ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Attribute - Based Data Sharing

Rahila Fatima[1], Dr. S. S. Lomte[2], Saad Siddiqui[3]

ME Student, Computer Science and Engineering, EESCOE&T, Aurangabad, India[1]

Professor, Computer Science and Engineering, EESCOE&T, Aurangabad, India[2, 3]

Abstract: There have been increasing demand and concerns for distributed security, with the recent adoption and diffusion of data sharing in distributed systems such as cloud computing. Enforcement of access policy and policy updates are the challenging issues in data sharing system. This issue can be solved by using cryptographic techniques. Cipher text policy attribute based encryption (CP-ABE) is one of the promising solutions. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. The major drawback is the key escrow problem. Escrow means storage, here the key is stored in third party that is key generation centre. The key generation center could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to 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. The proposed scheme can solve the two problems key escrow problem and revocation problem.

Keywords: Removing Escrow, Revocation, Attribute Based Encryption, Access Control.

I. INTRODUCTION

If we take today's scenario, the use of technology and internet made us relax in portability of data. We can nowadays share almost everything others like pictures, movies, thoughts, etc. If we need an emergency help from a doctor or hospital for chronic diseases like cardio, hepatic, neuro related previous data, we are now able to produce with the help of internet or cloud technology. Due to large number of internet users, it is also required to protect our data from being misused. An unauthorized person should not be made access to the private data of an individual. For this reason we are required to take care of data by implementing data protection techniques like cryptography. Our work in this area is based on Attribute based Encryption.The main objective is to provide secure sharing of data in cloud. Objectives of the system and how it is met are as follows:

- Data confidentiality-Unauthorized user should not access the plain text of the data. Data should be prevented from unauthorized users do not have attributes to satisfy the access policy. Here the data is in encrypted format and the technique used is customized blowfish.
- Fine grained access control-Access control list (ACL) is defined so that authorized user with required access policy can access the data.
- Collusion Resistance- Collusion resistance is one of the most important security property required in systems. If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone. Here the key is generated by Key Generation Centre kept in encrypted format in database which is not known to Key Generation Centre. Partial key is with user and partial key is with master admin, there is a chance that key can be decrypted. Here, Master Admin generates secret key which is also encrypted and stored in database with user name and rights.
- Removing Key escrow problem-Key escrow problem is removed by Key Generation Centre. Here a secret key is generated and stored in database which is not known to Key Generation Centre.
- Removing Revocation problem-: Key Revocation is removing the user private key. Revocation of key is not fully ensured since half of the key is with user and otherhalf withmaster admin. Here in the key revocation process of this system the users' key validity is removed.
- Scalability- Multiple users can access the data since it is deployed on cloud.

II. RELATED WORK

In literature we studied found that many researchers working on attribute based encryption uses almost similar techniques. Changsha et al [1] in their study propose a novel two-dimensional-scalable access control by generating access keys. Their analysis showed the scheme is able to provide collusion resistance, as well as forward and backward secrecy. Ming et al [2] enabled dynamic modification of access policies or file attributes supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Huang Qinlong et al [3] presented a multiparty access control model, enabled the disseminator to update the access policy of ciphertext if their attributes satisfy the access policy.

Zhu et al [4], Linke et al [5] [7] [9] experimentally proved that fuzzy authorization can achieve fuzziness of authorization among heterogeneous clouds with security and efficiency. Correa et al [6] and Jadliwala et al [15] proposed WhACKY! to harness the multi-source information from tweets to link Twitter profiles across other external services. WhACKY! Guarantees that the mapped profiles are 100% true-positive and helps quantify the unintended leakage of Personally Identifiable Information (PII) attributes. During the process,

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

WhACKY! is able to detect duplicate Twitter profiles connected to multiple external services. Yanchao et al [8] presented two novel schemes for users to detect fake top-k query results as an effort to foster the practical deployment and use of the proposed system. Yan Zhu et al [10] proposed a novel cryptographic comparison method based on forward and backward deviation functions. The method supported dual range comparisons and tree-oriented keyword search, as well as almost constant complexity for large size of integer range. They also providedseveral authentication mechanisms for preventing unpermitted access and verifying validity of protocol output.

