Attribute and Time Based Encrypted Data Access over Cloud

Kokate Yogesh K[1] Somwanshi Rahul P.[2] Amale Rohit R.[3] Jejurkar Navnath S.[4] Prof. Shaikh I.R.[5]
[1,2,3,4,5]SND COE & RC,Yeola, Maharashtra, India

Abstract— Data access management is an efficient way to make sure the knowledge security within the cloud. However, thanks to knowledge outsourcing and untrusted cloud servers, the information access management becomes a difficult issue in cloud storage systems. Existing access management schemes aren't any longer applicable to cloud storage systems, as a result of they either turn out multiple encrypted copies of constant knowledge or need a totally trusty cloud server. Ciphertext-Policy Attribute-based cryptography (CP-ABE) may be a promising technique for access management of encrypted knowledge. It needs a trusty authority manages all the attributes and distributes keys within the system. To guard knowledge confidentially against the honest-but-curious cloud service supplier, varied works are projected to support fine-grained knowledge access management. However, till now, no schemes will support each ne-grained access management and time-sensitive knowledge business enterprise. During this paper, by embedding timed-release cryptography into CP-ABE (Ciphertext-Policy Attribute-based Encryption), we tend to propose a replacement time and attribute factors combined access management on time-sensitive knowledge for public cloud storage.

Key words: Time Sensative Data, Access Control, Cloud Storage, Fine Granularity, CP-ABE, TRE

I. INTRODUCTION

Cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet.

The cloud computing benefits individual users and enterprises with convenient access, increased operational ciencies and rich storage resources by combining a set of existing and new techniques from research areas such as service-oriented architectures and virtulization. Although the great benefits brought by cloud computing are exciting for users, security problems may somehow impede its quick development .Currently, more and more users would outsource their data to cloud service provider (CSP) for sharing. However, the CSP which deprives data owners direct control over their data is assumed to be honest-but-curious, that may prompt security concerns. These security matters existing in public cloud motivate the requirement to appropriately keep data confdential. Several schemes exploiting cryptographic mechanisms to settle the secu- rity problems have been proposed. In order to guarantee secure data group sharing, identity-based broadcast encryption (IBBE) scheme [11] is employed in public cloud. The data owners could broadcast their encrypted data to a group of receivers at one time and the public key of the user can be regarded as email, unique id and user- name Hence, by using an identity, data owner can share data with other group users in a convenient and secure manner. Attribute-based encryption (ABE) is one of new cryptographic mechanisms used in cloud to reach flexible and fine-grained secure data group sharing. Especially, ciphertext-policy ABE (CP-ABE) allows data owners to encrypt data with an access policy such that only users whose attributes satisfy the access policy can decrypt the data [12]. Time-sensitive data such as a business plan and a tender, is a special data in cloud which requires time-based exposing [2] It means that data owner may want different users to disseminate data after different time. For instance, data owner may share sensitive business plan with directors, and he hopes these directors only can dissemi-nate business plan to managers at an early time and then to other employees at last.

II. LITERATURE SURVEY

A. Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud

Author: Qinlong Huang, Yixiang Yang and Jingyi Fu.
Publication: IEEE Transactions on Services Computing, 1-1, 2017.
Description: IBBE technique is used to achieve secure data group sharing in public cloud, which allows data owner to outsource encrypted data to semi-trusted cloud and share it with a group of receivers at one time. It is more convenient that email and username could be used as public keys for users. Access policy is designed for embedding releasing time and take the advantages of attribute-based CPRE, to achieve fine-grained and timed-release data group dissemination. The CSP can re-encrypt initial ciphertexts for data disseminator after the designate time if his attributes associated with the re-encryption key satisfy the access policy in the ciphertexts [1].

B. TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud

Author: Hong J., Xue K., Xue Y., Chen W., Wei D. S. L., Yu N., and Hong P.
Publication: IEEE Transactions on Services Computing, 1-1, 2017.
Description: By integrating TRE and CP-ABE in public cloud storage, an effcient scheme to realize secure negrained access control for time-sensitive data. In the proposed scheme, the data owner can autonomously designate intended users and their relevant access privilege releasing time points. Besides realizing the function, it is proved that the negligible burden is upon owners, users and the trusted CA. It is presented how to design access structure for any potential timed release access policy, especially embedding multiple releasing time points for di erent intended users. Timed-Release Encryption (TRE) becomes a promising primitive, in which, a trusted time agent, instead of data owners, uniformly executes the timedrelease function.

C. RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage

Author: Xue K., Xue Y., Hong J., Li, W., Yue, H., Wei, D. S. L., and Hong, P.
Publication: IEEE Transactions on Information Forensics and Security, 12(4), 953967, 2017.

