Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

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

Volume 5, Issue 4, April-2018

Attribute based Storage to avoid duplicate files on cloud

Chinmay Patil[1], Shubham Kasabe[2], Ronik Mahajan[3], Ajay Indani[4] , Prof. V.V. Waykule[5]

[1] Student, Department of Computer Engineering, AISSMSCOE, Pune. Maharashtra, India

[2] Student, Department of Computer Engineering, AISSMSCOE, Pune. Maharashtra, India

[3] Student, Department of Computer Engineering, AISSMSCOE, Pune. Maharashtra, India

[4] Student, Department of Computer Engineering, AISSMSCOE, Pune. Maharashtra, India

[5] Assistant Professor, Department of Computer Engineering, AISSMSCOE, Pune. Maharashtra, India

Abstract — ***Attribute-based cryptography (ABE) has been wide utilized in cloud computing wherever information{a knowledge|an information} supplier outsources his/her encrypted data to a cloud service supplier, and may share the information with users possessing specific credentials (or attributes). However, the quality ABE system doesn't support secure deduplication, that is crucial for eliminating duplicate copies of identical information so as to avoid wasting space for storing and network information measure. During this paper, we tend to gift an attribute-based storage system with secure deduplication in an exceedingly hybrid cloud setting, wherever a non-public cloud is accountable for duplicate detection and a public cloud manages the storage. Compared with the previous information deduplication systems, our system has 2 benefits. Firstly, it may be used to confidentially share information with users by specifying access policies instead of sharing cryptography keys. Secondly, it brings home the bacons the quality notion of linguistics security for information confidentiality whereas existing systems solely achieve it by process a weaker security notion. Additionally, we tend to place forth a technique to switch a ciphertext over one access policy into ciphertexts of an equivalent plaintext however underneath different access policies while not revealing the underlying plaintext.***

INTRODUCTION

Cloud computing greatly facilitates knowledge suppliers UN agency need to source their knowledge to the cloud while not revealing their sensitive knowledge to external parties and would love users with sure credentials to be able to access the information. this needs knowledge to be keep in encrypted forms with access management policies such nobody except users with attributes (or credentials) of specific forms will rewrite the encrypted knowledge. An coding technique that meets this demand is named attribute-based coding (ABE), wherever a user's personal secret's related to an attribute set, a message is encrypted beneath an access policy (or access structure) over a collection of attributes, and a user will rewrite a ciphertext with his/her personal key if his/her set of attributes satisfies the access policy related to this ciphertext. However, the quality ABE system fails to attain secure deduplication, that could be a technique to avoid wasting cupboard space and network information measure by eliminating redundant copies of the encrypted knowledge keep within the cloud. On the opposite hand, to the simplest of our data, existing constructions for secure deduplication aren't engineered on attribute-based coding. Notwithstanding, ABE and secure deduplication are widely applied in cloud computing, it might be fascinating to style a cloud storage system possessing each properties.

I. PROBLEM STATEMENT

Attribute-based cryptography (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 might share the information with users possessing specific credentials (or attributes). However, the quality ABE system doesn't support secure deduplication, that is crucial for eliminating duplicate copies of identical knowledge so as to avoid wasting cupboard space and network information measure.

We gift an attribute-based storage system with secure deduplication during a hybrid cloud setting, wherever a personal cloud is chargeable for duplicate detection and a public cloud manages the storage.

II. LITERATURE REVIEW

Title: A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram

Authors: Long Li, Tianlong Gu, Liang Chang, Zhoubo Xu, Yining Liu, Junyan Qian

Improves potency and capability within the expression of access policies, however additionally reduces the most computation of the KeyGen algorithmic program, the scale of secret key and therefore the main computation of the rewrite algorithmic program to constants, so taking off their relationships with the quantity of attributes. Besides, the potency of the encipher algorithmic program and therefore the size of ciphertext also can be improved.

Title: ClouDedup: Secure Deduplication with Encrypted Data for Cloud Storage

Authors: Pasquale Puzio, Refik Molva, Melek Onen, Sergio Loureiro

A secure and economical storage service that assures block-level deduplication and knowledge confidentiality at a similar time. though supported confluent secret writing, ClouDedup remains secure because of the definition of a part that implements a further secret writing operation associate degreed an access management mechanism.

Title: Improving Security and Efficiency in Attribute-Based Data Sharing

Authors : Junbeom Hur

The performance and security analyses indicate that the projected theme is economical to firmly manage knowledge|the info|the information} distributed within the data sharing system.

III. EXISTING SYSTEM

In the existing system the cloud service supplier, and may not share the infomation with users possessing specific credentials (or attributes).

In the existing system the quality ABE system doesn't support secure deduplication, that is crucial for eliminating duplicate copies of identical information so as to save lots of cupboard space and network information measure.

