High user-side potency is another prominent feature of the application,which makes it possible for users to use resource con-strained devices, e.g., mobile phones, to access cloud information. Our evaluations show promising results on the performance of the planned theme.

3. **Paper name:** Google Drive: rhetorical analysis of information remnants
Author: Darren fast n , Kim-Kwang Raymond Choo
Cloud storage is AN rising challenge to digital rhetorical examiners. The services square measure progressively employed by shoppers, business, and government, and may doubtless store giant amounts of information. The retrieval of digital proof from cloud storage services (particularly from offshore providers) is a challenge during a digital rhetorical investigation, thanks to virtualisation, lack of data on location of digital proof,privacy problems, and legal or territorial boundaries. Google Drive may be a common service, providing users an economical, and in some cases free, ability to access, store, collaborate, and air information. victimization Google Drive as a case study, artefacts were known that square measure probably to stay once the utilization of cloud storage, within the context of the experiments, on a laptop disc drive and Apple iPhone3G, and therefore the potential access point(s) for digital forensics examiners to secure proof

4.Paper name: Fuzzy Identity-Based encoding
Author: Mihir Bellare, Sriram Keelveedhi ,Thomas Ristenpart
Cloud storage service suppliers like Dropbox, Mozy,and others perform deduplication to avoid wasting house by solely storing one copy of every file uploaded. ought to shoppers conventionally cypher their files, however, savings square measure lost. Message-locked encoding (the most distinguished manifestation of that is focused encryption) re-solves this tension. but it's inherently subject to brute-force attacks that may recover files falling into a best-known set. we tend to propose AN design that gives secure deduplicated storage resisting brute-force attacks, and are aware of it during a system known as DupLESS. In DupLESS, shoppers cypher underneath message-based keys obtained from a key-server via AN oblivious PRF protocol.It allows shoppers to store encrypted information with AN existing service, have the service perform deduplication on their behalf, and nevertheless achieves sturdy confidentiality guarantees. we tend to show that encoding for deduplicated storage can do performance and house savings on the brink of that can deliver the goods performance and house savings on the brink of that can do performance and house savings on the brink of that of victimization the storage service with plaintext information.

5.Paper name: Attribute-Based encoding for Fine-Grained Access management of Encrypted information
Author: Vipul Goyal Omkant Pandey Amit Sahai brent goose Waters
As additional sensitive information is shared and hold on by third-party sites on the net, there'll be a requirement to cypher information hold on at these sites. One disadvantage of encrypting information, is that it is by selection shared solely at a coarse-grained level (i.e., giving another party your personal key). we tend to develop a brand new cryptosystem for fine-grained sharing of encrypted information that we tend to decision Key-Policy Attribute-Based encoding (KP-ABE). In our cryptosystem, ciphertexts square measure labelled with sets of attributes and personal keys square measure related to access structures that management that ciphertexts a user is ready to decode. we tend to demonstrate the pertinency of our construction to sharing of audit-log info and broadcast encoding. Our construction supports delegation of personal keys that subsumes ranked Identity-Based encoding (HIBE).

EXISTING SYSTEM

In the existing the cloud service provider, and would possibly share the knowledge with users possessing specific credentials (or attributes). inside the present system the standard ABE system does not support secure deduplication, that's crucial for eliminating duplicate copies of identical information therefore on save several area for storing and network system of measurement.

Disadvantages of existing system:

-System does not support secure de-duplication

-Access policies whereas not revealing the underlying plaintext.

-Existing systems alone succeed it by shaping a weaker security notion

PROPOSE SYSTEM

We gift associate attribute-based storage system with secure deduplication in an exceedingly} very hybrid cloud setting, where a personal cloud is guilty for duplicate detection and a public cloud manages the storage.
-The auditor may be a honest organization, which can provide unbiased auditing results for owners.
-TPA(Third Party Auditor) provide associate economical secure deduplication theme.
-Regenerate code through proxy server. this technique is been developed to provide integrity and regenerating code.

Advantages Of planned system:

-We gift associate attribute-based storage system

-We propose associate approach supported two science primitives, similarly as a zero-knowledge proof of information and a commitment theme, to realize data consistency at intervals the system.

-Time based totally and access policy is given by original owner of file administrative body transfer the data

