A Survey On Time And Attribute Factors Combined Access Control for Time-Sensitive Data in Public

[1]Dhanya K, [2]Prof. Preethi .S

[1]Mtech Student, [2]Associate Professor
[1]Department of Computer Science and Engineering
[2]Department of Information Science and Engineering

***Abstract*: This paper review on security of data stored in public cloud. This can be achieved by using encryption and decryption mechanism. The data owner can store the encrypted data within the cloud. Then the owner can issue the decryption keys to the authorized users. Based on this scheme data owners can easily share the data to intended users. Extensive number of users are trying to access data stored in the cloud simultaneously, it leads to new challenges mainly on confidentiality and integrity of data stored in cloud. This paper mainly addresses these issues and implement strategies for solving this, by combining CP-ABE (Cipher text-Policy Attribute Based Encryption) and TRE (Timed Released Encryption) commonly known as Time and Attribute Factors Combined Access control for Time Sensitive data in Public Cloud (TAFC).**

Keywords: Time sensitive data, Access control, Cloud storage, Fine granularity, CP-ABE, TRE

I. INTRODUCTION

Cloud computing is a technical and social reality and an emerging technology. Scientific and engineering applications, data mining, computational financing, gaming, and social networking as well as many other computational and data intensive activities can benefit from cloud computing. A broad range of data can be stored in cloud.Informations and applications in the cloud can be maintained by using internet and central remote servers. The main advantage of cloud computing is outsourcing of data to the cloud. As a result users can free from burden of data storage and its related maintenance. But it leads to another sophisticated issue such as integrity and confidentiality of data stored in the cloud.

We use different strategies to provide security on data stored in cloud. To achieve this, we provide overall control to data owners instead of these untrusted cloud service provider. Data stored in the cloud can be protected by using an effective method like information access mechanism. But the present server oriented access control methods are not beneficial for prolonged period of time frame. Nowadays many users can get access to data simultaneously. Different users can access the same data on different time period.so the data owner always stay online for giving variety encryption of same data. This leads more burden to data owner. And additionally, it leads to take extra storage for preserving these different keys, due to more than copies of cipher text for every information. To solve these problem by combining "CP-ABE and TRE" mechanism in public cloud. So different users can get different releasing time points.

II. TAFC ARCHITECTURE

This ensures the security of data stored in the cloud by combining two factors such as time and attributes. This method ensures the efficient access control for time sensitive data in public cloud, known as TAFC.It can be achieved by a) CP-ABE mechanism is used for inheriting fine granularity property b) Trap door mechanism known as TRE. [6]

Below figure fig1 shows the architecture of TAFC.It mainly contain Cloud service provider, a central authority, many information owners (owners) and several data consumers (users).

Cloud Service Provider: is a third party that offers infrastructure, cloud platform, storage and different application for requested users or organizations. It store large amount of data from users and provide data to users based on their demand. .

The central authority: is handling the overall protection of data in the cloud. It publishes the private key and secret key of each data based on its predefined time period.

The data owner: takes the decision based on access policy, that mainly focusing its attribute and time factor.After that it encrypt the data

The data consumer: also known as a user, assigned a private key from its central authority [1]. Any cipher text that stored in the cloud can be queried by this user, but the decryption is possible by satisfying the following terms. a) Attribute sets of the user must satisfies the access policy of central authority b) The present retrieval time is later than its corresponding deliver time.

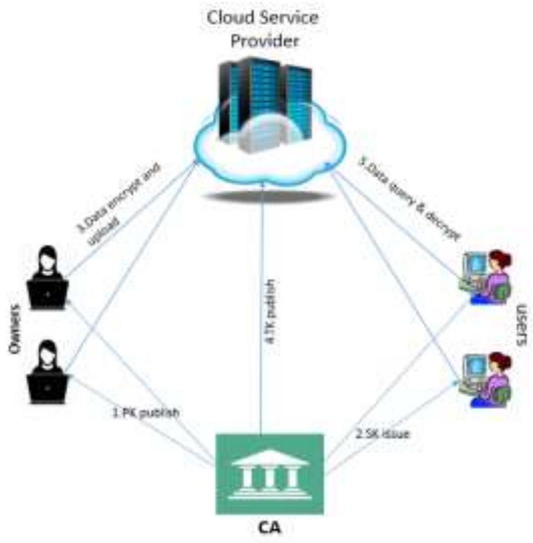

Fig.1 TAFC Architecture

.

A. Cipher text policy Attribute Based Encryption

This encryption technique consists of three entities: The central authority, user and information owner. The keys are issued by the central authority for the intended users. Then intended user can get data from the owner based on the access policy. Attribute and logic gate groups can be expressed as a tree that represents access policy in CP-ABE mechanism [9]. Attributes of each user can define the secret key generated from authority. Based on this scheme the cloud server has no responsibility related with this encryption and decryption .This scheme uses four algorithm to achieve its goal,that are a)Setup b)Key generation c)Encryption d)Decryption

B. Timed Release Encryption

This encryption mainly provide security to someone who wants to send a message to another one at later time or future. That means encrypted message cannot be decrypted by the intended user after a future time. For this purpose we required a trusted time agent [3] to manage the clock of the system. The time agent release a time token for each time point. The cipher text can be generated along with a particular releasing time and the public key of intended user.