IV. MATHEMATICAL MODEL

System = S {I, P , O}

Input - I

U= Users

$U = \{u_1, u_2, u_3, \ldots\ldots\ldots, u_n\}$

F = Files

F = $\{f_1, f_2, f_3, \ldots\ldots\ldots, f_n\}$

Process – P

Step 1

User upload the files ‘f’ and select the access policy ‘ a_p’ file as well as time period ‘t_p’ for accessing file

F = $\{f_1a_{p1}t_{p1}, f_2a_{p2}t_{p2\ldots\ldots\ldots}, f_na_{pn}t_{pn}\}$

Step 2

File tag generated ‘T’ by using SHA-1 algorithm

T → F = T(F)

Step 3

Key is generated (k)

K → F

Step 4

Check deduplication (D) by checking tag is exist in database server or not

i.e. D = T ϵ (T (F))

if (T = T (F))

“File does not exist”

else

“file exist”

i.e. T ł T (F)

then encrypt file by using AES algorithm with key.

Output - O

If file does not match with database server file then only file is stored on cloud

V. ARCHITECTURE DIAGRAM OF SYSTEM

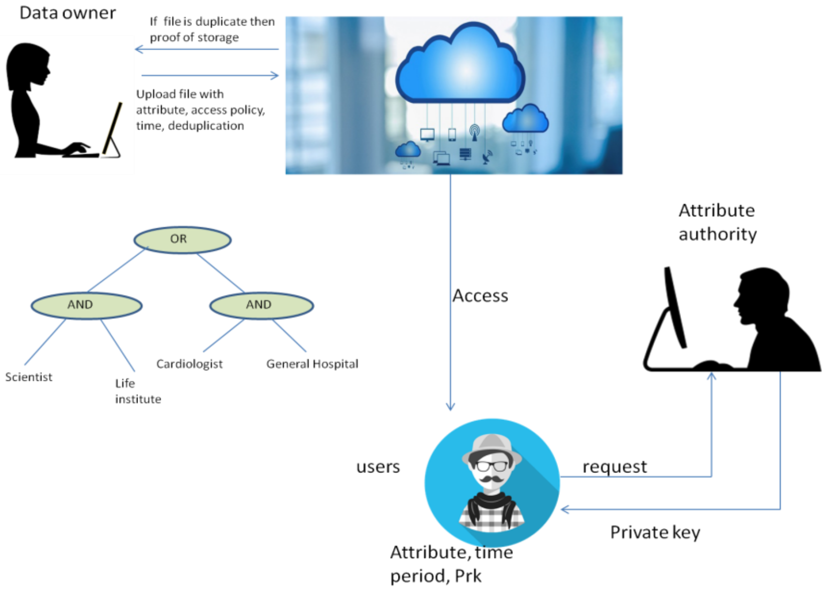
Data owner
If file is duplicate then proof of storage
Upload file with attribute, access policy, time, deduplication
OR
AND
AND
Scientist
Life institute
Cardiologist
General Hospital
Access
Attribute authority
users
request
Private key
Attribute, time period, Prk

Figure 4.2. Architecture diagram

VI. HARDWARE REQUIREMENT

System Processors	:	Core2Duo
Speed	:	2.4 GHz
Hard Disk	:	150 GB

VII. ADVANTAGES

- We present an attribute-based storage system that supports secure deduplication.
- 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.
- Time based and access policy is given by original owner of file who uploads the data.

VIII. DISADVANTAGES

- System does not support video and audio files.

IX. APPLICATION

- To avoid overhead
- Organization use this system to avoid duplicate file
- To save memory

X. CONCLUSION AND FUTURE SCOPE

In our system owner transfers the file with the attributes and access policy, accessing time, then transfers file check for checking whether the file is duplicate or not. On this if file is duplicate then the owner of the file will get proof of possession and if file is original then store it on cloud and once user request for file attribute authority can check the attributes of user then solely user can get key to access the file from cloud. The application will enable us to avoid redundant files in cloud which leads to save of storage space and network bandwidth. Also it improves the security notion as encryption algorithms are used and the misuse of files can be avoided as the sharing of files or data with other users is done by specifying the access policy rather than the decryption keys.

ACKNOWLEDGMENT

Authors want to acknowledge Principal, Head of department and guide of their project for all the support and help rendered. To express profound feeling of appreciation to their regarded guardians for giving the motivation required to the finishing of paper.

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.

[16] 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, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006, ser. Lecture Notes in Computer Science, vol. 5126. Springer, 2006, pp. 89–98.

[17] R. Ostrovsky, A. Sahai, and B.Waters, “Attribute-based encryption with non-monotonic access structures,” in Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007. ACM, 2007, pp. 195–203.

[18] A. B. Lewko and B. Waters, “Unbounded HIBE and attributebased encryption,” in Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings, ser. Lecture Notes in Computer Science, vol. 6632. Springer, 2011, pp. 547–567.

[19] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA.
IEEE Computer Society, 2007, pp. 321–334.

[20] L. Cheung and C. C. Newport, “Provably secure ciphertext policy ABE,” in Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA,
October 28-31, 2007. ACM, 2007, pp. 456–465.

[21] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded ciphertext policy attribute based encryption,” in Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik,