IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Measurement of Revocation –ID Encryption Process

[1]K.Ravikumar,[2] C.Banupriya
[1]Asst.professor, Dept.of.Computer science, Tamil University, Thanjavur-613010.
[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.

Abstract:

A user is able to decrypt a cipher text if and only if his attributes satisfy the cipher text access structure. Beside this basic property, matter-of-fact applications usually have other requirements. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise. Our basic scheme is proven to be selected plaintext secure under the decisional bilinear Hellman postulation. Process One of the most difficult issues in data sharing systems is the enforcement of access policies and the support of policies updates. Cipher text policy attribute-based encryption is becoming a promising cryptographic solution to this issue. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. However, the advantage comes with a major drawback which is known as a key escrow different side problem.

Keywords: ***Measurement, Crypto ,Services***

I. INTRODUCTION

People can share their lives with friends by uploading their private photos or messages into the online social networks such as Face book and My place or upload highly sensitive personal health records into online data servers such as Microsoft Health Vault, Google Health for ease of sharing with their primary doctors or for cost saving. One-to-many communication can be secured using one-to one public key cryptosystems in a straightforward manner. For example, a sender may encrypt data with a symmetric encryption key, and distribute this data key to every intended receiver using public key encryption. The can easily foresee that these security concerns and requirements would become more urgent in the coming era of cloud computing wherein individuals, organizations, and businesses may outsource their various types of data, including the highly sensitive data, into the cloud. Instead of addressing the issue in general settings, we particularly focus on practical application scenarios such as data sharing, which semi-trustable proxy servers are always available for providing various types of content services.

A sender must maintain a list of prospective receivers, as well as authorization information associated with each receiver. On each revocation event, the authority just generates several proxy re-encryption keys and transmits them to proxy servers. Proxy servers will update secret keys for all users but the one to be revoked.

Nevertheless, applying CP-ABE in the data sharing system has several challenges. In CP-ABE, the key generation centre (KGC) generates private keys of users by applying the KGC's master secret keys to users' associated set of attributes. Thus, the major benefit of this approach is to largely reduce the need for processing and storing public key certificates under traditional public key infrastructure (PKI). However, the advantage of the CP-ABE comes with a major drawback which is known as a key escrow problem. The KGC can decrypt every cipher text addressed to specific users by generating their attribute keys.

II. Scheme follows:

Sahai and Waters-rest introduced attribute based encryption for encrypted access control. In an ABE system, both the user secret key and the cipher text are associated with a set of attributes. Only if at least a threshold number of attributes overlap between the cipher text and his secret key, can the user decrypt the cipher text. Introduced the concept of CP-ABE based on. The idea of a CP-ABE scheme is as follows: the user secret key is associated with a set of attributes and each cipher text is embedded with an access structure. A user is able to decrypt a cipher text if and only if his attributes satisfythe access structure of the cipher text. The access structure is generalized as any Boolean formula over threshold gates on positive attributes and negative attributes. Proposed the CP-ABE construction under the generic group model. Proposed the provably secure CP-ABE under a standard assumption while only permitting AND gates and support in the access structure.

2.1. REVOCATION

Proposed first key revocation mechanisms in CP-ABE and KPABE settings respectively. These schemes enable an attribute key revocation by encrypting the message to the attribute set with its validation time. These attribute-revocable ABE schemes have the security degradation problem in terms of the backward and forward secrecy. Well-established d-BDH and decisional linear assumptions.