Below Table shows the comparative study of TAFC

Sno	Research Paper	Focus	Limitations
1	K.Yang,X.Jia,K.Ren, B.Zhang and R.Xie, "DAC-MACS: Effective data access control for multi authority cloud storage systems, "IEEE transactions on information Forensics & Security, vol. 7,2012	A new multiauthority CP-ABE scheme with efficient decryption & attribute revocation method that achieve both forward security and backward security (DAC-MACS).	Trusted authority only to manage all the attribute in the system and issues secret keys to users. Since the authority can decrypt all the encrypted data, it becomes a vulnerable security point in the system
2	Baishuang Hu, Qin Liu,Xuhui Liu,Tao Peng,Guojun Wang& Jie wu, "DABKS:Dynamic attribute based Keyword search in cloud computing",IEEE communication and information systems security symposium,2017	This paper proposes a dynamic attribute-based keyword search that incorporates proxy re-encryption and a secret sharing scheme into Attribute based keyword search	Data owner to delegate policy updating operations to the cloud that reduces its security.
3	Ming Li,Shucheng Yu,Yao Zheng,Kui Ren,Wenjing Lou, "Scalable and secure sharing of personal heath records in cloud computing using attribute based encryption,"IEEE transactions on parallel and distributed systems	This paper proposes a patient centric frame work for data access control to personal health records stored in semi trusted servers.	Data owner (patient) will generate keys, as a result it is a burden to him/her.

	, vol 24, 2013		
4	Quin Liu,Guojun Wang,& Jie wu,"Clock based proxy Re-encryption scheme in unreliable cloud,"IEEE 41st international conference on parallel processing workshops,2012	This paper mainly focus on cipher text policy attribute based encryption and proxy re-encryption, allows the data owner and the cloud to share a secret key in advance, with which the cloud can be delegated to re-encrypt data on behalf of the data owner	The challenge here is the time lag between when the data owner issues the ticket and when a user's request reaches the CSP.This time lag may be unknown since the user may delay sending his update to the cloud
5	Elli Androulaki,Claudio Soriente,Luka malisa & Srdjan Capkun, "Enforcing location and time based access control on cloud stored data,IEEE 34th international conference on Distributed computing systems,2014	This framework integrates the operation of a cloud provider and a localization infrastructure to enforce location and time based access control to cloud stored data.	If the localization mechanism does not detect,e.g.: relay attacks, malicious users could exploit such weakness to bypass the contextual policy
6	Kan Yang, he Liu,Xiaohua jia, "Time domain attribute based access control for cloud based video content sharing: A cryptographic approach,IEEE transaction on Multimedia, vol 18,2016	This frame work mainly focus on how to securely share video contents to a certain group of people during a particular time period in cloud based multimedia systems using Time domain attribute based access control	This scheme provide security for in generic bilinear group model and random oracle model. It does not provide access control on video contents generated in previous time slots

CONCLUSION

This paper mainly focus on secure storage of data in public cloud. And also it provide facility for grain grained access control of time sensitive data. To achieve this by integrating CP-ABE [9] and TRE [10] mechanism. Based on this scheme the data owners can decide which user able to access data and provide relevant access privilege releasing time points according to a well-defined access policy over attribute and releasing time. And also it provide a light weight overhead on both central authority and data owners. This mechanism is highly applicable for large scale access control system for cloud storage.

REFERENCES

[1] K.Yang, X.Jia, K.Ren, B.Zhang and R.Xie,"DAC-MACS: Effective data access control for multi authority cloud storage systems,"IEEE transactions on information Forensics & Security, vol. 7, 2012

[2] Ming Li,Shucheng Yu,Yao Zheng,Kui Ren,Wenjing Lou, "Scalable and secure sharing of personal heath records in cloud computing using attribute based encryption,"IEEE transactions on parallel and distributed systems, vol 24, 2013

[3] Elli Androulaki,Claudio Soriente,Luka malisa & Srdjan Capkun, "Enforcing location and time based access control on cloud stored data,IEEE 34th international conference on Distributed computing systems,2014.

[4] Baishuang Hu, Qin Liu,Xuhui Liu,Tao Peng,Guojun Wang & Jie wu, "DABKS:Dynamic attribute based Keyword search in cloud computing",IEEE communication and information systems security symposium,2017

[5] Quin Liu, Guojun Wang, & Jie wu,"Clock based proxy Re-encryption scheme in unreliable cloud,"IEEE 41st international conference on parallel processing workshops, 2012

[6] Kan Yang, he Liu, Xiao Hua jia, "Time domain attribute based access control for cloud based video content sharing: A cryptographic approach, IEEE transaction on Multimedia, vol 18, 2016.

[7] Kui Ren, Cong Wang & Quian Wang, "Security Challenges for the Public Cloud, IEEE Computer Society, Jan 2012

[8] Cong Wang, Quian Wang & Kui Ren, "Privacy preserving public auditing for data Storage Security in cloud Computing",IEEE communication society,2010.

[9] J. Bethencourt,A Sahai andb.Waters "cipher text Policy Attribute based encryption," In proceeding of the 28th IEEE symposium on security and privacy,IEEE 2007.

[10] R.L Rivest, A.Shamir and D.a Wagner,"Time lock puzzles and timed release Crypto,"Massachusets Institute of Technology, 1996