Survey on Ciphertext Policy Attribute-based Encryption (CP-ABE) for Sharing Hierarchical Files

P. Saranya[1] P. S. Smitha[2]
[1]PG Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Velammal Engineering College, Surapet, India

Abstract— Ciphertext Policy Attribute-Based Encryption (CP-ABE) provides access control in owner's hand in which the secret key of a user and the ciphertext are dependent upon attributes. The encryptor can fix the policy, which user can decrypt the encrypted message. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. In order to explore the hierarchy structure of shared files an Efficient File Hierarchy Attribute-Based Encryption scheme (FH-CP-ABE) is proposed. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated access structure. When two hierarchy files are shared, the performance of FH-CP-ABE scheme is better than CP-ABE's in terms of encryption and decryption's time cost, and CT's storage cost.

Key words: Ciphertext-Policy Attribute-Based Encryption (CP-ABE), FH-CP-ABE, Multilevel Hierarchy, Single Access Structure

I. INTRODUCTION

In cloud computing, to protect data from leaking, users need to encrypt their data before being shared [3]. Cloud Service Provider (CSP) is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated ciphertext to CSP. User downloads and decrypts the interested ciphertext from CSP. Attribute-Based Encryption (ABE) follows one-to-many encryption [12], allowing users to encrypt and decrypt data based on user attributes. Ciphertext-policy Attribute-Based Encryption (CP-ABE) is used to solve the challenging problem of secure data sharing in cloud computing [1]. The shared files usually have hierarchical structure. A group of files are divided into a number of hierarchy subgroups located at different access levels. FH-CP-ABE scheme helps to efficiently share the hierarchical files.

Hierarchical Attribute-Based Encryption (HABE) model [7], combines the hierarchical generation of keys in the Hierarchical Identity Based Encryption (HIBE) system and flexible access control in the CP-ABE system for sharing data in the cloud. The length of ciphertext and private keys, as well as the time during encryption and decryption, grows linearly with the depth of a recipient in the hierarchy. E.g. Personal Health Record (PHR).

PHR allows patients to manage their own medical records. PHR data should be encrypted so that it is scalable with the number of users having access. Since there are multiple owners (patients) in a PHR system and every owner would encrypts PHR files using a different set of cryptographic keys. A unified security framework for patient centric sharing of PHR in a multi-domain, multi authority PHR system with many users is provided.

II. LITERATURE SURVEY

File Hierarchy Ciphertext Policy-Attribute Based Encryption (FH-CP-ABE) [9], is based on layered access structure with hierarchical structure of access policy. The layered model of access structure is used to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure. The hierarchical files are encrypted with an integrated access structure and the ciphertext components related to attributes could be shared by the files. The three types of access structures used in existing CP-ABE schemes, AND gate, access tree, and Linear Secret Sharing Scheme (LSSS). The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files.

The CP-ABE scheme offers two types of systems; (i) Single Authority CP-ABE which is managed by sole authority, (ii) Multi-Authority CP-ABE [8], which is managed by totally different authorities. System Model for data access control in multi-authority cloud storage is considered with five types of entities in the system.

1) A certificate authority (CA)
2) Attribute authorities (AAs)
3) Data owners or vendors (owners)
4) Cloud server (server)
5) Data consumers (users)

CA sets up the system and accepts the registration of all the users and AAs [2], for every legal user within the system. Each attribute is related to a multiple AA, every AA will manage Associate in number of attributes. AA has full management over the structure. Multi Authority CP-ABE also provides backward and forward security. The revoked user cannot rewrite any new cipher text that requires the revoked attribute to rewrite (backward security). The freshly joined user may rewrite the previously printed ciphertexts, if it's comfortable attributes (Forward Security).

Hybrid Attribute-Based Encryption (HABE) technique [10] combines Ciphertext-Policy Attribute-Based Encryption with Location-Based Encryption (LBE). LBE can efficiently handle dynamic attributes with continuous values, such as location. In order to decrypt, both the CP-ABE policy (static attributes) and LBE constraints (dynamic attribute) have to be satisfied. We combine an offline key generation for static attributes with a lightweight online key generation for dynamic attributes. The targeted recipient's geographic location is combined with the session key to produce a location-locked key that is sent along with the encrypted message. This process is called location verification, it uses GPS receiver inside the recipient's mobile device.

To protect the Personal Health Records (PHR) stored in semi-trusted servers, Attribute-Based Encryption (ABE) is adopted as a main encryption primitive [11]. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. When an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR.

III. METHODOLOGY

The File Hierarchy Ciphertext Policy-Attribute Based Encryption scheme has the following methods to share the layered access of hierarchical files,

- Revocable ABE
- Break glass access
- Location Based Encryption
- Data Retrieval for Disruption Tolerant Network

A. *Revocable ABE*

It is challenging problem to revoke user/attributes efficiently in ABE. A simple but constrained solution is to include a time attribute. This solution would require each message to be encrypted with a modified access tree, which is constructed by augmenting the original access tree with an additional time attribute. The time attribute, represents the current 'time period' [6]. There are significant trade-offs between the extra load incurred by the authority for generating and communicating the new keys to the users and the amount of time that can elapse before a revoked user can be effectively purged.

This above solution has the following problems:

- Each user *X* needs to periodically receive from the central authority the fresh private key corresponding to the time attribute, otherwise *X* will not be able to decrypt any message.
- It is a lazy revocation technique; the revoked user is not purged from the system until the current time period expires.
- This scheme requires implicit time synchronization among the authority and the users.

To address these issues, we present a revocation scheme for revoking users using the non-monotonic access structure is to attach a negative constraint to the ciphertext's access policy which includes the IDs of the revoked users. A unified security framework for patient-centric sharing of PHRs in a multi-domain, multi-authority PHR system with many users is proposed. The application-level requirements of both public and personal use of a patient are PHRs, and distribute users' trust to multiple authorities that better reflects reality. Patients can choose and enforce their own access policy for each PHR file, and can revoke a user without involving high overhead.

