ISSN: 2320-1363

Cipher text Attribute based encryption for improving security and efficiency for distributed networks

G.Vanaja Kumari*1, S.Narendra*2, R.Pitchaiah*3

1*M.Tech Scholar, Dept of CSE, Universal College of Engineering & Technology, Perecherla, Dist: Guntur, AP, India

2*Assistant Professor, Dept of CSE, Universal College of Engineering & Technology, Perecherla, Dist: Guntur, AP, India

3*Associate Professor & HOD, Dept of CSE, Universal College of Engineering & Technology, Perecherla, Dist: Guntur, AP, India

ABSTRACT

Cloud computing and online social networks are the big business technologies which use the distributed servers to store and process the data. Providing accessing rights and security are two fundamental problems identified in the distributed networks. We are proposing a new algorithm called cipher-text attribute based encryption for provides the set access policies to the user in order to access the data on the distributed servers. The algorithm also improves the efficiency of the user data transmission over the network. The main aim of the proposed system is to solve the two major problems called key escrow problem and fine grained user revocation problem.

KEYWORDS: Distributed network security, access policies, Attribute based encryption, CP-ABE, data sharing.

I.INTRODUCTION

Cloud computing and online social networks are the big business technologies which use the distributed servers to store and process the data. The clients stores data on the servers and access the data. Online social networks improve the process of sharing common feelings of many people on the same sites like face book and orkut etc. Providing security to the user's data become

ISSN: 2320-1363

very important task for the online social network providers. We need to store data in a proper manner so that only an authorized person can access the data.

Attribute-based encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control. It provides a way of defining access policies based on different attributes of the requester, environment, or 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 ciphertext, and enforce it on the contents. 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].

II.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 sharing system because it puts the access policy decisions in the hands of the data owners [2], [3].

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 [4].

Using ABE, a user or data owner can encrypt the broadcast data using Cipher text attribute based encryption by using receiver

ISSN: 2320-1363

information or without using receiver information. Consider Alice want to set an access policy such that “CS” AND “Student” to reach the broadcasted message to all CS students without the receiver information. If Bob with attributes {“EE”,”Faculty”} cannot access the broad cat messages because he violated the access policy. It is simple procedure to apply on any number of attributes.

III.PROPOSED SYSTEM

Our proposed system has two modules.

3.1 Key Management

3.2 CP-ABE scheme

3.1 KEY MANAGEMENT

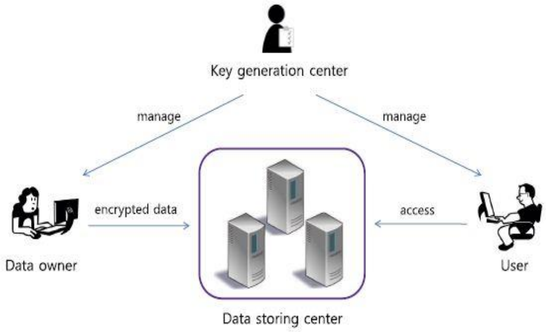

Figure1: data sharing and key management architecture

Key management mainly explains basic data sharing architecture and security model for providing basic security. It contains four basic terms called Key Generation center, Data owner, Data storage Center, User.

Key generation center 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. It is assumed to be honest-but-curious

Data-storing center is an entity 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

Data owner is a client who owns data, and wishes to upload it into the external data-storing center for ease of sharing or for cost saving.

3.2 CP-ABE SCHEME

CP-ABE scheme uses the basic architecture of key management system. The key generation center is a basic block which generates the private keys of users by applying the KGC's master secret keys to users' associated set of attributes.

CP-ABE has four fundamental algorithms called setup, key generation, encryption and decryption as explained below.

Setup Algorithm:

The Setup algorithm takes input *k* as the number of attributes in the system. It returns public key *PK* and master key *MK*. The public key is used for encryption while the master key is used for private key generation.

Key generation Algorithm:

The key generation algorithm takes the public key *PK*, the master key *MK* and the users attribute list *L* as input. It outputs the private key of the user.

Encryption Algorithm:

The Encrypt algorithm takes the public key *PK*, the specified access policy *W* and the message *M* as input. The algorithm outputs cipher text *CT* such that only a user with attribute list satisfying the access policy can decrypt the message. The cipher text also associates the access policy *W*.

Decryption Algorithm:

The Decrypt algorithm decrypts the cipher text when the user's attribute list satisfies the access policy specified in the cipher-text. It takes the public key *PK*, the private key *SK* of the user and the cipher text *CT* as input. It returns the plaintext *M* if *L j= W*, where *L* is the user's attribute list and *W* is the access policy.

IV.RESULTS AND DISCUSSION

The rekeying in the proposed scheme can be done in an immediate way as opposed to BSW. Therefore, a user can be revoked at any time even before the expiration time which might be set to the attribute. This enhances security of the shared data in terms of the backward/forward secrecy by reducing the windows of vulnerability. In addition, the proposed scheme realizes more fine-grained user revocation for each attribute rather than for the whole system. Thus, even if a user drops some attributes during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy.

ISSN: 2320-1363

V.CONCLUSION

Our proposed system cipher-text attribute based encryption (CP-ABE) provides the set access policies to the user in order to access the data on the distributed servers. The algorithm also improves the efficiency of the user data transmission over the network. The proposed algorithm mainly eliminates the problems key escrow problem and fine grained user revocation problem. We can extend our future work to improve the performance of the system.

VI.REFERENCES

1. J. Anderson, "Computer Security Planning Study," Technical Report 73-51, Air Force Electronic System Division, 1972.
2. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.
3. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.
4. 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.
5. Junbeom Hur "Improving Security and Efficiency in Attribute-Based Data Sharing" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 10, OCTOBER 2013 2271.
6. S.D.C. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P.Samarati, "Over-Encryption: Management of Access Control
7. Evolution on Outsourced Data," Proc. Int'l Conf. Very Large Data Bases (VLDB '07), 2007.
8. 7.D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Ann. Int'l

Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

9. A. Kate, G. Zaverucha, and I. Goldberg, "Pairing-Based Onion Routing," Proc. Privacy Enhancing Technologies Symp., pp. 95-112, 2007.
10. L. Cheung and C. Newport, "Provably Secure Ciphertext Policy ABE," Proc. ACM Conf. Computer and Comm. Security, pp. 456-465,2007.
11. 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.
12. 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.
13. The Pairing-Based Cryptography Library, http://crypto.stanford. edu/pbc/, 2012.
14. K.C. Almeroth and M.H. Ammar, "Multicast Group Behavior in the Internet's Multicast Backbone (MBone)," IEEE Comm. Magazine,vol. 35, no. 6, pp. 124-129, June 1997.
15. 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.
16. 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.
17. 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.