ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Amelioration of Decentralized Cipher Text Policy Attribute Based Encryption with Mediator technique by adding Salt

Varsha S Rasal
Department of Computer Science & Engineering, Nehru College of Engineering & Research Center, Thrissur Kerala, INDIA

Suraj U Rasal
Computer Engineering Department, Bharati Vidyapeeth University College of Engineering, Pune, INDIA

Alwin Anto K Joseph
Department of Software Engineering, Sichuan University, Chengdu, CHINA

Nefilda K Joseph
Applied Electronics and communication system , Nehru College of Engineering & Research Center,Thrissur Kerala, INDIA ,

Abstract: The existing techniques had focused more on the attribute based encryption, cipher text policies and multiple authorities to make the network security more sheltered. But due to the attribute leak problem, these techniques were disabled to protect user's privacy. To enhance the security level, the proposed system has added salting method into the DCP-ABE-M scheme. Here both the data and user attributes are utilized to avoid attribute leak problem. The proposed system has a decentralized environment which contains multiple authorities who generates secret keys by using user attributes, data attributes and also contains multiple mediators who act as the middleware between user-authority. Both the power's doesn't stores any user details or full secret keys in their DB or in system. That is, all the user details and secret key will be hidden. In some cases the different users may use same keywords as their passwords which may leads to rainbow table attack or dictionary attack. To avoid this problem, salting is added into DCP-ABE-M. A unique salt value is added into the passwords which makes the password more strong and different from other passwords. Hence the proposed system enhances the level of security by adding salt value and is more efficient than the previously existing schemes.

Keywords: DCP-ABE, Data attributes, Mediator, Salt method, User attributes.

I. INTRODUCTION

Internet services and applications that allows communication, storage and data management from anywhere has become an inextricable part of daily life. The major source of data available on the internet and web services is web applications. Unfortunately, as the complexity and count of web application raises there will be an increase in the complexity and number of security issues. These security issues can be solved by using modern cryptographic techniques. Modern cryptography is a study of secret writing on which networking is based. Cryptography is heavily based on the methods which convert the plain text into the target recipient and then again it is converted into its initial form. Internet is large data storage system which shares its data only with valid or authenticated user who have conformed his identity, can be called as authenticated user. Digital signatures, certificates and attributes can be also used for authentification purpose.

Traditional asymmetric cryptographic technique had used certificate, which is an electronic document containing key information, user identity and digital signature that provides privacy sensitive user information. In this scheme, a certificate authority is used which distributes individual certificates for every user but here the problem is certificate storage DB get overloaded when users increases. In 1984; as an alternative to traditional public key encryption technique, Shamir invented a scheme called Identity Based Encryption (IBE) which eliminates certificate storage problem. In this scheme, instead of using certificates Shamir used user's own identity as public key such as email id, phone number etc. But the major drawback of this system is, it only allows one to one communication and doesn't support one to many communication. Here the originator must gain the public key of the acknowledger and require more storage space, these are the some disadvantages of IBE system. In order to resolve this problem, Sahai and Waters proposed Fuzzy IBE as their seminal work. In this scheme a set of descriptive attributes gives the identity of the user. Then Fuzzy IBE is further extended into ABE [1] in 2005 by Sahai and Waters. In this scheme access control level is maintained by a single central authority. When the numbers of users are huge it becomes challenge for the central authority to maintain the overall system. Central authority problem is solved by Sahai and Waters by designing Multiple Authority Attribute Based Encryption (MABE) scheme which is then extended in 2009 by Melissa Chase [2][3]. Since MABE is mostly applicable on distributed system, it makes the use of cipher text policy based encryption technique. This scheme utilizes a single central authority whose function is system initialization only and also it uses multiple authorities which generates secret key for the user. Here this system lacks when the central authority get crashed.

Lewko and Waters [4] invented Decentralized Cipher Policy Attribute Based Encryption (DCP-ABE) approach which reduces the dependency on the central authority. In this scheme multiple authorities work independently and it doesn't need any central power. Then later DCP-ABE concept is extended into Decentralized Cipher Policy Attribute Based Encryption with Mediator (DCP-ABE-M) [5], in which the security is increased by using mediator. In this proposed scheme in order to strengthen the security, salt method is added into DCP-ABE-M scheme. Here the section 2 explains the existing approaches [6] and then it is followed by proposed system in section 3. Section 4 and 5 contains implementation and then conclusion.

II. LITERATURE SURVEY

A. IBE

A random oracle model based, Identity Based Encryption (IBE) scheme [7] was the initial scheme which is proposed by Boneh and Franklin. Then by using standard model, IBE is further extended [8][19]. In 1998, an alternative to traditional public key encryption technique is found by Shamir, which is named as IBE [10]. The original motivation of IBE is simplification of certificate management in email system. In this scheme PKG is used which provides the public and private keys to users. Here the users own identity such as phone number; email id is used as public key. In this scheme, for encryption latter identity is sufficient instead of certificates. The major limitation of this system is it doesn't support one to many communications, the originator must gain the public key of the acknowledger and require more storage space.

B. ABE

The first ABE (Attribute Based Encryption) scheme [11] was introduced by Sahai and Waters. In this scheme, a set of user attributes will be attached with the cipher text and secret key. These users attribute will be used as the public key. Further in 2005, Fuzzy Identity Based Encryption is introduced by Sahai and Waters. FIBE (Fuzzy Identity Based Encryption) scheme allows multicast communication. ABE is the one of an application of Fuzzy IBE and it enables multicasting. In this scheme, the data is encrypted in such a way that, any user can decrypt the data if he has a certain set of matching attributes. That is the data can be decrypted, if and only if the acknowledger have some attributes which matches with the senders attribute. There are two types of ABE: KP-ABE (Key Policy ABE) and CP-ABE (Cipher Policy ABE) [12][13][14] which is given by Goyal Pandey, Sahai and Waters. Central power is the major drawback of this system. Since the central power control overall system, any damage to central power will affect the entire system.

C. MABE

Lin et al [15][16] had proposed the standard model of Multiple Authority Cipher Policy ABE (MACP-ABE). Further, it is extended into a new scheme Multiple Authority ABE (MABE) by Chase [3]. The main advantage of this scheme is collusion resistance. In this scheme [3] a central authority is used for the initialization purpose which control and maintain all other multiple authorities. These multiple authorities generate sub secret keys by using the user attributes and the main secret key is generated by combining these sub keys. But the limitation of this scheme is central authority dependency and collusion occurrence. This problem is solved in [17] which is proposed by Sahai and Waters.

D. DCP ABE

Privacy Preserving Decentralized Cipher Text Policy Attribute Based Encryption (PPDCP-ABE) [18][19] is constructed based on the standard model. The previously existing DCP ABE [4] is constructed on the basis of random oracle model. DCP-ABE (Decentralized Cipher Text Policy Attribute Based Encryption) scheme [20] is introduced by Jinguang and Willy Sasilo, in which central authority is not required. In this scheme multiple authorities are placed in a decentralized environment, which generates secret keys for the users without knowing Global ID (GID) and user attributes. Anonymous credential system is used here to convince each authority that the user attributes and GID are monitored by himself, but in actual nothing is shared with the authorities. These independed authorities can join or leave the system at any time without affecting the remaining authorities. Here a central power is not required for the system initialization. Multiple authorities generates multiple sub secret keys and these sub keys are combined together to generate main secret key.

E. DCP-ABE-M

The privacy and security of previously existing DCP-ABE scheme can be strengthened by adding mediator concept in it. In DCP-ABE-M [5] scheme, multiple authorities are placed in a decentralized environment with multiple mediators. In this scheme both the user and data attributes are used for secret key generation, instead of using only user attributes as in previous methods. The user attribute leak problem can be solved by using combination of user and data attributes of the user. By using these attributes secret key is generated, this secret key is divided into two: one part of secret key will be stored in the authority table of authority and another part will be stored in the mirror table of mediator. In this way, the complete secret key will not be stored anywhere in the system. In this scheme, for each user a temporary DB will be allocated for temporary data storage. After the processing this DB will be deleted to erase everything permanently. Thus the mediator increases the security level of this scheme than the existing schemes.

