Time and Attribute Factor Combined Access Control for Time Sensitive Data in Public Cloud

E.Arshitha[1], G.Keerthi[2], Dr R. Ch.A.Naidu[3]
[12]Department of IT, [3]Department of CSE
[123]SMEC

Abstract- The new paradigm of outsourcing data to the cloud is a double-edged sword. On the one hand, it frees data owners from the technical management, and is easier for data owners to share their data with intended users. On the other hand, it poses new challenges on privacy and security protection. To protect data confidentiality against the honest-but-curious cloud service provider, numerous works have been proposed to support fine-grained data access control. However, till now, no schemes can support both fine-grained access control and time-sensitive data publishing. In this paper, by embedding timed-release encryption into CP-ABE (Ciphertext-Policy Attribute-based Encryption), we propose a new time and attribute factors combined access control on time-sensitive data for public cloud storage (named TAFC).

Keywords- CP-ABE, Data Owner, Data User, Cloud Storage

I. INTRODUCTION

Cloud storage service has significant advantages on bothconvenient data sharing and cost reduction. Thus, moreand more enterprises and individuals outsource their data tothe cloud to be benefited from this service. As cloud service separates thedata from the cloud service client (individuals or entities),depriving their direct control over these data, the dataowner cannot trust the cloud server to conduct secure dataaccess control. Therefore, the secure access control problemhas become a challenging issue in public cloud storage.Ciphertext-policy attribute-based encryption (CP-ABE) is a useful cryptographic method for data access control in cloud storage. All these CP-ABE based schemes enabledata owners to realize fine-grained and flexible access controlon their own data. However, CP-ABE determines users' accessprivilege based only on their inherent attributes without anyother critical factors, such as the time factor. In reality, thetime factor usually plays an important role in dealing with time-sensitive data . Inthese scenarios, both the mechanism of access privilege timedreleasing and fine-grained access control should be togethertaken into account . However, to our best knowledge, these schemes cannotsupport gradual access privilege releasing. A trivial solution is to let data ownersmanually release the time-sensitive data. However, this solutionforces the owner to repeatedly upload the different encryptionversions of the same data, which puts unnecessary and heavyburden on the data owner. proposed this first practical TRE algorithm, which has been subsequently introduced into different scenarios.

II. LITERATURE SURVEY

Transparent Data Deduplication in the Cloud) Authors(FrederikArmknecht, Jens-Matthias Bohli, Ghassan O. Karame, Franck Youssefauthors propose a novel storage solution, ClearBox, which allows a storage service provider to transparently attest to its customers the deduplication patterns of the (encrypted) data that it is storing. By doing so, ClearBox enables cloud users to verify the effective storage space that their data is occupying in the cloud, and consequently to check whether they qualify for benefits such as price reductions, etc.

Effective Data Access Control forMulti-Authority Cloud Storage Systems) Authors(Kan Yang, XiaohuaJia , KuiRenthe Authors proposed an effective data access controlscheme for multi-authority cloud storage systems, DACMACS.We also construct a new multi-authority CP-ABEscheme, in which the main computation of decryption is outsourcedto the server.

Time-based proxy re-encryption scheme for secure data sharing in a cloud environment Authors Q. Liu, G. Wang, and J. Wu,Time based Proxy Re-encryption scheme to achieve fine grained access control andscalable user revocation in a cloud environment. Thus, the data owner can be offline in the process of user revocations

III. OVER VIEW OF THE SYSTEM

Central Authority (CA):

The central authority (CA) is responsible to manage the security protection of the whole system:

Data owner (Owner):

The data owner (Owner) decides the access policy based on a specific attribute set and one or more releasing time points for each file, and then encrypts the file under the decided policy before uploading it.

Data Consumer (User):

The data consumer (User) is assigned a security key from CA. He/she can query any ciphertext stored in the cloud, but is able to decrypt it only if both of the following constraints are satisfied: 1) His/her attribute set satisfies the access policy; 2) The current access time is later than the specific releasing time.

Cloud service provider (Cloud):

Cloud service provider (Cloud) includes the administrator of the cloud and cloud servers. The cloud undertakes the storage task for other entities, and executes access privilege releasing algorithm under the control of CA.

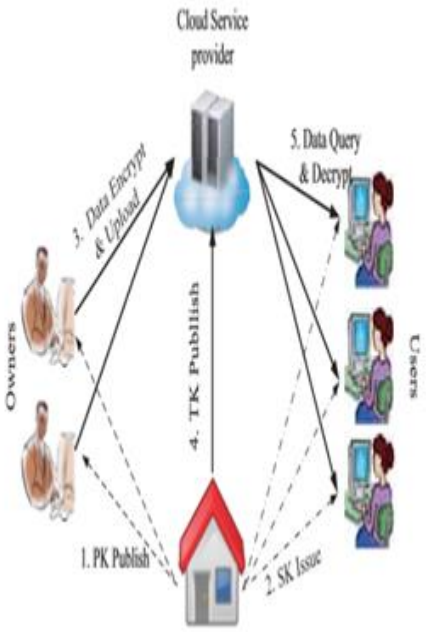

Fig-1: System Architecture

IV. METHODOLOGY

CP-ABE (Cipher text-Policy Attribute Based Encryption): Anciphertext-policy attribute based encryption scheme consists of four fundamental algorithms: **Setup, Encrypt, KeyGen, and Decrypt**.

