HYPERVISED TECHNIQUE IN MULTI POSTURE ATTRIBUTE BASED KEY GENERATION

[1] **Ms. M.Kalaiselvi.**
P.G Student, M.E, Computer Science and Engineering,
Dhaanish Ahmed college of Engineering, Chennai-601301, Tamilnadu, India.

[2] **Dr.T.Amitha.**
Professor, Dept of Computer Science and Engineering,
Dhaanish Ahmed college of Engineering, Chennai-601301, Tamilnadu, India.

***Abstract*— The main objective of this project is to improve the security and the efficiency while sharing the data between data owner and the users. Based upon the attributes of the users we are going to share the data. One of the most challenging issues in confidential data sharing systems is the enforcement of data access policies and the support of policies updates. Cipher text policy attribute based encryption (CP-ABE) is becoming a promising cryptographic solution to this kind of problem. 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 overcomes the key escrow problem. The Matrix type key generation can defend against key logging attacks and shoulder surfing attacks, by having the final password inputted by way of certain alphanumeric matrix letters which are separated by a particular distance from the letters forming the password in the alphanumeric matrix. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.**

1. INTRODUCTION

In the Distributed system, all users should trust the central authority. Since the user's data are sensitive, the problems exist when they are in the Distributed system. In the existing system, the following are the disadvantages,

i. The keys are generated to the user only in the random manner.
ii. The data are stored in the data center without any encryption.
iii. Key-Escrow problem.

These problems must be solved in order to avoid the above problem.

Furthermore, the data are retrieved to the user depending on the designation or hierarchy of the user. In this paper, the keys are generated using the attributes specified by the user. The user can specify which attribute to be taken into consideration. Depending on this attribute the keys are generated. Although the previous scheme generates the key, they are not as secure as the proposed one. The users do not have any rights on deciding which algorithm to encrypt the message. In the proposed system, the user can select any algorithm that they want to encrypt.

One of the most challenging issues in confidential data sharing systems is the enforcement of data access policies and the support of policies updates. Cipher text policy attribute based encryption (CP-ABE) is becoming a promising cryptographic solution to this kind of problem. It enables data owners to define their own access policies over their user attributes and enforce the policies on the data to be distributed. However, the advantage of the system comes with a major drawback which is known as a key escrow problem. The key generation center could decrypt any kind of messages addressed to specific users by generating their private keys. This is not suitable for data sharing typical 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. Ciphertext-Policy ABE (CP-ABE): In these schemes, the Ciphertext is associated with an access structure, while the secret keys are labeled with a set of attributes Therefore, in this study; we propose a novel CP-ABE scheme for a data sharing system by exploiting the characteristic of the system architecture.

2. EXISTING SYSTEM

A. Problem Statement:

In the prevailing system, the major issue the user facing is the key-escrow problem. This key-escrow problem is considered to be issues of the user privacy. This problem arises when any of the authority can decrypt the message and it can be viewed. The keys are generated with the algorithm without the intervention of the user. The users do not have any rights over their data. This cause the issue in the security.

Keys were generated randomly and it's decided by the key generation center and the user doesn't have any control/preferences or specification of deciding the key based on user centric purpose.

The key generation center (KGC) can decrypt every Ciphertext addressed to specific users by generating their attribute keys. This could be a potential threat to the data confidentiality or privacy in the data sharing systems. The revocation of any attribute or any single user in an attribute group would affect all users in the group. Most of the existing ABE (Attribute-based encryption) schemes are constructed on the architecture where a single trusted authority or KGC has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the KGC can decrypt every Ciphertext addressed to users in the system by generating their secret keys at any time.

B. Disadvantage of Existing System:

The main disadvantage of the existing system is that the data sharing is not much secure in the existing system. Other users can easily access the data in the data store. If the central authority is malicious, then the data can be misused. The system will not distribute the data based on the attributes of the user. Instead, they are distributed in the random fashion. The data are generated in the data storage center. They are stored without any encryption in the data. Thus if the authority in the data center is malicious, they can easily misused by the data.

3. PROPOSED SYSTEM

The problems in the existing system are solved in the proposed system. The key-escrow problem which is considered to be the most unsecure are get resolved in the proposed system.

The keys are generated using the attributes that are defined by the user. The user may enter many details while they register.

