Hierarchical Attribute-Based Encryption: A Survey

V.S. Sajitha[1], V. Reena Catherine[2]

[1]M.Phil scholar, [2]Assistant Professor

Department of CS, Nanjil Catholic Collge of Arts and Science,

Kaliyakkavilai, Tamilnadu, India.

Abstract: Cloud computing, as a promising computing model, enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. However, allowing Cloud Service Providers (CSPs), which are not in the same trusted domains as enterprise users, to take care of confidential data, may raise potential security and privacy issues. To keep the sensitive user data confidential against entrusted CSPs, a usual way is to apply cryptographic approaches, by disclosing decryption keys only to authorized users. However, when enterprise users outsource confidential data for sharing on cloud servers, the adopted encryption system should not only support fine-grained access control, but also provide high performance, full delegation, and scalability, so as to best serve the needs of accessing data anytime and anywhere, delegating within enterprises, and achieving a dynamic set of users. In this paper, we propose a scheme to help enterprises to efficiently share confidential data on cloud servers. We achieve this goal by first combining the Hierarchical Identity- Based Encryption (HIBE) system and the ciphertext-policy Attribute-Based Encryption (CP-ABE) system.

Keywords

Cloud computing, hierarchical attribute-based encryption, fine-grained access control, scalability

I. INTRODUCTION

Cloud computing has rapidly become a widely adopted model for delivering services over the internet. Therefore cloud service provider must provide the trust and security, as there are large amount of important and sensitive data stored on the clouds. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms. With the emergence of sharing confidential corporate data

on cloud servers, it is essential to adopt an efficient encryption system with a fine-grained access control to encrypt outsourced data, X. Liu et al 2014. Ciphertext-Policy Attribute-Based Encryption (CP-ABE), as one of the most promising encryption systems in this field, allows the encryption of data by specifying an access control policy over attributes, so that only users with a set of attributes satisfying this policy can decrypt the corresponding data. However, a CP-ABE system may not work well when enterprise users outsource their data for sharing on cloud servers, due to the following reasons: First, one of the biggest merits of cloud computing is that users can access data stored in the cloud anytime and anywhere using any device, such as thin clients with limited bandwidth, CPU, and memory capabilities, Wang et al 2010. Therefore, the encryption system should provide high performance. Second, in the case of a large-scale industry, a delegation mechanism in the generation of keys inside an enterprise is needed. Although some CP-ABE schemes support delegation between users, which enables a user to generate attribute secret keys containing a subset of his/her own attribute secret keys for other users, we hope to achieve a full delegation, that is, a delegation mechanism between Attribute Authorities (AAs), which independently make decisions on the structure and semantics of their attributes. Third, in case of a large-scale industry with a high turn overrate, a scalable revocation mechanism is a must. The existing CP-ABE schemes usually demand users to heavily depend on AAs and maintain a large amount of secret keys storage, which lacks flexibility and scalability. Our main design goal is to help the enterprise users to efficiently share confidential data on cloud servers. Specially, we want to make our scheme more applicable in cloud computing by simultaneously achieving fine-grained access control, high performance, practicability, and scalability. In this paper, we first propose a Hierarchical Attribute-Based Encryption (HABE) model by combining a HIBE system and a CP-ABE system, to provide fine-grained access control and full delegation, Goyal et al 2006. Based on the HABE model, we construct a HABE scheme by making a performance-expressivity tradeoff, to achieve high performance. Finally, we propose a scalable revocation scheme by delegating to the CSP most of the computing tasks in revocation, to achieve a dynamic set of users efficiently.

II. LITERATURE SURVEY

Attribute-Based Encryption (ABE):

An attribute based encryption scheme was introduced by Sahai and Waters in 2005 and the goal is to provide security and access control Sahai et al 2007. Attribute-based encryption (ABE) is a public-key algorithm based one to many encryptions that allows users to encrypt and decrypt data based on user attributes. In their context, the role of the parties is taken by the attributes. Thus, the access structure will contain the authorized sets of attributes. They restrict the attention to monotone access structures. However, it is also possible to realize general access structures using the techniques by having the attribute as a separate attribute altogether. Thus, the number of attributes in the system will be doubled. From now on, unless stated otherwise, by an access structure we mean a monotone access structure.

Cipher Text Policy Attribute-Based Encryption

Another modified form of ABE called CP-ABE was introduced by Sahai. In a CP-ABE scheme, every ciphertext is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. CP-ABE works in the reverse way of Key Policy Attribute-Based Encryption (KP-ABE). The access structure built in the encrypted data can let the encrypted data choose which key can recover the data; it means the user's key with attributes just satisfies the access structure of the encrypted data. The concept of this scheme is similar to the traditional access control schemes. The encryptor specifies the threshold access structure for his/her interested attributes while encrypting a message. Based on this access structure, the message is then encrypted such that only those whose attributes satisfy the access structure can decrypt it.

Key Policy Attribute-Based Encryption (KP-ABE)

KP-ABE is the modified form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. To reflect the access tree structure, the secret key of the user is defined, Changji Wang et al 2013. Ciphertexts are labeled with sets of attributes and private keys are associated with monotonic access structures that control which ciphertexts a user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications

III. PROPOSED WORK

The Hierarchical Attribute-Based Encryption (HABE) is derived by Wang et al The HABE model consists of a Root Master (RM) that corresponds to the Third Trusted Party (TTP),Multiple Domain Masters (DMs) in which the top-level DMs correspond to multiple enterprise users, and numerous users that correspond to all personnel in an enterprise. This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. This scheme can satisfy the property of fine grained access control, scalability and full delegation. It can share data for users in the cloud in an enterprise environment. Furthermore, it can apply to achieve proxy re-encryption. But in practice, it is unsuitable to implement. Since all attributes in one conjunctive clause in this scheme may be administered by the same domain authority, the same attribute may be administered by multiple domain authorities.

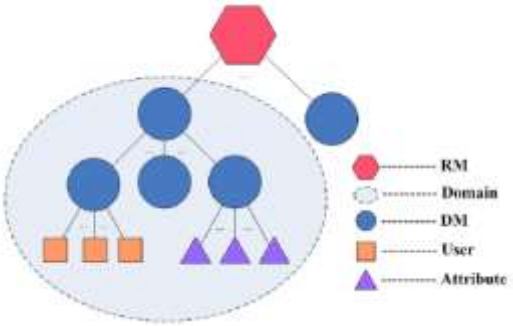
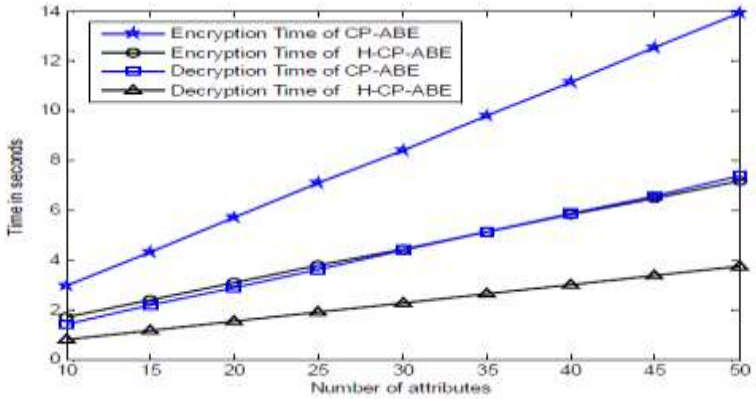


Figure : A three-level HABE Model

In HABE model, the RM's role closely follows the root private key generator (PKG) in a HIBE system, is responsible for the generation and distribution of system parameters and domain keys. The DM, whose role integrates both the properties of the domain PKG in a HIBE system and AA in a CP-ABE system.



It is responsible for delegating keys to DMs at the next level and distributing keys to users. Specifically, we enable the leftmost DM at the second level to administer all the users in a

domain, just as the personnel office administers all personnel in an enterprise, and not to administer any attribute. Also other DMs administer an arbitrary number of disjoint attributes, and have full control over the structure and semantics of their attributes. In the HABE model, we first mark each DM and attribute with a unique identifier (ID), but mark each user with both an ID and a set of descriptive attributes. Then,as Gentry et al 2002, we enable an entity's secret key to be extracted from the DM administering itself, and an entity's public key, which denotes its position in the HABE model, to be an ID tuple consisting of the public key of the DM administering itself and its ID.

CONCLUSION

In this paper, we construct a scheme, which has several qualities such as high performance, fine-grained access control, scalability and full delegation. Our HABE scheme, which is also collusion resistant, can be proven to be semantically secure against adaptive chosen plaintext attacks under the Bilinear Diffie-Hellman (BDH) assumption and the random oracle model.

REFERENCES

1. J. Bettencourt, A. Sahai, and B.Waters " Ciphertext-Policy Attribute Based Encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

2. Chase M., "Multi-Authority Attribute Based Encrypt-Ion," in Proceedings of the 4th Conference on Theory of Cryptography, Berlin, pp. 515-534, 2007.

3. X. Liu, J. Ma, J. Xiong, and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," International Journal of Network Security, vol. 16, no. 6, pp. 437–443, July 2014.

4. G. Wang, Q. Liu, and J.Wu," Hierachical attibute- based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security.

5. Changji Wang and Jianfa Luo," An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length", Hindawi Publishing Corporation Mathematical Problems in Engineering, Volume 2013, Article ID 810969, 7 pages.

Volume 2013, Article ID 810969, 7 pages 6. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98, October 2006.

7. C. Gentry and A. Silverberg. Hierarchical ID-Based Cryptography. In Proceedings of ASIACRYPT 2002, pages 548-566.