2.2. Attribute-Based Encryption with Non-Monotonic Formulas:

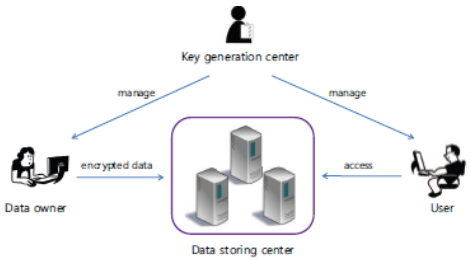
Our second key contribution is that we show how our techniques can be applied to achieving efficient Attribute-Based Encryption schemes with nonmonotonic access formulas. Ostrovsky, Sahai, and Waters showed a connection between revocation schemes and achieving non-monotonic access formulas in ABE; to negate an attribute in an access formula one applies a revocation scheme using the attribute as an identity to be revoked. Ostrovsky, Sahai, and Waters give a particular instance by adapting the revocation scheme of Naor and Pinkas to the ABE scheme of Goyal.

III.OUR CONTRIBUTION

Provide the rstconstruction of a cipher text policy attribute-based encryption to address this problem, and give the construction of such a scheme. In our system, a user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party

encrypts a message in our system, they specify an associated access structure over attributes. A user will only be able to decrypt a cipher text if that user's attributes pass through the cipher text's access structure.

At a mathematical level, access structures in our system are described by a monotonic access tree", where nodes of the access structure are composed of threshold gates and the leaves describe attributes. We note that AND gates can be constructed as n-of-n threshold gates and OR gates as 1-of-n threshold gates. Furthermore, we can handle more complex access controls such as numeric ranges by converting them to small access trees see discussion in the implementation section for more details.



IV. ATTRIBUTE-BASED ENCRYPTION

Our simple revocation scheme also gives rise to a new efficient Attribute-Based Encryption (ABE) scheme that allows access policies to be expressed in terms of *any* access formula over attributes. Until the recent work of Ostrovsky, Sahai, and Waters, all previous ABE schemes were limited to expressing only monotonic access structures. Our new ABE scheme, however, achieves significantly superior parameters in terms of key size.

4.1. Performance Measurements

They now provide some information on the performance achieved by the cpabe toolkit. Figure 3 displays measurements of private key generation time, encryption time, and decryption time produced by running cpabe-keygen, cpabe-enc, and cpabe-dec on a range of problem sizes. The measurements were taken on a modern workstation.4

4.2. Security of Revocable IBE

We define the selective-revocable-ID security for Revocable IBE schemes. Our security model captures the standard notion of selective-ID security but it also takes into account possible revocations. Since we explicitly consider time periods, in the beginning of the experiment in addition to the challenge identity the adversary also declares the challenge time. Just as in the standard slective-ID security definition the adversary can request to learn users' keys. In addition we let the adversary to revoke users of its choice (including the challenge identity) at any period of time and see all key updates.

4.3. Our Construction

In this section we provide the construction of our system. We begin by describing the model of access trees and attributes for respectively describing ciphertexts and private keys. Next, we give the description of our scheme. Finally, we follow with a discussion of security, efficiency, and key revocation. We provide our proof of security in Appendix A.

4.4. Challenges and Our Contributions

The main challenge of our construction is to formulate a reasonable security model

and provide formal security proofs when combining CP-ABE with proxy re-encryption. Our contribution can be summarized as follows. Firstly, we provide the definition for attribute revocation in CP-ABE with honest-but-curious severs, and formulate the security model to respect possible attacks. Secondly, the proposed scheme enables the authority to revoke any attribute of users at any time while placing a minimal load on him. Thirdly, the proposed scheme is provably secure under the Decisional Bilinear Di_e-Hellman (DBDH) assumption. Last but not least, our method is applicable to the KPABE counterpart in which the authority is able to revoke any partial access privilege of users.

4.5. Data Confidentiality

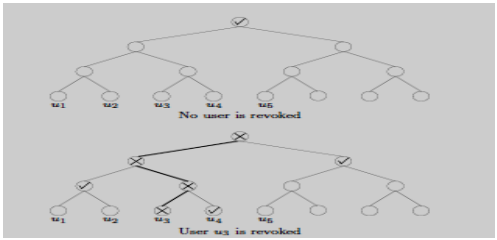
In our trust model, the KGC is no longer fully trusted as well as the data storing centre even if they are honest. Therefore, the plain data to be shared should be kept secret from them as well as from unauthorized users. Data confidentiality on the shared data against outside users who have not enough attributes can be trivially guaranteed. If the set of attributes of a user cannot satisfy the access tree in the cipher text, he cannot recover the desired value (*e.*g.) *rs* during the decryption process, where *r* is a random value uniquely assigned to him.