Description: To address the single-point performance bottleneck of key distribution existed in the existing schemes, here propose a robust and efficient heterogeneous framework with single CA (Central Authority) and mu tiple AAs (Attribute Authorities) for public cloud storage. The heavy load of user legitimacy verification is shared by multiple AAs, each of which man- ages the universal attribute set and is able to independently complete the user legitimacy verification, while CA is only responsible for computational tasks. This is the first work that proposes the heterogeneous access control framework to address the low efficiency and single-point performance bot- tleneck for cloud storage. It is reconstructed the CP-ABE scheme to fit our proposed framework and propose a robust and high-efficient access control scheme, meanwhile the scheme still preserves the fine granularity, flexibility and security features of CP-ABE.

III. PROPOSED FRAMEWORK

We propose an efficient time and attribute factors combined access control scheme, named TAFC, for time-sensitive data in public cloud. Our scheme possesses two important capabilities: 1) It inherits the property of ne granularity from CP-ABE; 2) By introducing the trapdoor mechanism, it further retains the feature of timed release from TRE. Note that in TAFC, the introduced trapdoor mechanism is only related to the time factor, and only one corresponding secret needs to be published when expos- ing the related trapdoors. This makes our scheme highly efficient, which only brings about little overhead to the original CP-ABE based scheme. We should address how to design an efficient access structure for arbitrary access privilege construction with both time and attribute factors, especially when an access policy embeds multiple access privilege releasing time points. As an extension of the previous conference version, we give the potential sub-policies for time-sensitive data, and then present an efficient and practical method to construct relevant access structures.

IV. MATHEMATICAL MODEL

Mathematical modeling is the art of translating problems from an application area into tractable mathematical formulations whose theoretical and numerical analysis provides insight, answers, and guidance useful for the originating application.

$$S = (U, AS, SS, O)$$

Here S stands for System, here we are developing an system for stregthen the authentication system.