III. EXISTING WORK

A. Architecture

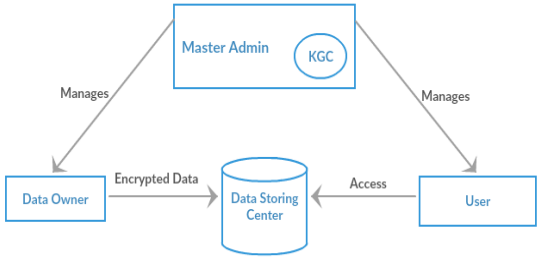

Figure 1: Existing system architecture

B. System

In the given system there are 3 types of users, figure 1:

1. Master Administrator: The Master Admin has the KGC (Key generation Center) with him. The KGC is used to generate a random key which is known to the Master Admin. Master Admin assign key to users.
2. Data Owner: Data owner is a user which modifies the data stored in the data storing center. He uses the key provided by the Master Admin to encrypt his data while storing in the data center. This encryption is done on the basis of the key given by the Master Admin to ensure data confidentiality and integrity. This user doesn't have the privileges to decrypt the data.
3. User: The user has access to the encrypted data who can view the encrypted data by decrypting the data with the help of a key assigned by the master admin. The master admin first assigns the key to the user and then decrypts the data based on that key.

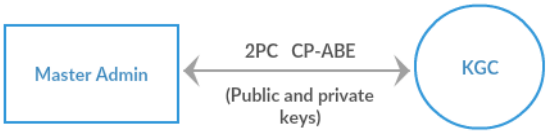

Figure 2: Existing system user interface

When the master admin generates the keys of any of the above users a key-pair is generated consisting of public and private keys for each admin. The encryption technique used here is CP-ABE(Ciphertext Policy Attribute based encryption) which works on 2PC protocol(2 Phase commit protocol). In this type of protocol the encryption is done with the help of the two keys generated. The plaintext entered by the data owner is encrypted partially by the public key which resides with the master admin and the other partial half is done with the help of the private key which resides with the data owner. The 2PC protocol works on SSL handshake which is a technique used to manage the encryption keys during the plaintext encryption done by both the keys, figure 2.

Similarly, the decryption of data is done by the private key from the admin and the public key from the user. Here again the 2PC protocol is used to manage both the keys.

IV. IMPROVISED WORK

In the improvised system we have entities data admin, user and Key Generation Center. Here a key is generated by KGC and stored in data storing center in encrypted form this key is generated and processed on separate service which is not known to anyone. The only thing data admin has to do is to get a key from the service and assign the key to the user.The user in the improvised system is divided according to the access control list provided by the admin.

A. Architecture

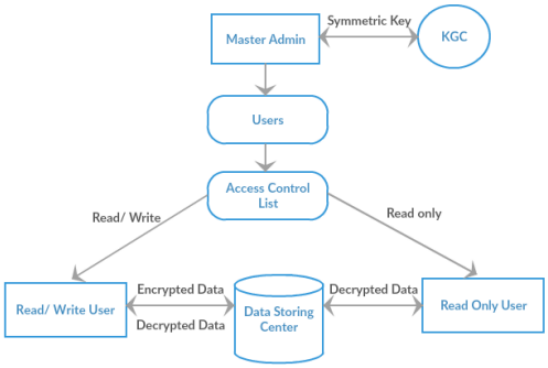

Figure 3: Improvised System Architecture

B. Improvised System

In the given system there are two types of Admin

1. Master Admin
2. User

In this improvised system the KGC is separated from the master admin. The key generated by KGC is not known to anyone.The key is generated and processed on a separate service. The key is generated and stored in the data storing center in encrypted form. The only thing the master admin has is to get the key from the service and assign the key to the user.