Setup:

The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Encrypt(PK,M, A):

The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes.

Key Generation(MK,S):

The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

Decrypt(PK, CT, SK):

The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

V. RESULTS

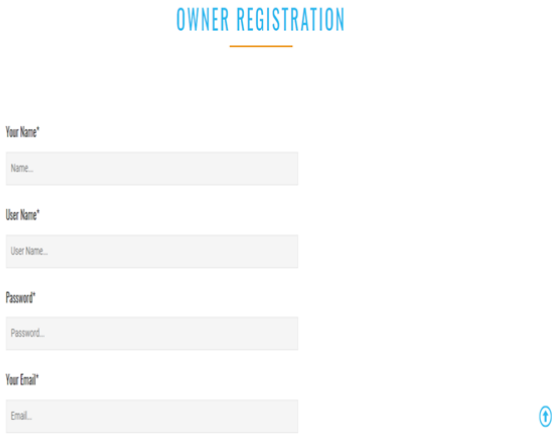

Fig.2: Data Owner Registration

Fig.3: Data Owner Login

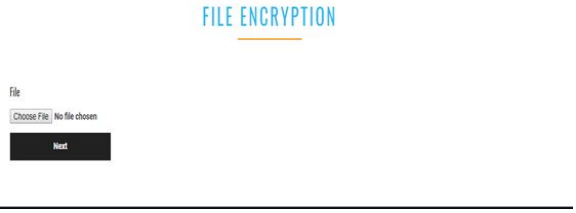

Fig.4: File Upload

Fig.5: File data

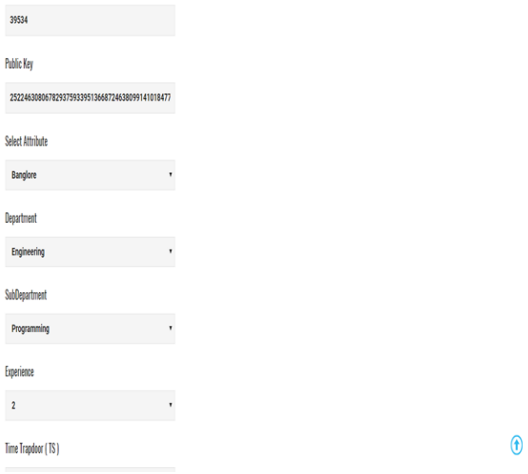

Fig.6: Key generation

Fig.7: file Decryption

VI. CONCLUSION

This paper aims at fine-grained access control for timesensitive data in cloud storage. One challenge is to simultaneously achieve both flexible timed release and fine granularitywith lightweight overhead, which was not explored in existingworks. In this paper, we proposed a scheme to achieve thisgoal. Our scheme seamlessly incorporates the concept oftimed-release encryption to the architecture of ciphertextpolicy attribute-based encryption. With a suit of proposedmechanisms, this scheme provides data owners with the capability to flexibly release the access privilege to different usersat different time, according to a well-defined access policyover attributes and release time. We further studied accesspolicy design for all potential access requirements of timesensitive, through suitable placement of time trapdoors. Theanalysis shows that our scheme can preserve the confidentialityof time-sensitive data, with a lightweight overhead on both CAand data owners. It thus well suits the practical large-scaleaccess control system for cloud storage.

VII. REFERENCES

[1]. Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A surveyof proxy re-encryption for secure data sharing in cloudcomputing," IEEE Transactions on Services Computing,Avaliable online, 2016.

[2]. F. Armknecht, J.-M.Bohli, G. O. Karame, and F. Youssef, "Transparent data deduplication in the cloud," inProceedings of the 22nd ACM SIGSAC Conference onComputer and Communications Security, pp. 886–900,ACM, 2015.

[3]. R. Masood, M. A. Shibli, Y. Ghazi, A. Kanwal, andA. Ali, "Cloud authorization: exploring techniques andapproach towards effective access control framework,"Frontiers of Computer Science, vol. 9, no. 2, pp. 297–321, 2015.

[4]. K. Ren, C. Wang, and Q. Wang, "Security challengesfor the public cloud," IEEE Internet Computing, vol. 16,no. 1, pp. 69–73, 2012.

[5]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicy attribute-based encryption," in Proceedings of the28th IEEE Symposium on Security and Privacy (S&P'07), pp. 321–334, IEEE, 2007.

[6]. Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchicalattribute-based solution for flexible and scalable accesscontrol in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754,2012.

[7]. K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DACMACS: Effective data access control for multi-authoritycloud storage systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1790–1801, 2013.