Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 10, October -2017

Survey on Timed and Attribute Based Storage Secure Deduplication of Data in Cloud

[1]Pallavi, [2]Jyoti, [3]Ajinkya, [4]Chandrashekhar

[1,2,3,4] *Department Of Computer Engineering, SIT, Lonavala.*

Abstract — *Attribute-based cryptography (ABE) has been wide utilized in cloud computing wherever a knowledge supplier outsources his/her encrypted knowledge to a cloud service supplier, and might share the info with users possessing specific credentials (or attributes). However, the standard ABE system doesn't support secure deduplication, that is crucial for eliminating duplicate copies of identical knowledge in order to avoid wasting space for storing and network information measure. During this paper, we tend to gift Associate in nursing attribute-based storage system with secure deduplication during a hybrid cloud setting, wherever a personal cloud is to blame for duplicate detection and a public cloud manages the storage. Compared with the previous knowledge deduplication systems, our system has 2 benefits. Firstly, it may be wont to confidentially share knowledge with users by specifying access policies instead of sharing coding keys. Secondly, it achieves the quality notion of semantic security for knowledge confidentiality whereas existing systems solely accomplish it by shaping a weaker security notion. additionally, we put forth a technique to change a ciphertext over one access policy into ciphertexts of an equivalent plaintext however underneath alternative access policies without revealing the underlying plaintext.*

Keywords- *ABE, Storage, Deduplication.*

I. INTRODUCTION

Cloud computing greatly facilitates knowledge suppliers WHO wish to source their knowledge to the cloud while not revealing their sensitive knowledge to external parties and would really like users with bound credentials to be ready to access the info. 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 decipher the encrypted knowledge. associate cryptography technique that meets this demand is named attribute-based cryptography (ABE), wherever a user's non-public key's related to associate attribute set, a message is encrypted below associate access policy (or access structure) over a collection of attributes, and a user will decipher a ciphertext with his/her non-public 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 may be a technique to save lots of space for storing 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 are not designed on attribute-based cryptography. yet, since ABE and secure deduplication are wide applied in cloud computing, it'd be fascinating to style a cloud storage system possessing each properties.

II. LITERATURE SURVEY

According to literature survey after studying various IEEE paper, collected some related papers and documents some of the point describe here:

1. **Paper name:** Attribute-Based Encryption With Verifiable Outsourced Decryption
   Author: Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng
   Description: ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and ciphertexts.

2. **Paper name:** Improving Security and Efficiency in Attribute-Based Data Sharing
   Authors: Junbeom Hur
   Description: The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system

3. **Paper name:** 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
   Description: Improves potency and capability within the expression of access policies, however conjointly reduces the most computation of the KeyGen rule, the scale of secret key and also the main computation of the

decipher rule to constants, so pruning their relationships with the quantity of attributes. Besides, the potency of the code rule and also the size of ciphertext also can be improved.

4. **Paper Name:** ClouDedup: Secure Deduplication with Encrypted Data for Cloud Storage
Author: Pasquale Puzio, Refik Molva, Melek Onen, Sergio Loureiro
Description: A secure and economical storage service that assures block-level deduplication and knowledge confidentiality at an equivalent time. though supported oblique coding, ClouDedup remains secure because of the definition of a element that implements a further coding operation associate degreed an access management mechanism.
5. **Paper Name:** A Secure Cloud Backup System with Assured Deletion and Version Control
Author: Arthur Rahumed, Henry C. H. Chen, Yang Tang, Patrick P. C. Lee, and John C. S. Lui
Description: In this paper particular file save data accordingly to container but same data or duplicate data save in another container .To access duplicate data that time proof-of-ownership concept is used

III.EXISTING SYSTEM

In the prevailing the cloud service supplier, and might share the information with users possessing specific credentials .In the prevailing system the quality ABE system doesn't support secure deduplication, that is crucial for eliminating duplicate copies of identical information so as to avoid wasting cupboard space and network information measure.

