Advancement in Security and Efficiency for Attribute Based Data Sharing System

Vaibhav Satane[1], **Arindam Dasgupta**[2]

[1]Department of Information Technology, AVCOE Sangamner, University of Pune, Ahmednagar, India

Abstract: ***Data sharing system such as social network or cloud computing there is an demand for distributed data security .The challenging issue in data sharing system is access policy and support of policy update cipher text .The policy attribute based encryption (CP-ABE)is cryptographic solution to this issue. The data owner defines their own access policy over user attribute and applies this policy on data. In this research work the proposed novel CP-ABE scheme is used to solve the key escrow problem by escrow free key issuing protocol generated by using two party computations between key generation center and data store center.***

Keywords: Attribute based encryption, Key Escrow, Access Structure, Revocation, Secret Sharing Scheme

1. Introduction

As a use of internet increases the people store their data online such as social site like Facebook, Twitter and cloud services also store and shared the data to enterprise. Sometime People can share their private data such as picture, messages on this site this data is highly confidential to them but they are an aware of data security so that sometime an unauthorized user can use their data in wrong intention such as in terrorist attack. People send their mail to each other and share their data; the data is confidential so there is a need data of security. So people want to access their data only to authorized people. There will be need to encrypt data stored at this site.

2. Related Work

First cryptographic approach such as Attribute Based Encryption [1][2][3] is proposed by Vipu lGoyal, PandeyAmit and Sahaiz Brent Waters with fine grained data access. It provides way define access policy based on different attribute. In Attribute Based Encryption (ABE) system user key's and cipher text associated with set of descriptive attributes and particular key can decrypt a particular cipher text if there is match between the attributes. this type of encrypting data have an drawback it can be selectively shared only coarse grained level that means private key shared with another party. The Sahai and Waters proposed the Threshold ABE system for error tolerant identity based encryption scheme in which ciphertext associated with set of attributes S and user private key associate with both threshold parameter and another set of attribute. In order decrypt a ciphertext at least k attribute overlapped with cipher text and private keys. The drawback of Threshold ABE is threshold semantic are not expressive. A. Sahai and B. Waters proposed the new Attribute based encryption, in this scheme private keys can represent any access formula including non monotone. it can handle any access structure that represent Boolean formula such as AND,OR, Not and so.

To solve this issue a new encryption technique is proposed by Vipul Goyal in 2006 called as Key Policy Attribute Based Encryption (KP-ABE)[1].In this system cipher text are associated with set of attributes and private key are associated with access structure that specify. The key policy Attribute based encryption allow decryptor for decryption of the ciphertext only when at least k attributes overlapped between ciphertext and key structure. In the Key policy Attribute based encryption system also define scheme known as secret sharing scheme of data where the access structure involved threshold gate Shamir and Balkley first time proposed the secret sharing scheme and in which if t or more parties come together they can create secret. The secret sharing scheme (SSS)[1] specify tree access structure where interior node consist of AND &OR gate and leave consist different parties. Any set of parties that satisfy the tree come together and reconstruct secret. In KP-ABE user key's associated with tree access Structure and leaves are associated with attributes. The user able to decrypt ciphertext if attributes associated with ciphertext satisfies key access structure. The difference between SSS and KP-ABE is secret sharing scheme allow for cooperation between different parties and in KP-ABE parties have forbidden. The example given is that if Sam has the key associated with access structure "X & Y" and Bob has an key associated with access structure "Y & Z" then we would not want to able to decrypt a ciphertext who has only an attribute Y by colluding..Key Policy-Attribute Based Encryption scheme consist of four algorithms.

2.1 Key Policy Attribute Based Encryption Algorithm

- **Setup:** This algorithm does not take any input other than implicit security parameter. It outputs the public key (Pk) and master key (Mk).
- **Encryption:** This algorithm takes the input as a message m, a set of attributes γ and public key (Pk).It outputs the ciphertext E.

- **Key Genration:** This algorithm takes input as access structure A, the master key Mk and the public key Pk. It outputs the decryption key D
- **Decryption:** This algorithm takes input a ciphertext E that was encrypted under set of attributes y, the decryption key D for access control structure A and the public key Pk. It outputs the message M if γ € A.

The Ciphertext Policy Attribute Based Encryption (CP-ABE)[7][8][9][10] proposed by John Bettencourt, Amit

Sahai and Brent waters. By using this technique the data confidentiality achieved and secure against collusion attacks. In some distributed system user only able to access if any server storing the data is compromised then confidentiality of data also compromised. The CP-ABE keeps data confidential. In the CP-ABE, user's private key associated with set of attributes. Then party encrypts message in system, theyspecify the access structure over attributes. a authorized user only able to decrypt the ciphertext if that user attribute pass through ciphertext access structure. The Ciphertext Policy Attribute Based Encryption scheme is more appropriate to the data sharing system because CP-ABE keeps the access policy decision in hands of data owner's.CP-ABE support multilevel threshold access structure In CP-ABE the key generation center is responsible for generation of private keys. The key generation centers decrypt any message addressed to user by generating the user's private key.

In The Ciphertext Policy Attribute Based Encryption AND gates constructed as n -of –n threshold gates and OR gate as 1-of-n threshold gate and access structure is monotonic. The disadvantage in Key Policy Attribute based encryption; the encryptor has no control over who has access data, except the choice of descriptive attributes for data. The main objective of CP-ABE is attaining the collusion resistance. That means if several user collude then should not able to decrypt the ciphertext if at least one user decrypt it on their own. If we don't want to decrypt data by colluders then combine their attributes. This type of security knows as sine qua non of access control. The CP-ABE scheme consists of four fundamental algorithms.

2.2 Ciphertext Policy Attribute Based Encryption Algorithm

- **Setup:** This algorithm does not take any input other than implicit security parameter. It outputs the public key (Pk) and master key (Mk).
- **Encryption:** This algorithm takes the input as a message M, access structure A and public key (Pk).the algorithm encrypt M and produce ciphertext CT such as only authorized user with set of attribute that satisfy access structure will be able to decrypt the message.
- **Key Genration:** This algorithm takes input as the master key Mk and the set of attributes S that describe the key. It outputs the private key Sk.
- **Decrypt:** This algorithm takes input as a public key (Pk), ciphertext CT and private key Sk which is private key of set of attribute. If set of attributes satisfy the access structure A then only the algorithm decrypt by escrow free key issuing protocol key. It is constructed using two party computations and second fine grained user revocation per each attribute is done by proxy encryption which improves efficiency Chase and Chow proposed the distributed KP-ABE scheme to solve the key escrow problem [5] in multi authority system. In this all attribute authority which participates in key generation protocol in distributed way so they cannot pool the multiple data and link by single user. . In this scheme no centralized key authority present. Each attribute authority communicates with one another for private key generation this result in performance and communication degradation. Xiaohui Liang and Rongxing Lu proposed the CP-ABE with efficient revocation [6], [7], [10], [11] Develop revocation technique to improve the efficiency key update algorithm.

They modified the CP-ABE scheme to revocable CP-ABE model. In which each user assign with unique identifier which central revocation possible. Encryption and decryption algorithm are not affected by unique identifiers and providing the efficient and expressive operation. Be then court and boldy reva first proposed the key revocation mechanism in CP-ABE and KP-ABE. In this scheme revocation achieved by encrypting message to attribute set with validation time. Attrapadung and Imai proposed the user revocable ABE scheme in which data owner maintaining all membership list for each attribute group to enable the direct user revocation. The key issuing protocol generates secret key by performing secure two party computations between key generation center and data storing center such that none of them generate whole set of user key alone so user not require full trust on KGC and data storing center in order to protect the data which is shared. User revocation achieved via proxy encryption which then are used to reencrypt the ciphertext encrypted under the CPABE algorithm. Each revocation done at attributes level rather than system level.

3. Comparison Table

Table 1: Comparison between ABE, KP-ABE, CP-ABE

Attribute Based Encryption	*Key Policy Attribute Based Encryption*	*Cipher Text Policy Attribute Based Encryption*	*Novel CipherText Policy Attribute Based Encryption*
It provides way to define the access policy based on different attribute.	*In KP-ABE encryptor has no control over who access the data.The intelligence assumes.*	*In Cp-ABE, encryptor has intelligently decided who access the data.*	*It enables data owner to decide their own access policy.*
In this user key's and ciphertext associated with set of descriptive attributes	*Each private key associated with access structure that specifies which type of ciphertext can decrypt.*	*In CP-ABE, the KGC generate private key of user by applying master key to user set of attributes*	*In this scheme, key issuing protocol generates user's secret key. By performing secure two party computation*

4. Conclusion

This Paper presents literature survey on improving security in data sharing system by using encryption technique such as Attribute based Encryption which involve basic encryption scheme as well as advance scheme such as Ciphertext policy attribute base encryption ,Key Policy Attribute based encryption and Novel Ciphertext policy based encryption.

References

[1] 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.

[2] Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc.Int'l Conf. Theory and Applications

of Cryptographic Techniques (Eurocrypt ’05), pp. 457-473, 2005.

[3] 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.

[4] 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.

[5] 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.

[6] Boldyreva, V. Goyal, and V. Kumar, “Identity-Based Encryption with Efficient Revocation,” Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.

[7] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp.Security and Privacy, pp. 321-334, 2007.

[8] L. Cheung and C. Newport, “Provably Secure Ciphertext Policy ABE,” Proc. ACM Conf. Computer and Comm. Security, pp. 456-465,2007.

[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] 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.

[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.

Author Profile

Satane Vaibhav V. received the B.E. in Information technology from M.S.Bidve Engg. College Latur and Perusing M.E. from AVCOE Sangamner.