The user in the improvised system is divided according to the access control list provided by the admin. There are two kinds of access control lists

1. Read and Write: The user with this access privileges can modify his own data which he entered before. This user has the rights of encrypting plaintext data, modifying the plaintext data previously entered and decrypting the data previously entered.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

2. Read-Only: The user with this access privileges can only view the data but cannot modify the data. This user can also view other user's data. This user only has the privilege of decrypting information and displaying it in plaintext form

Figure 4: Improvised system user interface

The key in this improvised system is a symmetric key. Unlike the key-pair which uses private and public key the symmetric key contains only private key. This key is not with the master but it is resides only with the user. This key also has validity set by the master admin during assignment. The master admin makes request for the key to the KGC service. The KGC services generate a private key which is randomly generated and is also encrypted and stored in the data center.

The encryption technique used here is Blowfish. Blowfish is a symmetric key algorithm. It generates only one key which is a private key and it is shared directly with the user.When the key expires the user contacts with the master admin to seek a new key from KGC. The master admin generates the key and assigns the key to the user. If the user privileges are read and write the previously entered data is re-encrypted and is stored with the user, as shown in Figure 4.

C. User Processes

When the user having read write privilege accesses his account using a user name and password assigned by the master admin, the user's privileges are checked which was granted by the master admin during registration. This process where access control lists are checked against the user is called authorization. After authorizing the user the user's key validity is check. This process is called validation where user's key duration is checked. After all the checkpoints the user's key is applied to his session. The same process is followed to readonly privileged user but only with the decryption authority.

V. RESULT

Existing System Problems: The escrow problem is the major disadvantage in this form of the system. In the existing system the escrow problem is dealt with key revocation mechanism. The key revocation involves removing the private keys granted to the users. This task is done by master admin. The keys revocation doesn't fully ensure the removal of rights from the using because only half of the key is revoked which resides with the user that is the private key whereas the private key still persists with the admin. Another major disadvantage of this system is that the master admin knows both the keys as the KGC resides with the master admin. So, in the absence of the user the master admin himself may violate the data confidentiality and integrity process and might sneak in the private data of the data owner. Yet another major disadvantage is that the CP-ABE encryption technique used in this system is a slow process as it has to communicate with both the entities to perform encryption.

Overcoming the existing problem**:** The escrow problem is fully resolved within this process. In the key revocation process of this system the user's key validity is removed. Unlike the existing system, in the absence of the user no one can access his private data as the key is not known to anyone and it is also encrypted and stored in database. One added advantage the improvised system has over the existing system is the encryption technique. The encryption technique used is proven to be the strongest and hasn't been decrypted until date.