Where,

U = Set of Users who attempts to access the system

$$U = \sum_{n-1} U = u1; u2; u3; :::::; un:$$

ex. End users

SS = Set of Security Checks

$$SS = \sum_{n-1}^{4} I = Q1;Q2;Q3;Q4:$$

where,

Q1= Check Username

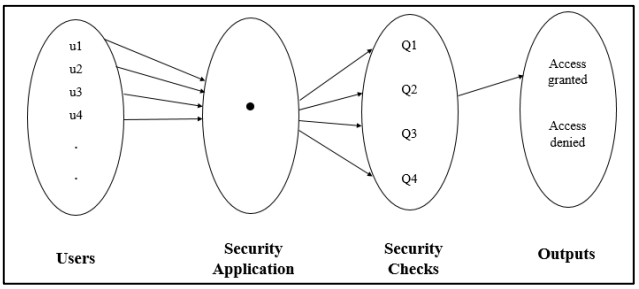
Q2= Check user password + salt

Q3= Check CAPTCHA

Q4= Check key stroke

O = Set of Outputs

$$O = \sum_{n-1}^{2} U = Accessgranted; Accessdenied:$$



V. RESULTS

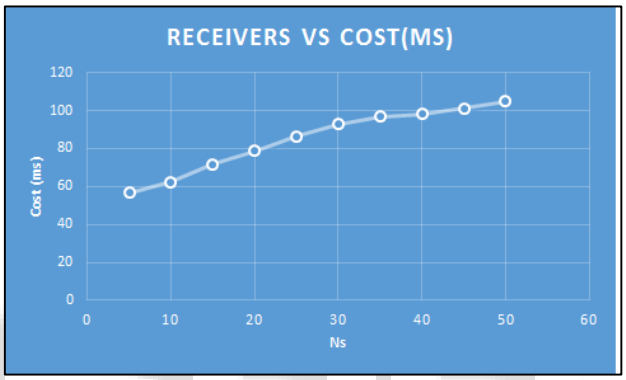


Fig. 1: Receivers vs Cost in Encryption

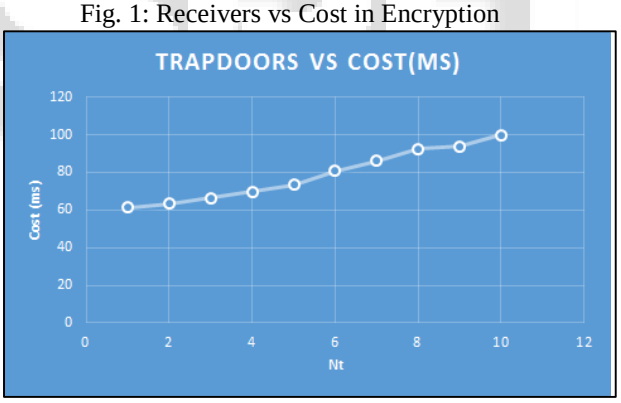


Fig. 2: Trapdoors vs Cost in Encryption

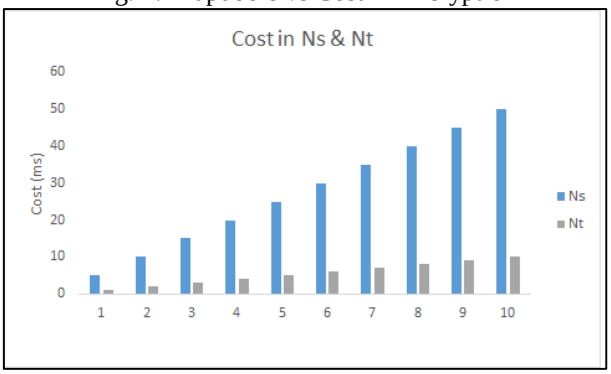


Fig. 3: Cost for Ns & Nt in Encrption

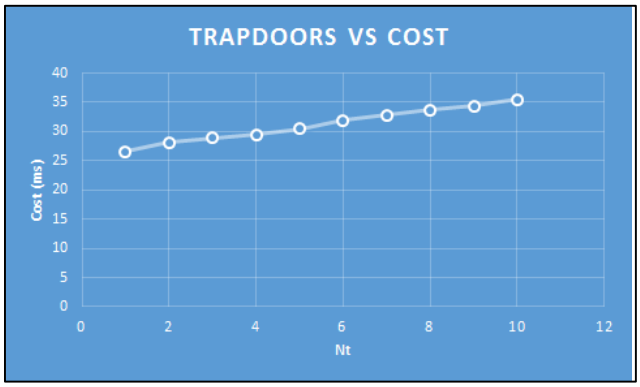


Fig. 4: Trapdoors vs Cost in ReEncryption

VI. CONCLUSION

We implemented a secure data sharing and dissemination scheme in public cloud based on attribute-based and timed-release with CP-ABE. Our approach is very helpfull for sharing the time-sensitive data for public cloud. We had propses a scheme which incorporates the concept of timed-release encryption to the architecture of ciphertext policy attribute-based encryption. With this approach data owners capable to flexibly re- lease the access privilege to different users at different time, according to a well-defined access policy over attributes and release time.

REFERENCES

[1] Huang Q., Yang Y., and Fu J. Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud. IEEE Transactions on Services Computing, 11, 2018
[2] Hong J., Xue K., Xue Y., Chen W., Wei D. S. L., Yu N., and Hong P. TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud. IEEE Transactions on Services Computing, 1-1, 2017
[3] Xue K., Xue Y., Hong J., Li, W., Yue, H., Wei, D. S. L., and Hong, P. RAAC: Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage. IEEE Transactions on Information Forensics and Security, 12(4), 953967, 2017.
[4] F. Armknecht, J.-M. Bohli, G. O. Karame, and F. Youssef, Transparent data deduplication in the cloud, in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 886900, ACM, 2015.
[5] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, DACMACS: Effective data access control for multi-authority cloud storage systems, IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 17901801, 2013.
[6] Q. Liu, G. Wang, and J. Wu, Time-based proxy reencryption scheme for secure data sharing in a cloud environment, Information Sciences, vol. 258, no. 3, pp. 355370, 2014.
[7] H. Wang, Identity-based distributed provable data possession in multicloud storage, IEEE Transactions on Services Computing, vol. 8, no. 2, pp. 328340, 2015.
[8] Z. Zhou, H. Zhang, Q. Zhang, Y. Xu, and P. Li, Privacy-preserving granular data retrieval indexes for outsourced cloud data, in Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM 14), pp. 601606, IEEE, 2014.
[9] R. Rivest, A. Shamir, and D. Wagner, Time Lock Puzzles and Timed-release Crypto, Mas-sachusetts Institute of Technology, MA, USA, 1996.
[10] K. Ren, C. Wang, and Q. Wang, Security Challenges for the Public Cloud, IEEE Internet Com-puting, vol. 16, no. 1, pp. 69-73, 2012.
[11] C. Delerable, Identity-based Broadcast Encryption with Constant Size Ciphertexts and Private Keys, Proc. the 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007), pp. 200-215, 2007.
[12] Z. Wan, J. Liu, and R. Deng, HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Computing, IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754, 2012