Any one among them will be taken into consideration. Depending on that attribute, the key are generated in the application center. The key will be combined with some algorithm and the modified key is stored in the data storage center. This is stored with the double encryption.

The key escrow problem is resolved by a key issuing protocol that exploits the characteristic of the data sharing system architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing center with their own master secrets. The immediate user revocation can be done by using proxy encryption mechanism together with the CP-ABE algorithm. Attribute group keys are selectively distributed to the valid users in each attribute group, which then are used to re-encrypt the Ciphertext encrypted under the CP-ABE algorithm. The proposed scheme delegates most laborious tasks of membership management and user revocation to the data storing center while the KGC is responsible for the attribute key management as in the previous CP-ABE schemes without leaking any confidential information to the other parties.

There may also a security question given in order to retrieve the key from the data storage center. While sending the key to the user, it is double encrypted. After the user receives this key, double encryption is done in the user's side in order to get the original key.

If the user want to get the data, that are given in the hierarchal fashion. The data view may be varied with the hierarchy/designation. The higher authority may be given more rights to view more authenticated data. While the others are given some lower priority data to be viewed.

User is given the priority to select the algorithm in which the keys should be generated for their own data. If the data is highly secure, the rich algorithm should be taken into consideration. If it is little secured, then the algorithm should be in such a case. Thus customizing algorithm gives more support to the proposed system.

A. Advantages:

i. The data is shared between the data owner and the users based on the attributes.
ii. The escrow problems are solved in the existing system

4. WORKING

The user enters the attributes during his registration. He can also define which algorithm to use to encrypt.

There are three centers

i. Application Center
ii. Key Generation Center
iii. Data Storing Center

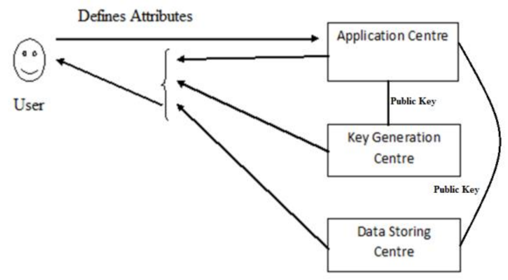

Figure 1. Architecture Diagram.

Keys were generated in these three centers. After that all keys are combined to get the encrypted key. This will be stored in the data storage center after the encryption.

5. DEFINING ATTRIBUTE

Attributes of the user will be taken as an input in the system. In addition, the position / designation of the user will be taken in to consideration.

The first one specified in the previous line is used to generated a 2PC (two-party computation) protocol between the KGC (Key generation center) and the data storing center. We can define this system as 3PC (Three-Party computation). The reason is due to generation of the key in the Application Center too.

On the other end, the second option of fetching the designation is used to get the data retrieval in the hierarchical manner. So that, a partial disclosure of data comes into the picture.

Our overall ideas towards this project are to create a multi location based key generation associated with hierarchical based data distribution and hiding.

6. ESCROW-FREE KEY ISSUING PROTOCOL

In this module the KGC and the data storing center are involved in the user key issuing protocol. In the protocol, a user is required to contact the two parties before getting a set of keys.

The KGC is responsible for issuing attribute keys to user and the secret key is generated through the secure 2PC protocol between the KGC and the data storing center. To decrypt the data the user needs the keys from the data storing center and KGC. Thus we overcome the escrow technique by using this protocol.

Our proposed system incorporated 3PC protocol where the key will be generated in Application center too and the keys will be merged using Ant-Colony Algorithm.

7. AUTHENTICATION

Authentication Module describes the interface between the user and system and the admin provided the type of authentication.

The user is allowed to create his credentials to login into the system. An admin need to approve the users created and login approval the user will be allowed to access the application.

This module displays a form in which the customers have to enter his/her user name. When the name attribute is entered, the module creates a corresponding matrix format and it is displayed in the form.

The matrix that is created consists of random characters which consist of alphabets and numbers. The key code that was given by the user during his/her registration would now be taken into account to create the new password.

The key code that is given by the user always contains even number of characters. Now each characters is paired with its adjacent characters moving from left to right. Now each pair of characters is considered in the new password creation. If a pair is taken, the 1st character is matched with the character in the row of the matrix that is displayed and the second character is matched with the characters in the column of the matrix.

Now the character that is present in the intersecting location of the former row and the column is taken and it is given as the first character of the new password. To get the other characters for the new password, the same procedure is repeated with the adjacent pairs of characters that were got from the key code.