VI. SIMULATION PROCEDURE

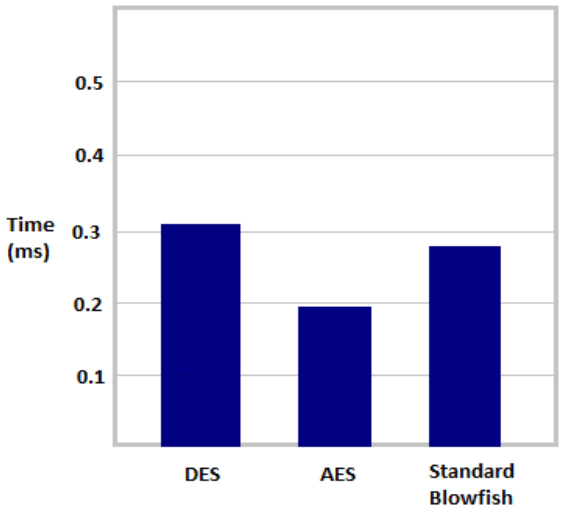

Figure 5: Existing system encryption time

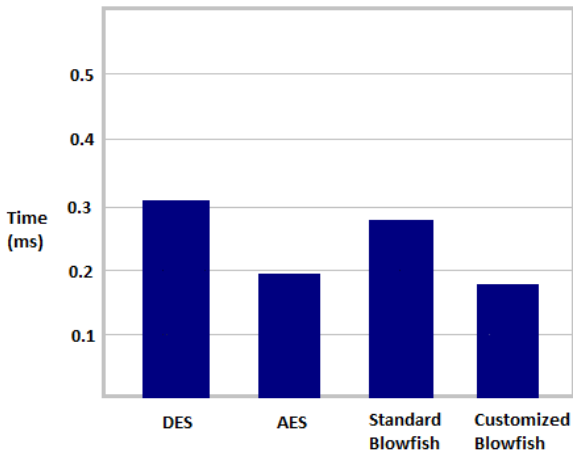

Figure 6: Improvised Encryption time

Main purpose here is to calculate the Encryption and Decryption speed of each algorithm for different packet sizes. Their implementation is tried to optimize the maximum performance for the algorithm. The throughput for encryption as well as decryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption scheme.The encryption techniques used to calculate the throughput is: Data Encryption Standard (DES), Advanced Encryption Standard (AES)

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

VII. CONCLUSION

To conclude, the implementation of access policies is important in the data sharing environment. In this study, we proposed an attribute based data sharing scheme which will be implemented on a fine-grained data access control. The proposed scheme issues a key that removes key escrow. The user keys are generated by computation such that any key generation center cannot derive the private key. Thus, the proposed scheme enhances data privacy and confidentiality in the data sharing system. Therefore, the proposed scheme achieves more secure and fine-grained data access control in the data sharing system. We would like to point that the proposed scheme is efficient and scalable to securely manage user data in the data.

ACKNOWLEDGEMENT

I express my sincere thanks to my dissertation guide **Prof. Saad Siddiqui**, for guiding me every step in making this project. He motivated me & boosted my confidence &i must admit that the work would not have been accomplished with his guidance and encouragement.
I would like to extend my special thanks to **Dr. S. S. Lomte** for spending his valuable time to go through my report and providing many helpful suggestions.
Most likely I would like to express my sincere gratitude towards my parents, my Family and friends, for always being there with me. With all respect and gratitude, I would like to thank all the people, who have helped me directly or indirectly. Without their silence support and encouragement for this work could not have been possible.

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] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Euro crypt '05), pp. 457-473, 2005.
[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-PolicyAttribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
[6] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf.Computer and Comm. Security, pp. 195-203, 2007.
[7] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems withVery Small Private Keys,"Proc. IEEE Symp. Security and Privacy,pp. 273-285, 2010.
[8] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.
[9] N. Attrapadung and H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption," Proc. Int'l Conf. Palo Alto on Pairing-Based Cryptography (Pairing), pp. 248-265, 2009.[10] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems," Proc. ACM Conf. Computer and Comm. Security, 2006.
[11] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," ACM Computing Surveys, vol. 35,no. 3, pp. 309-329, 2003.
[12] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A Content-Driven Access Control System," Proc. Symp. Identity and Trust on the Internet, pp. 26-35, 2008.
[13] 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.
[14] S.D.C. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P.Samarati, "Over-Encryption: Management of Access Control Evolution on Outsourced Data," Proc. Int'l Conf. Very Large DataBases (VLDB '07), 2007.
[15] 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.
[16] A. Kate, G. Zaverucha, and I. Goldberg, "Pairing-Based Onion Routing," Proc. Privacy Enhancing Technologies Symp., pp. 95-112,2007.
[17] L. Cheung and C. Newport, "Provably Secure Ciphertext Policy ABE," Proc. ACM Conf. Computer and Comm. Security, pp. 456-465,2007.
[18] 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.
[19] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded CiphertextPolicy Attribute Based Encryption,"Proc. Int'l Symp. Information, Computer, and Comm. Security (ASIACCS), pp. 343-352, 2009.
[20] The Pairing-Based Cryptography Library, http://crypto.stanford.edu/pbc/, 2012.
[21] 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.
[22] 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.
[23] Junboemhur "Improving Security and Deficiency in attribute based Data Sharing".
[24] Schneier, Description of new variable length key, 64bit block cipher (Blowfish) "Fast software Encryption", Cambridge security workshop Proceedings,(DEC 1993),pp.191