4.6. Application Considerations

Our scheme considers application scenarios of data sharing in which data are encrypted and stored on semi-trustable servers for sharing. In this scheme, the authority generates proxy re-key's whenever an attribute revocation event occurs. Proxy re-key's are then transmitted to proxy servers, who will re-encrypt existing cipher texts stored on them and update user secret key components if necessary. For simplicity of description, our scheme just considers one revocation event. Multiple revocation events are assumed to be handled by repeatedly executing these operations. When this assumption is convenient for theoretical analysis of the scheme, it will cause efficiency issue in practice since proxy servers have to re-encrypt cipher texts stored upon each revocation event.

4.7. Main Construction Execution:

Every user gets keys corresponding to its identity computed on polynomials of all



nodes on the path from the leaf node corresponding to that user to the root node. To be able to decrypt a cipher text encrypted with time t, any user just needs one key update corresponding to t computed on any one of the polynomials of nodes on the path from the leaf node of the user to the root node. Thus, when no user is revoked, key authority just needs to publish the key update computed on the polynomial of the root node. When a subset of the users is revoked, key authority first finds the minimal set of nodes in the tree which contains an ancestor or, the node itself among all the leaf nodes corresponding to non-revoked users. Then, key authority publishes key updates on polynomials of the nodes in this set.

V. CONCLUSIONS

This paper proposal to enforcement of access policies and the support of policy updates are important challenging issues in the data sharing systems. Proposed an IBE scheme with efficient revocation, whose complexity of key updates is significantly reduced from linear to logarithmic in the number of users compared to the previous solution. Discussed several variants achieving different levels of security. Also discussed how to construct an attribute-based encryption scheme with efficient revocation. Our schemes should be particularly useful in the settings where a large number of users is involved and scalability is an issue. We also note that decryption requires two or three pairings per share utilized in decryption, depending on whether the share corresponds to a non-negated attribute or a negated attribute, respectively. We also note that we use a random oracle for description simplicity and efficiency of the system.

VI. REFERENCES

[1]Sattam S. Al-Riyami, John Malone-Lee, and Nigel P. Smart. Escrow-free encryption supporting cryptographic workflow. *Int. J. Inf. Sec.*, 5(4):217–229, 2006.

[2] Walid Bagga, Refik Molva, and Stefano Crosta. Policy-based encryption schemes from bilinear pairings. In *ASIACCS*, page 368, 2006.

[3]J. Benaloh and L. J. Generalized Secret Sharing and Monotone Functions. In Advances in Cryptol-ogy {CRYPTO, volume 403 of LNCS, pages 27{36. Springer, 1988.

[4] J. Bethencourt, A. Sahai, and B. Waters. The cpabe toolkit. http://acsc.csl.sri.com/cpabe/.

[5] G. R. Blakley. Safeguarding cryptographic keys. In National Computer Conference, pages 313{317. American Federation of Information Processing Societies Proceedings, 1979.

[6] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In CRYPTO, pages 213–229, 2001.

[7] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In EUROCRYPT, pages 207–222, 2004.

[8] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In EUROCRYPT, pages 255–271, 2003.

[9] N. Attrapadung, H. Imai, ”Conjunctive Broadcast and Attribute-Based Encryption,” Proc. Pairing 2009, LNCS 5671, pp. 248–265, 2009.

[10] M. Pirretti, P. Traynor, P. McDaniel, B. Waters, ”Secure Attribute-Based Systems,” Proc. ACM Conference on Computer and Communications Security 2006, 2006.