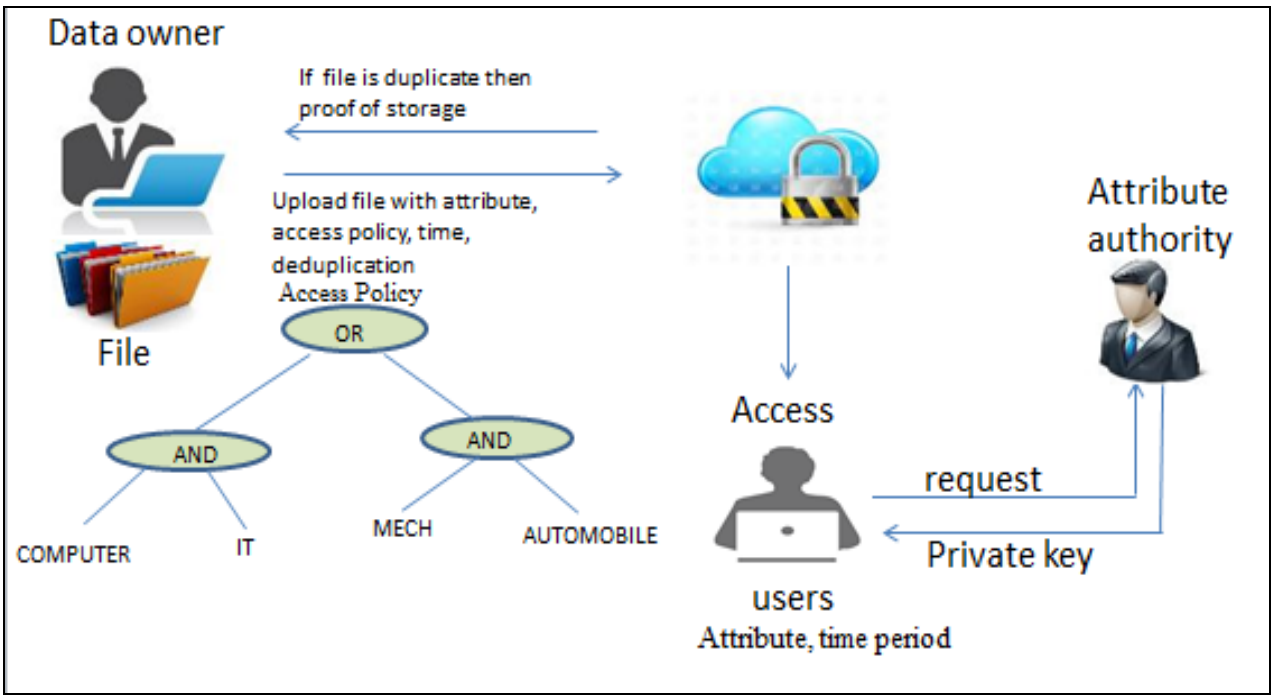
IV.DISADVANTAGES

System doesn't support secure de-duplication
Access policies while not revealing the underlying plaintext.
Existing systems solely accomplish it by process a weaker security notion

V.PROPOSED SYSTEM

In the planned system associate attribute-based storage system with secure De-duplication .De-duplication during a hybrid cloud environment, wherever a personal cloud is chargeable for duplicate detection and a public cloud manages The storage. planned system Compared with the previous information de-duplication systems. As our system support high security and potency, additionally as our system to boot file transfer upload file by specifying period and access policy.

VI.SYSTEM DESIGN



VII. ADVANTAGES

We give an attribute-based storage system
We propose an approach supported 2 cryptanalytic primitives, as well as a zero-knowledge proof of knowledge and a commitment theme, to attain information consistency within the system.
Time based mostly and access policy is given by original owner of file UN agency transfer the information.

VIII. CONCLUSION

In proposed system owner transfer the file with the attributes and access policy, accessing time, then transfer file check for weather file is duplication or not. once this if file is duplicate then owner of the get proof of possession and if file is original then store 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.

REFERENCES

[1]LAI, Junzuo; DENG, Robert H.; GUAN, Chaowen; and WENG, Jian. Attribute-based encryption with verifiable outsourced decryption. (2013). IEEE Transactions on Information Forensics and Security. 8, (8), 1343-1354. Research Collection School Of Information Systems.

[2] Arthur Rahumed, Henry C. H. Chen, Yang Tang, Patrick P. C. Lee, and John C. S. Lui. A Secure Cloud Backup System with Assured Deletion and Version Control, 1530-2016/11 $26.00 © 2011 IEEE DOI 10.1109/ICPPW.2011.17

[3] Junbeom Hur, Improving Security and Efficiency in Attribute-Based Data Sharing. IEEE transactions on knowledge and data engineering vol:25 no:10 year 2013

[4] Long Li, Tianlong Gu , Liang Chang, Zhoubo Xu , Yining Liu, Junyan Qian, A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram. Article Citation information: DOI 10.1109/ACCESS.2017.2651904, IEEE Access

[5] Pasquale Puzio , Refik Molva , Melek Onen , Sergio Loureiro , ClouDedup : Secure Deduplication with Encrypted Data for Cloud Storage, 978-0-7695-5095-4/13 $31.00 © 2013 IEEE, 2013 IEEE International Conference on Cloud Computing Technology and Science

[6] 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

[7] K. R. Choo, J. Domingo-Ferrer, and L. Zhang, "Cloud cryptography: Theory, practice and future research directions," Future Generation Comp. Syst., vol. 62, pp. 5sss1–53, 2016.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