B. *Break Glass Access*

When an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department (ED). To prevent from abuse of break-glass option [11], the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

C. *Location Based Encryption*

Location-Based Encryption (LBE) can efficiently handle the dynamic attributes with continuous values, while CP-ABE handles the Static Attributes within an encryption policy. We combine an offline key generation for static attributes with a lightweight online key generation for dynamic attributes.

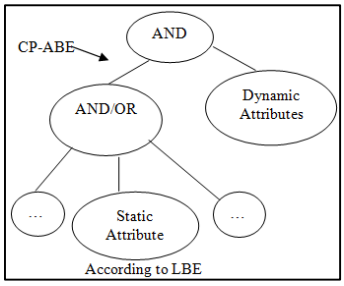

Fig. 1: Access Structure of LBE

The targeted recipient's geographic location is combined with the session key, in order to produce a location-locked key. This location-locked key is then sent along with the encrypted message. As a result the ciphertext can only be decrypted if the session key can be recovered from the location-locked key [10]. In turn, LBE requires that this decryption is only possible if the recipient's device is physically presented at location or, respectively, inside a geographic area associated with Location. This process is called location verification.

D. *Data Retrieval for Disruption Tolerant Network*

Disruption Tolerant Network (DTN) technologies are designed to enable nodes to communicate with one another in some challenging network scenarios which suffer from intermittent connectivity and frequent partitions e.g. battlefield and disaster recovery. This scheme provides a flexible fine-grained access control such that the encrypted contents can only be accessed by authorized users. Two unique features of the scheme provide are: (i) the incorporation of dynamic attributes whose value may change over time, and (ii) the revocation feature [4].

Two solutions to address the Disruption problem: The set of a user attributes does not necessarily belong to the set of the local authority's attributes. The static and dynamic attributes are the two access structure, one tree with the static attributes and another with the dynamic attributes connected by an 'AND' gate. To decrypt this ciphertext the receiver needs to have private keys for the leaf nodes of both of the access trees.

Techniques	Access Control	Efficiency	Flexibility	Scalability	Security
ABE	High	Low	High	High	Low
CP-ABE	High	High	Low	Low	Low

KP-ABE	High	Low	Low	Low	Low
IBE	Low	Low	Low	Low	High
HABE	High	Low	Low	High	Low
MA-ABE	High	High	High	High	Low

Table 1: Comparison of Encryption Schemes.

IV. CONCLUSION

We analyzed different Attribute-Based Encryption schemes: ABE, CP-ABE, ABE with non-monotonic access structure, HABE, FH-CP-ABE, TR-MABE; classified according to their access policy. Our proposed system FH-CP-ABE is intended to enhance the security of military networks and Personal Health Record (PHR) where data owner can achieve secure and self-centric access control over the PHR data. Main goal of this system is to provide security against decrypting every CT by single CA in MA-ABE system. The improvement in multi authority attribute encryption scheme is shown on removing the Central Authority. Also enables dynamic modification of access policies that supports efficient on-demand attribute revocation and break-glass access under emergency scenarios. Online/offline ABE scheme can be implemented to improve the speed of key generation and encryption.

REFERENCES

[1] J.Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute- Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.
[2] Bing Li, Dijiang Huang, Zhijie Wang, and Yan Zhu. "Attribute-based Access Control for ICN Naming scheme,"IEEE Transactions on Dependable and Secure Computing, 2015.
[3] Go Ohtake, Kazuto Ogawa and Reihaneh Safavi-Naini, "Privacy Preserving System for Integrated Broadcast-broadband Services using Attribute-Based Encryption," IEEE Transactions on Consumer Electronics, Vol. 61, No. 3, August 2015.
[4] Guojun Wang, Qin Liu, Jie Wu, Minyi Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Elsevier,2011.
[5] Jun Zhou, Zhenfu Cao, Xiaolei Dong, Xiaodong Lin, "TR-MABE: White-Box Traceable and Revocable Multi-authority Attribute-based Encryption and Its Applications to Multi-level Privacy-preserving e-Healthcare Cloud Computing Systems," IEEE Conference on Computer Communications, 2015.
[6] S. Roy, M. Chuah and Bethlehem, "Secure Data Retrieval Based on Ciphertext-Policy Attribute- Based Encryption (CP-ABE) System for the DTNs,"Proc. Milcom, 2006.
[7] Shashikant Govind Vaidya, Shailesh Kisan Hule, Gaurav Balvant Dagade, Sharad Arjun Jadhav. "HABE (Hierarchical Attribute Based Encryption) Model for Supporting dynamic structure of organization," Proc. of the Second International Conference on Advances in Computing, Control and Communication (CCN), 2009.
[8] Shivarathri Ravinder and B. Sarada, "Secure Multi Authority Cloud Storage Based on CP-ABE and Data Access Control," International Journal of Electronics Communication and Computer Engineering, Vol.6, Sept.2015.
[9] Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen, and Weixin Xie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud computing," IEEE Transactions on Information Forensics and Security, Vol.11,No.6,June 2016.
[10] Stefan G. Weber, "A Hybrid Attribute-Based Encryption Technique Supporting Expensive Policies and Dynamic Attributes," Information Security Journal: A Global Perspective, 21:297–305, 2012.
[11] M.Vanaja and T.Vijaya Madhavi, "Advanced Attribute-Based Encryption For secure and Scalable Sharing of Personal Health Record in Cloud Computing," Vol. 4, Issue Spl - 4, Oct - Dec 2013.
[12] William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition published by Prentice Hall, November 16, 2005.