An aspect of the invention can provide a password input system and method that can defend against key logging attacks and shoulder surfing attacks, by having the final password inputted by way of certain alphanumeric matrix letters which are separated by a particular distance from the letters forming the password in the alphanumeric matrix. Also, an aspect of the invention can provide a password input system and method that can further increase the probability of defending against key logging attacks and shoulder surfing attacks, by having the final password inputted by way of certain alphanumeric matrix letters which are separated by a particular distance from the letters forming the password in the alphanumeric matrix, but with the alphanumeric matrix rotated every time a letter is inputted.

8. DATA RE-ENCRYPTION

The data owner uploads the data in data storing center after encryption. Before sending those Ciphertext to the users the data storing center re-encrypt it by using re-encryption algorithm. If the user needs to access the data means they need to decrypt the data twice. After the authentication module, the user allowed to enter into system if he enters the valid password based on the key code given during the registration process. The user now allowed entering the text in the area provided for that. There will be another area provided that displays the encrypted text for the given normal text. Before entering any text in the normal text field, there will be an encrypted text for the empty space. Based on the designation of the user, the data gets encrypted. For the same normal data, with the different designation, different encrypted text is created and shown. After entering the text, the user should click the insert data button. Now the data gets stored.

9. HIERARCHICAL / PARTIAL DISCLOSURE

The Data in the system will be stored in a Hierarchical manner. Same data will store in a different format based on the designation / Hierarchy.

User will be provided an option of defining the algorithm for storing the data is one of the possible way incorporated in this module.

Due to partial disclosure algorithm, the data will be retrieved based on the hierarchy.

10. ALGORITHM CUSTOMIZATION

Algorithm customization plays main role in the system. This option provides the option that enables the users to select an encryption algorithm of his/her choice. User will be provided an option of defining the algorithm for encryption. The user can define in which algorithm his data should be encrypted. Individuals can select different algorithm.

Different levels of hierarchies are available in the system. The confidentiality depends on the hierarchies. Thus more security must be given to higher hierarchies. This gets achieved through this algorithm customization.

11.ALGORITHM: MD5:

The **MD5 Message-Digest Algorithm** is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value.

One MD5 operation. MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. *F* is a nonlinear function; one function is used in each round. M_i denotes a 32-bit block of the message input, and K_i denotes a 32-bit constant, different for each operation. $\lll_s$ denotes a left bit rotation by *s* places; *s* varies for each operation. $\boxplus$ denotes addition modulo 2^{32}.

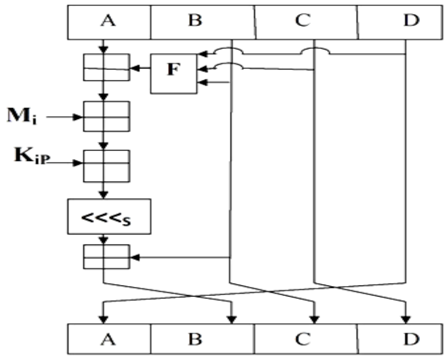

Figure 2. Operation of md5 algorithm.

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted *A*, *B*, *C* and *D*. These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed *rounds*; each round is composed of 16 similar operations based on a non-linear function *F*, modular addition, and left rotation. Figure 1 illustrates one operation within a round. There are four possible functions *F*; a different one is used in each round:

$$F(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$

$$G(X, Y, Z) = (X \wedge Y) \vee (X \wedge \neg Z)$$

$$H(X, Y, Z) = X \oplus Y \oplus Z$$

$$I(X, Y, Z) = Y \oplus (X \vee \neg Z)$$

12.CONCLUSION

The CP-ABE scheme reduces the problem of key-escrow. It will be attracted a lot, because the attribute based encryption help a lot to improve the security of the data.

Therefore, in this study, we proposed 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 by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation center and the data storing center.

(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.

The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and the Editor–in–Chief for their valuable comments that have helped us to improve the manuscript and they are very thankful to IJACT Journal for the support to develop this document.

REFERENCES

[1] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proceedings: Public Key Cryptography - PKC'11 (D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, eds.), vol. 6571 of Lecture Notes in Computer Science, (Taormina, Italy), pp. 53–70, Springer, March 6-9 2011.