PROPOSE SYSTEM ARCHITECTURE

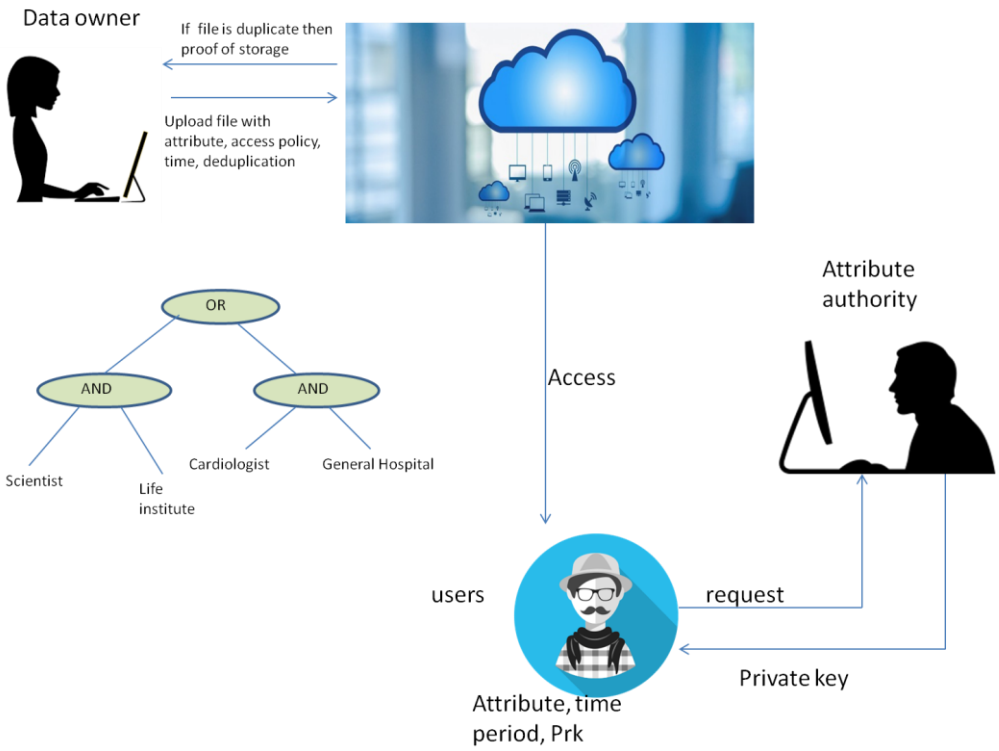

Figure 4.1. System Architecture

The architecture of our attribute-based storage system with secure deduplication is shown in Figure in which four entities are involved: data owner, attribute authority (AA), cloud and users. A data owner wants to outsource his/her data to the cloud and share it with users possessing certain credentials. The AA issues every user a decryption key associated with his/her set of attributes. The cloud consists of a public cloud which is in charge of data storage and a private cloud which performs certain computation such as tag checking. When sending a file storage request, each data provider firstly upload file with the attribute,access policy, time, and then encrypts the data under an access structure over a set of attributes.

CONCLUSION AND FUTURE SCOPE

We planned a public auditing theme for encrypted knowledge that will accomplish knowledge integrity auditing and storage first state duplication at identical time. By utilizing the thought of proxy re-encryption, the cloud server solely should store one copy of encrypted knowledge. To first state duplicate the verification tags generated by totally fully completely different venders, we tend to tend to tend to mixture the tags. The integrity of first state duplicated knowledge ar about to be properly checked by the checker on behalf of any venders. The inquiry and trial results show that our theme is secure and economical.
The planned storage system enjoys a combine of major blessings. Firstly, it's about to be accustomed confidentially share knowledge with fully completely different users by specifying award access policy instead of sharing the key writing key. Secondly, it accomplishs the quality notion of linguistics security whereas existing deduplication schemes solely win it at a lower place a weaker security notion.

The standard CP-ABE(CIPHER-PLAINTEXT ATTRIBUTE based totally ENCRYPTION) systems don't support secure deduplication, that makes them valuable to be applied in some business storage services.

REFERENCES

[1] D. Quick, B. Martini, and K. R. Choo, Cloud Storage Forensics. Syngress Publishing / Elsevier, 2014. [Online]. Available: http://www.elsevier.com/books/cloud-storageforensics/
quick/978-0-12-419970-5

[2] K. R. Choo, J. Domingo-Ferrer, and L. Zhang, “Cloud cryptography: Theory, practice and future research directions,” Future Generation Comp. Syst., vol. 62, pp. 51–53, 2016.

[3] K. R. Choo, M. Herman, M. Iorga, and B. Martini, “Cloud forensics: State-of-the-art and future directions,” Digital Investigation, vol. 18, pp. 77–78, 2016.

[4] Y. Yang, H. Zhu, H. Lu, J.Weng, Y. Zhang, and K. R. Choo, “Cloud based data sharing with fine-grained proxy re-encryption,” Pervasive and Mobile Computing, vol. 28, pp. 122–134, 2016.

[5] D. Quick and K. R. Choo, “Google drive: Forensic analysis of data remnants,” J. Network and Computer Applications, vol. 40, pp. 179– 193, 2014.

[6] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, ser. Lecture Notes
in Computer Science, vol. 3494. Springer, 2005, pp. 457–473.

[7] B. Zhu, K. Li, and R. H. Patterson, “Avoiding the disk bottleneck in the data domain deduplication file system,” in 6th USENIX Conference on File and Storage Technologies, FAST 2008, February 26-
29, 2008, San Jose, CA, USA. USENIX, 2008, pp. 269–282.

[8] M. Bellare, S. Keelveedhi, and T. Ristenpart, “Message-locked encryption and secure deduplication,” in Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the
Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ser. Lecture Notes in Computer Science, vol. 7881. Springer, 2013, pp. 296–312.

[9] M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev, “Message-locked encryption for lock-dependent messages,” in Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology

Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, ser. Lecture Notes in Computer Science, vol. 8042. Springer, 2013, pp. 374–391.

[10] S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: Serveraided encryption for deduplicated storage," in Proceedings of the 22th USENIX Security Symposium, Washington, DC, USA, August 14-16, 2013. USENIX Association, 2013, pp. 179–194.

[11] M. Bellare and S. Keelveedhi, "Interactive message-locked encryption and secure deduplication," in Public-Key Cryptography – PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 – April 1, 2015, Proceedings, ser. Lecture Notes in Computer Science, vol.9020. Springer, 2015, pp. 516–538.

[12] S. Bugiel, S. N¨ urnberger, A. Sadeghi, and T. Schneider, "Twin clouds: Secure cloud computing with low latency - (full version)," in Communications and Multimedia Security, 12th IFIP TC 6 / TC 11 International Conference, CMS 2011, Ghent, Belgium, October 19- 21,2011. Proceedings, ser. Lecture Notes in Computer Science, vol. 7025. Springer, 2011, pp. 32–44.

[13] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems (extended abstract)," in Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA. ACM, 1985, pp. 291– 304.

[14] M. Fischlin and R. Fischlin, "Efficient non-malleable commitment schemes," in Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings, ser. Lecture Notes in Computer Science, vol. 1880. Springer, 2000, pp. 413–431.

[15] S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270–299, 1984.