International Journal of Research in Advent Technology, Vol.3, No.2, February 2015
E-ISSN: 2321-9637

A Secure Data Sharing Using Attribute Based Encryption

Miss. Priti D. Wanmali, Dr. D. G. Harkut
M.E. (CE) II Year, Dept. Computer Science and Engineering
Prof. Ram Meghe College of Engineering & Management
Amravati, India
pritiwanmali@gmail.com, dg.harkut@gmail.com

Abstract— The data security concerns and requirements are very essential for social networks or for cloud computing where individuals, organizations, and businesses may outsource their various types of data, including highly sensitive data into the cloud. Always people would like to make their sensitive or private data only accessible to authorized people having some access policies. Attribute-based encryption provides a way of defining access policies based on different attributes of the requester, environment or the data object. Specially, in ciphertext-policy attribute-based encryption (CP-ABE) each user is associated with a set of attributes and data are encrypted with access structure.The decryptor should have the attribute set to decrypt the ciphertext. But there is a major issue of key escrow problem. As the key generation center could decrypt the data of a specified user by generating their private keys which is not acceptable in data sharing scenerios where data owner would like to access their private data only to a specified users. Also applying CP-ABE in data sharing scenerios have problem of user revocation because the access policies are defined on the basis of attributes universe. Therefore, a novel CP-ABE scheme is introduced to overcome the drawbacks. This scheme have following achievements :1) The key issuing problem is resolved by a key issuing protocol which generates and issues user secret keys by performing secure two-party computation protocol between key generation center (KGC) and the data-storing centers with their own master secrets. 2) The immediate user revocation can be done via proxy encryption mechanism together with the CP-ABE algorithm. The performance of this scheme indicates that it is efficient to securely manage data over the data sharing systems. But key generation center and the data storing centre's are semitrusted, they can collude with each other and can access plaintext of the encrypted data. So we propose a new approach to overcome this issue. The keys for encrypted files which are also in encrypted form and the attributes are also in encrypted form are stored in database so that only authorized user can decrypt the secure data. The proposed scheme enhances data privacy and confidentiality in the data sharing system.

Index Terms—Cloud computing, Attribute based encryption, Escrow, Revocation.

1. INTRODUCTION

Nowdays development of network is very fast which makes data sharing paradigm easier in distributed systems such as online social network or cloud computing. People may share data or messages through online social network or as the cloud computing provides a more cost effective environment, many corporate companies share data within company or in between different different companies. With the facilities of technology and services, there is increase in demands of data security and control access. People always want to access their private data to the authorized people which should possess some credentials.

An attribute-based encryption is an encryption technique which achieves a fine-grained data access control in which access policies are defined based on different attributes.

Ciphertext policy attribute-based encryption (CP-ABE) enables encryptor to define the set of attributes which decryptor have to possess to decrypt the ciphertext. In CP-ABE scheme, the key generation centre provide private keys to users by applying the KGC's master secret keys to users having a set of attributes which reduces the need of storing public key certificates in traditional public key infrastructure.

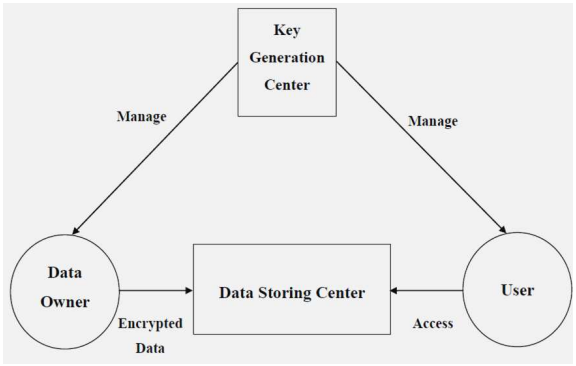

Fig1.Data Sharing System

This advantage came with a issue of key escrow problem. The KGC can decrypt ciphertext of every user which decreases data confidentiality in data sharing systems. Also there is another issue of key revocation. Sometimes, users may change their set of attributes. So, to make the system secure, attributes should be updated. In attribute-based encryption, each attribute is shared by multiple users. Therefore, the revocation of any attribute or any user affects all other users which may results in bottleneck during rekeying procedure [1].

2. MOTIVATION

The data security is very essential for social network or cloud computing where sharing of data takes place between users. Every user wants their data to be accessed or shared by authorized user having some credentials. Traditional data sharing system have semitrusted authorities such as key generation centre and data storing center. Many of the previously proposed encryption techniques which are used in data sharing scenario have some issues like varying size of ciphertext, private and public key size etc. So in order to overcome these issues and to increase the performance of the system we are planning to propose a secure data sharing using attribute based encryption.

3. LITERATURE REVIEW

Crescenzo, Ostrovsky and Rajgopalan [2] came up with an economical and secure time-release cryptography theme employing a "time server" that inputs this time into the system. Additionally they give a proper definition for the cryptanalytic task of a timed-release cryptography theme and resolution to the present task. They introduce a replacement variant of oblivious transfer protocol, that they called as conditional oblivious transfer and a construction for an instance of it.

Cramer and Shoup [3] presented a new public key cryptosystem. They analysed that it is provably secure against adaptive chosen ciphertext attack. This is the only scheme which is quite practical and provably secures which relies only on a standard intractability assumption.

Boneh and Franklin [4] came up with a fully functional identity-based encryption scheme. The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffie-Hellman problem.

Sahai and Waters [5] introduced the concept of Fuzzy Identity Based Encryption. This concept allows error-tolerance between the identity of a private key and the public key used to encrypt a ciphertext. They described two practical applications of Fuzzy-IBE of encryption using biometrics and attribute-based encryption.

Boneh, Crescenzo, Ostrovsky and Persiano [6] studied the problem of searching on data which is encrypted using a public key system. They proposed a mechanism called Public Key Encryption with keyword search which enables user to provide a key to the gateway that enables the gateway to test whether the specific word is a keyword in the email without learning more about email.

Nali, Adams, Miri [7] described a provably-secure efficient collusion-resistant threshold attribute-based encryption (thABE) scheme. The proposed scheme handles multiple attribute sets with dynamically-specifiable threshold values and can be used to support biometric based cryptographic access control.

Pirretti, Traynor, McDaniel and Waters [8] presented a novel secure information management architecture and implementation. They illustrated the infrastructure through the creation and performance evaluation of two applications: a HIPAA compliant distributed file system and a social network.

Bethencourt, Sahai and Waters [9] came up with a system for ciphertext-Policy Attribute Based Encryption which allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. This system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys.

Ostrovsky, Sahai and Waters [10] presented the first Attribute Based Encryption system that supports the expression of non-monotone formulas in key policies. They achieved this through a novel application of revocation methods into existing ABE schemes.

Sun and Liu [11] came up with a multi-group key management scheme that achieves hierarchical access control in secure group communication in which multiple data streams are distributed to group members having various access privileges. The proposed scheme has less overhead associated with key management.

Cheung, Cooley, Khazan and Newport [12] proposed a new scheme called group key management scheme which is based on ciphertext-policy attribute-based encryption. An individual group member is identified by a set of attributes and is given a secret key in the CP-ABE system that corresponds to their attribute set.

Cheung and Newport [13] presented several related CP-ABE schemes.

Boldyreva, Goyal and Kumar [14] proposed an identity-based encryption scheme with efficient revocation, whose complexity of key updates is significantly reduced compared to the previous solution. They also discussed about how to construct an attribute based encryption scheme with efficient revocation.

Chase and Chow [15] came up with an attribute based encryption scheme without the trusted authority and an anonymous key issuing protocol.

Belenkiy, Camenisch, Chase, Kohlweiss, Hysyanskaya and Shacham [16] proposed an efficient delegatable anonymous credentials system. They revised the entire approach to construct anonymous credentials and identify randomizable zero-knowledge proof of knowledge systems as the key building block.

Canetti and Hohenberger [17] proposed a definition of security against chosen ciphertext attacks for proxy re-encryption schemes and presented a scheme that satisfies definition. Also they formalize definitions of security against chosen ciphertext attacks for re-encryption schemes as game-based definition and two simulation-based definition that guarantee universally composable security.

Goyal, Pandey, Sahai and Waters [18] developed a new crypto system for fine-grained sharing of encrypted data called Key-Policy Attribute-Based Encryption (KP-ABE). In proposed crypto system, ciphertexts are labelled with sets of attributes and private keys are associated with access structures that specify which ciphertext a user is able to decrypt.

Yu, Ren, Lou and Li [19] came up with a novel KP-ABE to prevent abuse attack which is able to detect any illegal key distributer's ID. The main idea in this scheme is black box tracing which traces to the illegal key distributer's ID only by observing the pirate output for certain inputs.

Canetti, Halevi and Katz [20] proposed the first non-trivial scheme of forward-secure public-key encryption schemes. This scheme mainly achieves security against chosen-plaintext attacks under the decisional bilinear Diffie-Hellman assumption in the standard model. They also proposed slightly more efficient scheme in the random oracle model. These schemes can be extended to achieve security against chosen ciphertext attacks and to support an unbounded number of time periods.

Boneh and Boyen [21] came up with two efficient Identity Based Encryption (IBE) systems that are provably selective identity secure without the random oracle model. Their first system is based on the Decision Bilinear Diffie-Hellman (Decision BDH) assumption which extends to give an efficient selective identity secure Hierarchical IBE without random oracle while second system is based on a related assumption called the Bilinear Diffie-Hellman inversion assumption.

Boneh, Gentry and Waters [22] came up with two new public key encryption schemes which are fully collusion resistant. In first scheme the broadcast message and user's private keys are of constant size. The second scheme is generalization of the first that enable tradeoff, public key size for ciphertext size.

Agrawal, Kiernan, Srikant and Xu [23] presented an encryption mechanism called as Order Preserving Encryption Scheme (OPES) which allows comparison operations to be directly applied on encrypted data without decrypting the operands. The results produced by query processing are exact. OPES handles updates gracefully and new values can be added without requiring changes in the encryption of other values.

Y. Hanaoka, G. Hanaoka, J. Shikata and H. Imai [24] came up with a novel approach of identity-based encryption in which decryption key can be renewed without making changes in its public key. In order to deal with this, they constructed a new IBE model in which decryption key can be updated non-interactively which allows user to renew and update his decryption key without having help from the central authority and without changing their identity.

Lin, Cao, Liang and Shaon [25] proposed a threshold multi authority fuzzy identity based encryption (MA-FIBE) scheme without any central authority like key generation centre. In this scheme, an encryptor can encrypt message such that a user can only decrypt if he has at least d_k of given attributes about message for at least t+1, $t \leq n/2$ honest authorities of all n attribute authorities. The proposed MA-FIBE which is extended to multi authority attribute based encryption is also presented.

Vimercati, Foresti, Jajodia, Paraboschi and Samarati [26] have put forward the idea of enforcing the authorization policy by using a two-layer selective encryption. Their solution offers significant benifits in terms of quicker and less costly realization of authorization policy updates and general efficiency of the system.

Staddon, Golle, Gagne and Rasmussen[27] came up with a system to protect identity and other sensitive information by controlling access to an individual's attributes through encryption. Their system encrypts not only sensitive personal information, but also groups of personal attributes which may indirectly allow for the inference of a person's identity, even though none of the attributes is directly sensitive.

Goyal, Jain, Pandey, Sahai [28] presented the first construction of a ciphertext-policy attribute based encryption scheme having a security proof based on a number theoretic assumption and supporting advanced access structures.

Ibraimi, Petkovic, Nikova, Hartel and Jonker [29] proposed a scheme as mediated Ciphertext-Policy Attribute Based Encryption that supports revocation of user attributes. The scheme allows the encryptor to encrypt a message according to an access policy over a set of attributes and users who satisfy the access policy and whose attributes are not revoked can able to decrypt the ciphertext.

Chow [30] proposed a new notion of anonymous ciphertext indistinguishability against attacks which is orthogonal to existing notions like user anonymity and came up with new system architecture with an anonymous key issuing protocol to protect the confidentiality of the users' identities.