[2] N. P. Smart, "Access control using pairing based cryptography," in *The Cryptographers' Track at the RSA Conference - CT-RSA'03*, vol. 2612 of *LNCS*, pp. 111–121, 2003.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings: IEEE Symposium on Security and Privacy (S & P'07)*, (Oakland, California, USA), pp. 321– 34, IEEE, May 20-23 2007.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings: Advances in Cryptology - EUROCRYPT'05* (R. Cramer, ed.), vol. 3494 of *Lecture Notes in Computer Science*, (Aarhus, Denmark), pp. 457–473, Springer, May 22-26 2005.

[5] M. Chase, "Multi-authority attribute based encryption," in *Proceedings: Theory of Cryptography Conference-TCC'07* (S. P. Vadhan, ed.), vol. 4392 of *Lecture Notes in Computer Science*, (Amsterdam, The Netherlands), pp. 515–534, Springer, February 21-24 2007.

[6] S. Muller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption," in *Proceedings: Information Security and Cryptology-ICISC'08* (P. J. Lee and J. H. Cheon, eds.), vol. 5461 of *Lecture Notes in Computer Science*, (Seoul, Korea), pp. 20–36, Springer, December 3-5 2008.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multiauthority attribute based encryption without a central authority," in *Proceedings: International Conference on Cryptology in India- INDOCRYPT'08* (D. R. Chowdhury, V. Rijmen, and A. Das, eds.), vol. 5365 of *Lecture Notes in Computer Science*, (Kharagpur, India), pp. 426–436, Springer, December 14-17 2008.

[8] A. Lewko and B. Waters, "Decentralizing attribute - based encryption," in *Proceedings: Advances in Cryptology-EUROCRYPT'11* (K. G. Paterson, ed.), vol. 6632 of *Lecture Notes in Computer Science*, (Tallinn, Estonia), pp. 568–588, Springer, May 15-19 2011.

[9] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," in *Proceedings: ACM Symposium on Information, Computer and Communications Security-ASIACCS'11*, pp. 386–390, ACM, 2011.

[10] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings: Advances in Cryptology-CRYPTO'01* (J. Kilian, ed.), vol. 2139 of *Lecture Notes in Computer Science*, (Santa Barbara, California, USA), pp. 213–229, Springer, August 19-23 2001.

[11] Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in Proceeedings: European Symposium on Research in Computer Security-ESORICS'11 (V. Atluri and C. Diaz, eds.), vol. 6879 of Lecture Notes in Computer Science, (Leuven, Belgium), p. 278297, Springer, September 12-14 2011.

[12] S. Muller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," Bulletin of the Korean Mathematical Society, vol. 46, no. 4, pp. 803–819, 2009.

[13] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings: IEEE International Conference on Computer Communications-INFOCOM'10, (San Diego, CA, USA), pp. 534– 542, IEEE, March 15-19 2010.

[14] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, 2011.

[15] S. Yu, K. Ren, and W. Lou, “FDAC: Toward fine-grained data access control in wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 22,

[16] J. Herranz, F. Laguillaumie, and C. R´afols, “Constant size ciphertext in threshold attribute-based encryption,” in Proceedings: Public Key Cryptography-PKC’10 (P. Q. Nguyen and D. Pointcheval, eds.), Lecture Notes in Computer Science, (Paris, France), pp. 19–34, Springer, May 26-28 2010.

[17] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute- based encryption and (hierarchical) inner product encryption,” in Proceedings: Advances in Cryptology-EUROCRYPT’10 (H. Gilbert:, ed.), vol. 6110 of Lecture Notes in Computer Science, (French Riviera), pp. 62–91, Springer, May 30 - June 3 2010.

Biographies

Dr.T.Amitha received the B.E degree in Computer Science and Engineering from the University of Madras, Chennai, Tamilnadu, in 2000, and the M.Tech degree in Computer Science of Engineering from the University of Bharath, Chennai, Tamilnadu 2006, and the Ph.D. degree from the University of Bharat, Chennai, Tamilnadu 2011, respectively. She is an associate professor in college affiliated to Anna University, Chennai. Her teaching and research area include Data mining, Information Security, Operating System, Artificial Intelligence, Cryptography and Network Security.

M. Kalaiselvi received the B.E degree in Computer Science and Engineering from the Anna University, Chennai, Tamilnadu, in 2011, and doing M.Tech degree in Computer Science of Engineering from the College affiliated to Anna University, Chennai, Tamilnadu .