A Study of Time and Attribute Based Deduplication of Secure Storge

[1]Miss. Pallavi Gorade, [2]Miss.Jyoti Patil, [3]Mr.Ajinkya Keshar Khane, [4]Mr.Chandrashekhar Hiwrale

Department of Computer Engineering,
Sinhgad Institute of Technology, Lonavala.

***Abstract* — Attribute-based cryptography (ABE) has been wide developed in cloud computing wherever a knowledge supplier outsources his/her encrypted knowledge to a cloud service supplier, and might share the info with users having specific credentials (or attributes). However, the standard ABE system doesn't support secure deduplication, that is critical for removing 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 responsibility for duplicate detection and a public cloud manages the storage. Compared with the earlier knowledge deduplication systems, our system has 2 benefits. Firstly, it may be wont to confidentially share knowledge with users by specifying access policies in its place of sharing coding keys. Secondly, it achieves the quality notion of semantic security for knowledge confidentiality whereas existing systems just accomplish it by shaping a weaker security notion. Moreover, we put forth a technique to change a ciphertext over one access policy into ciphertexts of an equivalent plaintext however under alternative access policies without revealing the fundamental 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

[1] Paper Name:"A Secure Cloud Backup System with Assured Deletion and Version Control"
Authors: Arthur Rahumed, Henry C. H. Chen, Yang Tang, Patrick ,P. C. Lee, and John C. S. Lui (Corresponding Author)
Description: Cloud storage is an emerging service model that enables individuals and enterprises to outsource the storage of data backups to remote cloud providers at a low cost. However, cloud clients must enforce security guarantees of their outsourced data backups. We present Fade Version, a secure cloud backup system that serves as a security layer on top of todays cloud storage services. Fade Version follows the standard version controlled backup design, which eliminates the storage of redundant data across different versions of backups. On top of this, Fade Version applies cryptographic protection to data backups. Specifically, it enables fine-grained assured deletion, that is, cloud clients can assuredly delete particular backup versions or files on the cloud and make them permanently inaccessible to anyone, while other versions that share the common data of the deleted versions or files will remain unaffected. We implement a proof-of-concept prototype of Fade Version and conduct empirical evaluation atop Amazon S3. We show that Fade Version only adds minimal performance overhead over a traditional cloud backup service that does not support assured deletion.

[2] Paper name: Attribute-based encryption with verifiable outsourced decryption
Authors: Junzuo LAI, Robert H. DENG, Chaowen GUA,Jian WENG
Description: Attribute-based encryption (ABE) is a public key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher texts. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. Recently, Green et al. proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher text satisfied by that users attributes or access

policy into a simple cipher text, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher text. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious cloud) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud. In this paper, we consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. We give the formal model of ABE with verifiable outsourced decryption and propose a concrete scheme. We prove that our new scheme is both secure and verifiable, without relying on random oracles.

[3] Paper name :Improving Security and Efficiency in Attribute-Based Data Sharing
Authors: Junbeom Hur
Description: With the recent adoption and diffusion of the data sharing paradigm in distributed systems such as online social networks or cloud computing, there have been increasing demands and concerns for distributed data security. One of the most challenging issues in data sharing systems is the enforcement of access policies and the support of policies updates. Cipher text policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic solution to this issue. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. However, the advantage comes with a major drawback which is known as a key escrow problem. The key generation center could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users. In addition, applying CP-ABE in the data sharing system introduces another challenge with regard to the user revocation since the access policies are defined only over the attribute universe. Therefore, in this study, we propose a novel CP-ABE scheme for a data sharing system by exploiting the characteristic of the system architecture. The proposed scheme features the following achievements: 1) the key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two party computation between the key generation center and the data-storing center, and 2) fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.

[4] Paper Name:ClouDedup: Secure Deduplication with Encrypted Data for Cloud Storage
Authors: Pasquale Puzio, Re_k Molva,Melek Onen,Sergio Loureiro
Description: With the continuous and exponential increase of the number of users and the size of their data, data deduplication becomes more and more a necessity for cloud storage providers. By storing a unique copy of duplicate data, cloud providers greatly reduce their storage and data transfer costs. The advantages of deduplication unfortunately come with a high cost in terms of new security and privacy challenges. We propose ClouDedup, a secure and efficient storage service which assures block-level deduplication and data confidentiality at the same time. Although based on convergent encryption, ClouDedup remains secure thanks to the definition of a component that implements an additional encryption operation and an access control mechanism. Furthermore, as the requirement for deduplication at block-level raises an issue with respect to key management, we suggest to include a new component in order to implement the key management for each block together with the actual deduplication operation .We show that the overhead introduced by these new components is minimal and does not impact the overall storage and computational costs.

[5]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: Cipher text-policy attribute-based encryption (CP- ABE) is widely used in many cyber physical systems and the Internet of things for guaranteeing information security. In order to improve the performance and efficiency of CP-ABE, this paper makes a change to the access structure of describing access polices in CP-ABE, and presents a new CP-ABE system based on the ordered binary decision diagram (OBDD). The new system makes full use of both the powerful description ability and the high calculating efficiency of OBDD. First, in the access structure, the new system allows multiple occurrences of the same attribute in a strategy, supports both positive attribute and negative attribute in the description of access polices, and can describe free-form access polices by using Boolean operations. Second, in the key generation stage, the size of secret keys generated by the new system is constant and not affected by the number of attributes; furthermore, time complexity of the key generation algorithm is O(1). Thirdly, in the encryption stage, both the time complexity of the encryption algorithm and the size of generated cipher text are determined by the number of valid paths contained in the OBDD instead of the number of attributes occurring in access polices. Finally, in the decryption stage, the new system supports fast decryption and the time complexity of the decryption algorithm is only O(1). As a result, compared with existing CP-ABE schemes, the new system has better performance and efficiency. It is proved that the new CP-ABE system can also resist collision attack and chosen-plaintext attack under the decisional bilinear Diffie-Hellman assumption.

III.EXISTING SYSTEM

- In the prevalent the cloud service supplier, and might share the information with users having specific authorizations (or attributes).
- In the prevalent system the quality ABE system doesn't support secure deduplication, that is critical for eliminating duplicate copies of identical information so as to avoid wasting cupboard space and network information measure.

DISADVANTAGES OF EXISTING SYSTEM

- System doesn't support secure de-duplication
- No deadline was define to access specific file
- Access policies while not revealing the underlying plaintext.
- Existing systems solely accomplish it by process a weaker security notion
- Not supported mobile devices

IV.PROPOSED SYSTEM

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

V. SYSTEM ARCHITECTURE

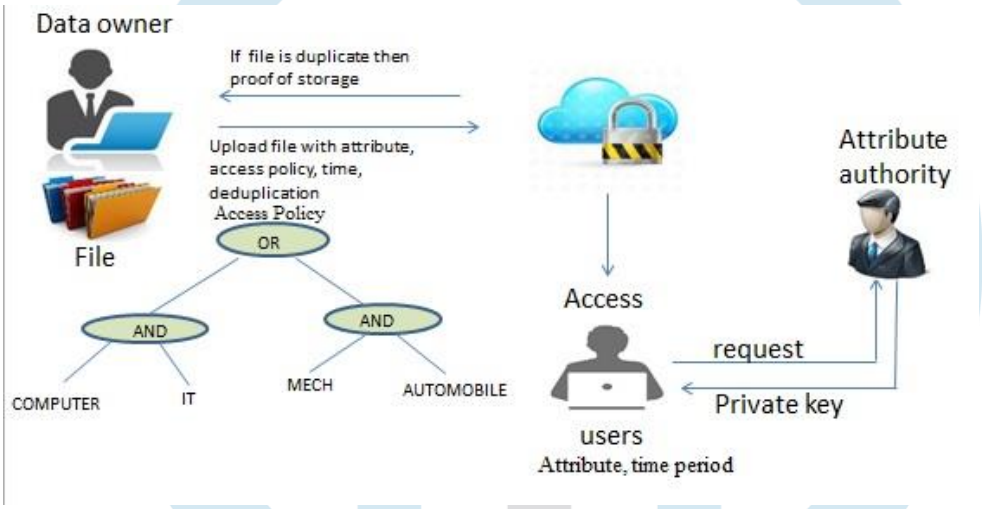

Figure : Architecture

ADVANTAGES OF PROPOSED SYSTEM

- We propose an approach supported 2 cryptanalytic primitives, as well as a zero-knowledge proof of knowledge and a guarantee theme, to achieve information consistency within the system.
- Time based mostly and access policy is given by original owner of file UN agency transfer the information.
- An attribute-based storage supporting system with secure De-duplication.
- System support high security and efficiency, as well as system additionally uploads the file by specifying time period and access policy.

VI.APPLICATIONS

- Encryption Decryption System
- Enterprise or any organization can use this application for securely share data within their network.
- Cloud provider can also this system to avoid data leakage.

VII. CONCLUSION AND FUTURE SCOPE

In our system owner transfer the file with the attributes and access policy, accessing time, then transfer file check for weather file is duplicate or not. once this if file is duplicate then owner of the get proof of ownership and if file is original then store on cloud and once user request for file attribute authority can check the attributes of user then exclusively user can get key to access the file from cloud.

FUTURE SCOPE

In the future, the system can be integrated to specific network applications. A social network mobile application can be developed that can in real-time find and make friends in the near vicinity. A corporate app for business purposes can be developed too.

REFERENCES

[1]E. De Cristofaro and G. Tsudik; Practical private set intersection protocols with linear complexity in Proc. 14th Int. Conf. Financial Cryptography Data Security, 2010.

[2] W. Dong, V. Dave, L. Qiu, and Y. Zhang; Secure friend discovery inmobile social networks in Proc. IEEE INFOCOM, 2011.

[3]M. Chase; Multi-authority attribute based encryption in Proc. 4th Conf.
Theory Cryptography.

[4] M. J. Freedman, K. Nissim, and B. Pinkas; E_cient private matching and set intersection in Proc. Int. Conf. Theory Appl. CryptographicTech

[5]V. Goyal, O. Pandey, A. Sahai, and B. Waters; Attribute-based encryption for fine-grained access control of encrypted data in Proc. 13th ACM Conf. Comput. Commun. Security, 2006

[6]Lan Zhang, Member, IEEE, Xiang-Yang Li, Senior Member, IEEE, Kebin Liu, Member, IEEE, Taeho Jung, Student Member, IEEE, and Yun-hao Liu, Senior Member, IEEE; Message in a Sealed Bottle: Privacy Preserving Friending in Mobile Social Networks in IEEE transactions on mobile computing, VOL. 14, NO. 9, SEPTEMBER 2015.

[7] http://t.qq.com/, 2013

[8] http://magnetu.com, 2013

[9] 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.