Lewko, Sahai and Waters [31] presented a simpler revocation system which has following features: both public and private keys are of size independent of the number of users, the ciphertext only contains O(r) group elements, where r is the number of revoked users.

Yu, Wang, Ren and Lou [32] addressed an important issue of attribute revocation for attribute based systems. In particular they considered practical application scenerios in which semi-trustable proxy servers are available and proposed a scheme supporting attribute revocation. One plus point of this scheme is that it places minimal load on authority upon attribute revocation events. They achieve it by uniquely combining the proxy re-encryption technique with CP-ABE and enabled the authority to delegate most laborious tasks to proxy servers.

4. COMPARATIVE STUDY

Table 1. Comparison between existing model

Sr. No.	Methodology	Performance Evaluation			
		Key Size	Ciphertext Size	Security	Computation Overhead
1	Fully functional identity-based encryption scheme [4]	-	-	Moderate	-
2	Fuzzy identity-based encryption [5]	Vary	Vary	High	Moderate
3	Public key encryption with keyword search [6]	Vary	-	Moderate	Moderate
4	Threshold attribute-based encryption for practical biometric-based access control [7]	Vary	-	High	Moderate
5	Ciphertext policy attribute-based encryption [9]	-	Vary	Moderate	Moderate
6	Identity-based encryption with efficient revocation[14]	-	-	Moderate	-
7	Key-Policy Attribute-based encryption (KP-ABE) [18]	Vary	Vary	Moderate	Moderate
8	Novel Key-Policy Attribute-based encryption scheme [19]	Vary	-	Moderate	Moderate
9	Efficient Selective-ID Secure Identity-based encryption (IBE) [21]	-	-	Moderate	-
10	Order Preserving Encryption [23]	Vary	-	High	Moderate
11	Attribute-based data sharing with attribute revocation [32]	-	Vary	Moderate	Moderate

In above table we have done the comparative study of various techniques of encryption. In our proposed approach, we are planning to overcome some of the limitation of techniques such as varying size of ciphertext, private and public key size, semi trustable proxy servers because of which the performance of model increases. In our proposed model attributes will be stored in database because of which the size of ciphertext will not vary after the revocation of attributes of any user and those attributes will be stored in database in an encrypted form. Also in our proposed model private and public keys will not contain attributes in it and those attributes will be stored in database in an encrypted form so that key size will not increase or decrease after including attributes or after revocation of attributes and intruder would not be able to decrypt the data. As key generation centre or data storing centre are semitrusted, we will not rely on them and the keys will be system generated keys so that they would not be able to decrypt the data.

5. CONCLUSION

In this paper we have done a review of a secure data sharing using attribute based encryption. We have studied various encryption techniques with their goals and limitations. In order to increase the performance of the model we are planning to overcome some of the limitations of these techniques.

ACKNOWLEDGEMENT

The authors thank Junbeom Hur for this work.

REFRENCES

[1] Junbeom Hur. (2013): Improving Security and Efficiency in Attribute-Based Data Sharing. IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10.

[2] Di Crescenzo, G.; Ostrovsky, R.; Rajagopalan, S. (1999): Conditional Oblivious Transfer and Timed-Release Encryption. In Advances in Cryptology { Eurocrypt '99, Lecture Notes in Computer Science, Vol. 1592, pp. 74.

[3] Cramer, R.; Shoup, V. (1998): A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Advances in Cryptology { Crypto, Lecture Notes in Computer Science, Vol. 1462, Springer-Verlag, pp. 13.

[4] Boneh, D.; Franklin, M.K. (2001): Identity-Based Encryption from the Weil Pairing. Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229.

[5] Sahai.; Waters, B. (2005): Fuzzy Identity-Based Encryption. Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt '05), pp. 457-473.

[6] Boneh, D.; Crescenzo, G.D.; Ostrovsky, R.; Persiano, G. (2004): Public-Key Encryption with

Keyword Search. In *Advances in Cryptology { Eurocrypt*, volume 3027 of *LNCS*, pages 506{522. Springer.

[7] Nali, D.; Adams, C.; Miri, A. (November 2005): Using threshold attribute-based encryption for practical biometric-based access control. 1(3):173–182.

[8] Pirretti, M.; Traynor, P.; McDaniel, P.; Waters, B. (2006): Secure Attribute-Based Systems. Proc. ACM Conf. Computer and Comm. Security.

[9] Bethencourt, J.; Sahai, A.; Waters, B. (2007): Ciphertext-Policy Attribute-Based Encryption. Proc. IEEE Symp. Security and Privacy, pp. 321-334.

[10] Ostrovsky, R.; Sahai, A.; Waters, B. (2007): Attribute-Based Encryption with Non-Monotonic Access Structures. Proc. ACM Conf. Computer and Comm. Security, pp. 195-203.

[11] Sun, Y.; Liu, K. (March 2004): Scalable hierarchical access control in secure group communications. In Proc. of the IEEE Infocom, Hong Kong, China.

[12] Cheung, L.; Cooley, J.; Khazan, R.; Newport, C. (2007): Collusion-resistant group key management using attribute-based encryption. Cryptology ePrint Archive Report 2007/161. http://eprint.iacr.org/.

[13] Cheung, L.; Newport, C. (2007): Provably Secure Ciphertext Policy ABE. Proc. ACM Conf. Computer and Comm. Security, pp. 456-465.

[14] Boldyreva, A.; Goyal, V.; Kumar, V. (2010): Identity-Based Encryption with Efficient Revocation. Proc. ACM Conf. Computer and Comm. Security, pp. 417-426.

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

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

[17] Canetti, R.; Hohenberger, S. (2007): Chosen-Ciphertext Secure Proxy Re-Encryption. In Proc. of CCS, New York, NY, USA.

[18] Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. (2006): Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. Proc. ACM Conf. Computer and Comm. Security, pp. 89-98.

[19] Yu, S.; Ren, K.; Lou, W.; Li, J. (2009): Defending Against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems. In Proc. of Securecomm, Athens, Greece.

[20] Ran Canetti; Shai Halevi; Jonathan Katz. (2003): A forward-secure public-key encryption scheme. In Proceedings of Eurocrypt. Springer-Verlag.

[21] Boneh, D.; Boyen, X. (2004): Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles. In *Advances in Cryptology { Eurocrypt*, volume 3027 of *LNCS*, pages 223{238. Springer.

[22] Boneh, D.; Gentry, C.; Waters, B. (2005): Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. In *Advances in Cryptology { CRYPTO*, volume 3621 of *LNCS*, pages 258{275. Springer.

[23] Agrawal, R.; Kierman, J.; Srikant, R.; Xu, Y. (June 2004): Order preserving encryption for numeric data. In Proc. Of ACM SIGMOD 2004, Paris, France.

[24] Hanaoka, Y.; Hanaoka, G.; Shikata, J.; Imai, H. (2005): Identity-based hierarchical strongly key-insulated encryption and its application. In ASIACRYPT, pages 495–514.

[25] Huang Lin; Zhenfu Cao; Xiaohui Liang; Jun Shao. (2008): Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority. In *INDOCRYPT*, volume 5365 of *LNCS*, pages 426–436. Springer.

[26] Vimercati, S.D.C.; Foresti, S.; Jajodia, S.; Paraboschi, S.; Samarati, P. (2007): Over-Encryption: Management of Access Control Evolution on Outsourced Data. Proc. Int'l Conf. Very Large Data Bases (VLDB).

[27] Golle, P.; Staddon, J.; Gagne, M.; Rasmussen, P. (2008): A Content-Driven Access Control System. Proc. Symp. Identity and Trust on the Internet, pp. 26-35.

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

[29] Ibraimi, L.; Petkovic, M.; Nikova, S.; Hartel, P.; Jonker, W. (2009): Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application. Proc. Int'l Workshop Information Security Applications (WISA), pp. 309-323.

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

[31] Lewko, A.; Sahai, A.; Waters, B. (2010): Revocation Systems with Very Small Private Keys. Proc. IEEE Symp. Security and Privacy, pp. 273-285.

[32] Yu, S.; Wang, C.; Ren, K.; Lou, W. (2010): Attribute Based Data Sharing with Attribute Revocation. Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS).