Improving Security and Efficiency in Attribute-Based Data Sharing

1.Mr.Nilesh Gadhe
Department of Computer Engineering,Shri Chhatrapti Shivaji College of Engineering,Rahuri,India
gadhenilesh449@gmail.com
2.Mr.Swapnil Bhaskar
Department of Computer Engineering,Shri Chhatrapti Shivaji College of Engineering,Rahuri,India
bhaskarswapnil15@gmail.com

1.Prof.D.P.Gade
Asst. Professor, Department of Computer Engineering, Shri Chhatrapti Shivaji College of Engineering Rahuri Factory, India

Abstract- In some distributed systems a user should be able to access data if a user having a certain set of credentials data or attributes. The method for enforcing such policies are employ a trusted server to store the data and hypnosis access control .In our paper we present a system for complex access control on encrypted data that is Cipher-text Policy Attribute-Based Encryption. The cipher-text policy attribute-based encryption (CP-ABE) is becoming a cryptographic solution for this issue. The data owner define their own access policies over user attributes and impliment, the policies on the data to be distributed .So, the major drawback in previous system is a key escrow problem. The KGC could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scheme where the data owner make their private data only accessible to designated users. In addition, applying CP-ABE in the data sharing system introduces another challenge with regard to the user revocation since the access policies are defined only over the attribute universe. Therefore, in this study, we propose a novel CP-ABE scheme for a data sharing system by exploiting the characteristic of the system architecture. The proposed scheme features the following achievements: 1) the key escrow problem could be solved l, which is constructed using the secure two-party computation between the key generation center and the data-storing center, and 2) fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.

Keywords—Data sharing, attribute-based encryption, revocation, access control, removing escrow

Introduction

A recent development of the network and computing technology enables to share their data with others using online external storages. Attribute-based encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control [3], [4], [5], [6]. It provides a way of defining access policies based on different attributes of the data object. Especially, cipher-text policy attribute-based encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher-text, and enforce it on the contents [5].Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the data storage server for preventing unauthorized

data access, which is the traditional access control approach of such as the reference monitor [1].Nevertheless, applying CP-ABE in the data sharing system has several challenges. In CP-ABE, the key generation center (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 ciphertext addressed to specific users by generating their attribute keys. This could be apotential threat to the data confidentiality or privacy in the data sharing systems. Another challenge is the key revocation. Since some users may change their associate attributes at some time, or some private keys might be compromised, key revocation or update for each attribute is necessary in order to make systems secure. This issue is even more difficult especially in ABE, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a set of users as an attribute group). This implies that revocation of any attribute or any single user in an attribute group would affect all users in the group. It may result in bottleneck during rekeying procedure or security degradation due to the windows of vulnerability.

Related Work

ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE. In KP-ABE, attributes are used to describe the encrypted data and policies are built into users' keys; while in CP-ABE, the attributes are used to describe users' credentials, and an encryptor determines a policy on who can decrypt the data. Between the two approaches, CP-ABE is more appropriate to the data haring system because it puts the access policy decisions in the hands of the data owners[1].Cipher text-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the cipher text is associated with an access policy over attributes. The user can decrypt the cipher text if and only if the attribute set of his secret key satisfies the access policy specified in the cipher text. In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control [2]. In [3], they created public key revocation encryption systems with small cryptographic private and public keys. Their systems have two important features relating respectively to public and private key size. First, public keys in our two systems are short and enable a user to create a cipher text that revokes an unbounded number of users. This is in contrast to other systems where the public parameters bound the number of users in the system and must be updated to allow more users. Second, the cryptographic key material that must be stored securely on the receiving devices is small. Keeping the size of private key storage as low as possible is important as cryptographic keys will often be stored in tamper-resistant memory, which is more costly. This can be especially critical in small devices such as sensor nodes, where maintaining low device cost is particularly crucial [3]. Identity-based encryption (IBE) is an exciting alternative to public-key encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI). The senders using an IBE do not need to look up the public keys and the corresponding certificates of the receivers, the identities (e.g. emails or IP addresses) of the latter are sufficient to encrypt. Any setting, PKI- or identity-based, must provide a means to revoke users from the system. The most practical solution requires the senders to also use time periods when encrypting, and all the receivers (regardless of whether their keys have been compromised or not) to update their private keys regularly by contacting the trusted authority [4].

1]Existing Systems and Proposed Solution

The key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation centre and the data storing centre, fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system

A]Existing System

The existing attribute based encryption system are constructed on the architecture where key generation center (KGC) generate the private keys of users with its secret information .The key escrow problem is inherent such that the KGC can decrypt every cipher text addressed to users in the system by generating their secret keys at any time. The key generation center could decrypt any messages to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would make their private data only accessible to the users.

B]Proposed Solution

In this paper, we propose a novel CP-ABE scheme for a secure data sharing. The key issuing protocol generates and issues private keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing centre with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data storing centre in the proposed scheme.The key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation centre and the data storing centre. Fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.

2]Attribute Based Data Sharing System

A]Data Owner

It is a client who owns data, and wishes to upload it into the external data storing centre for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. Data Owner to get key from key generator Encrypt the file. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people

B]Data Storing Centre

It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. The data storing centre is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are

used to enforce a fine-grained user access control. Data storing centre store the data. Data Storage Centres provides offsite record and tape storage, retrieval, delivery and destruction services.

C]User

This is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then he will be able to decrypt the cipher text and obtain the data.

D]Key Generation Centre

It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted.

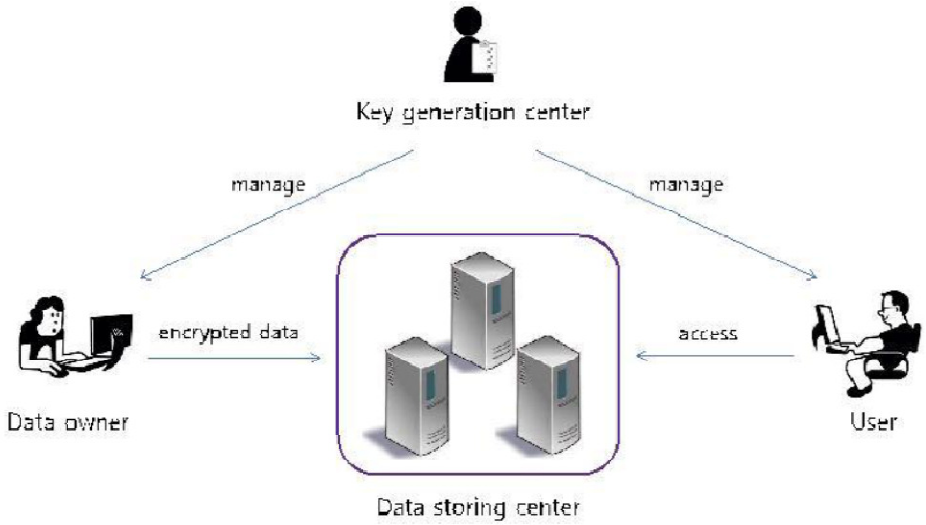

Fig.1-Architecture of a data sharing system.

Application

- Military application
- Companies
- Personal data sharing

Conclusion

In our paper, we proposed a attribute based data sharing scheme to enforce a fine-grained data access control by exploiting the characteristic of the data sharing system. The proposed scheme features a key issuing mechanism that removes key escrow during the key generation.

Referance

[1] Junbeom Hur,*Improving Security and Efficiency in Attribute-Based Data Sharing,*ISBN: 1041-4347/13,IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, October 2013

[2] Luan Ibraimi, Milan Petkovic, Svetla Nikova, Pieter Hartel and Willem Jonker, *Mediated Cipher text-Policy Attribute- Based Encryption and Its Application*,Information Security Applications, Lecture Notes in Computer Science, DOI: 10.1007/978-3-642-10838-9_23, pp 309-323,2009.

[3] Lewko, Allison; Sahai, Amit; Waters, Brent,*Revocation Systems with Very Small Private Keys*,Security and Privacy (SP), IEEE Symposium, May 2010, 978-1-4244-6895-9, pp 273 – 285, 2010.

[4] Alexandra Boldyreva, Vipul Goyal, Virendra Kumar,*Identity-based encryption with efficient revocation*,Proceedings of the 15th ACM conference on Computer and communications security, ISBN: 978-1-59593-810-7, pp 417-426, 2008.

[5] Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou,*Attribute based data sharing with attribute revocation*, Proceedings of the 5th ACM Symposium on Information, ISBN: 978-1-60558-936-7, pp 261-270, 2010.

[6] Ling Cheung, Calvin Newport,*Provably secure cipher text policy ABE*, Proceedings of the 14th ACM conference on Computer and communications security, ISBN: 978-1-59593-703-2, pp 456-465, 2007.

[7] B. SakthiSaravanan, R.Dheenadayalu, A.Vijayaraj,*Improving,Efficiency and Security Based Data Sharing in Large Scale Network*,IJESIT;Volume2; Issue1;January2013

[8]John Bethencourt, Amit Sahai, Brent Waters,*Ciphertext-Policy Attribute-Based Encryption.*

[9] V. Goyal, A. Jain, O. Pandey, and A. Sahai, *Bounded Ciphertext Policy Attribute-Based Encryption*,Proc. Int'l Colloquium Automata,Languages and Programming (ICALP), pp. 579-591, 2008.

[10] X. Liang, Z. Cao, H. Lin, and D. Xing,*Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption*, Proc. Int'l Symp. Information, Computer, and Comm. Security (ASIACCS), pp. 343-352, 2009.

[11] M. Chase and S.S.M. Chow,*Improving Privacy and Security in Multi-Authority Attribute-Based Encryption*,Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.

[12] S.S.M. Chow, *Removing Escrow from Identity-Based Encryption*, Proc. Int'l Conf. Practice and Theory in Public Key Cryptography(PKC '09), pp. 256-276, 2009.

[13] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Hysyanskaya, and H. Shacham, *Randomizable Proofs and Delegatable Anonymous Credentials*, Proc. Ann. Int'l Cryptology Conf.Advances in Cryptology (Crypto '09), pp. 108-125, 2009.