III. PROPOSED SYSTEM

1. SALTING

Salt is a technique which is used to hash passwords by giving additional input to one-way functions. It is a single hash function which mainly focuses on the prevention of rainbow table attack and dictionary attack. Salt is build uniquely for each and every password. The salt value may be of any length and it will be stored in a table. The main aim of adding salt value is, to make the password more strong and unbreakable. In some cases, users may use the same keywords as their passwords. In such cases the system will not be able to provide password security. To solve this problem a unique salt value will be added into the password which makes the password different from other password.

2. SYSTEM ARCHITECTURE AND WORKING

The proposed system has a decentralized environment in which multiple mediators and authorities are placed. Here the multiple authorities generates secret key for the user and multiple mediator are used to store the sub secret key. Each and every authority of this system is independent in nature. In case of any authority failure, the system assigns a new authority instead of the failed one based upon the policy and protocol suit. A secret key is given to the new authority for login in to the system. Here two temporary data bases are allocated for each user; temporary data base for the encryption DB-E and temporary database for decryption DB-D. These DB are used for the temporary data storage of user and then the entire db is deleted after the connection disclose. Salting technique makes the password stronger by adding some value into the password. The system architecture is given below,

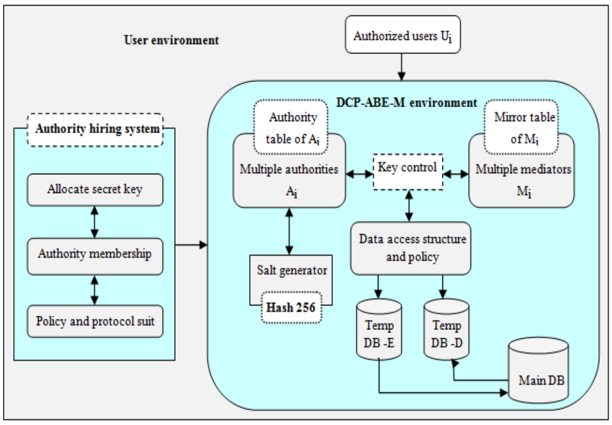

Figure 1. DCP-ABE-M-S system architecture

Encryption

User authentification can be done by using user attribute set A_u and data attribute set A_d. When the user enters into the system, attribute verification is done initially. Here a_1, a_2 ....a_n describes user attributes and d_1, d_2 ....d_n describes data attributes [21]. When these attribute sets are merged together, it forms a main attribute set A_m . Here X is a variable which is an element of A_m as well as $A_u \cup A_d$.

$A_u = \{ a_1, a_2 \,........ a_n \}$
$A_d = \{ d_1, d_2 \,........ d_n \}$
$A_m \supseteq \{ A_u \cup A_d \} \Rightarrow \{ a_1, a_2 \,........ a_n , d_1, d_2 \,........ d_n \}$
$\forall X \{X \in A_m \rightarrow X \in (A_u \cup A_d)\}$

K_e indicates encryption key which is generated by authority, using main attribute set. Here A_{uk} describes user attribute key and A_{dk} describes user data attribute key.

$K_e = \sum (A_u, A_d)_k$

$K_e = \sum (A_{uk}, A_{dk})$

$K_e = A_{uk} + A_{dk}$

K_e is generated by using main attribute set and then salt is added into the available key. Then the available secret key is divided into two A_{uk}, A_{dk}. By combing user attribute key and user data attribute key, main attribute key is generated.

$A_{uk} + A_{dk} \Rightarrow A_{mk}$
$\forall X \{X \in A_{mk} \veebar X \in (A_{uk} + A_{dk})\}$

$K_e = \{\forall X \{X \in A_m \rightarrow X \in (A_u \cup A_d)\}\}_k$

$K_e = \forall X \{X \in A_{mk} \rightarrow X \in (A_{uk} \cup A_{dk})\}$

$K_e = A_{mk}$

$K_e = (A_{uk} \cup A_{dk}) \veebar A_{mk}$

$K_e = (\neg (A_{uk} \cup A_{dk}) \oplus A_{mk}))\vee((A_{uk} \cup A_{dk}) \oplus \neg A_{mk})$

$K_e = \sum (A_{mk} , S_v)$

After generating main attribute key , salt value S_v is added into the available key to generate more strong secret key K_s. SHA 256 (Secure Hash Algorithm 256) is an algorithm which generates hash for the secret key. Generated hash will be of fixed size of 256 bit and unique. It can't be decrypted because hash is a one way function.

$K_e = A_{mk} + S_v$
Hash = SHA 256 ($A_{mk} + S_v$)
Verifier = S_v + Hash ($A_{mk} + S_v$)

$K_e = A_{mk} + S_v \rightarrow K_s$

$K_e = K_s$

K_s indicates secret key which will be divided into two: K_m mediator key and K_a authority key. Where mediator key [22] will be stored in mirror table M_t and authority key will be stored in authority table A_t .
$K_s = K_m + K_a$
$\sum (K_m , K_a) \rightarrow K_s$
$K_m + K_a \rightarrow K_s$

$M_t \rightarrow K_m$, $A_t \rightarrow K_a$

The following flow chart shows the encryption process

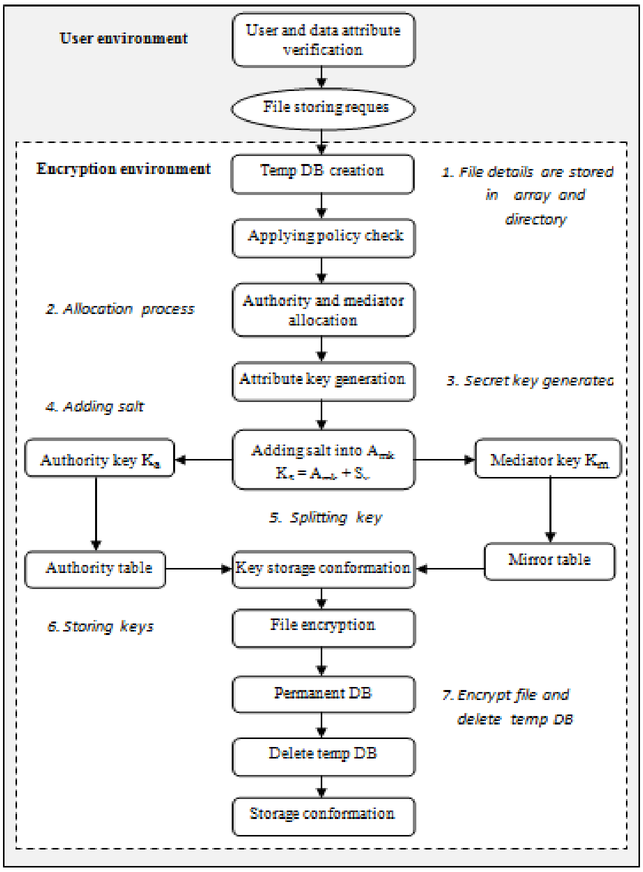

Figure 2. Encryption chart

Decryption

A_{mv} specifies verifiers main attribute set , which is a combination of verifiers user attribute A_{vu} and verifiers data attribute A_{vd} . By using attribute set, system verifies the data requesting user.

$A_{mv} \supseteq (A_{vu} \cup A_{vd})$

Then $A_{mv} \subseteq A_{mu}$

$\forall X \{X \in A_{mv} \rightarrow X \in A_{mu}\}$

The data access is granted to verifier if and only if there is a match between the user attribute, data attribute and verifier attribute, verifier data attribute. If there is no match between the attributes of two users then access is denied.

$$\left.\begin{array}{l} A_{vu} \subseteq A_u \\ A_{vd} \subseteq A_d \end{array}\right\} \longrightarrow \text{Access granted}$$

$$\left.\begin{array}{l} A_{vu} \neq A_u \\ A_{vd} \neq A_d \end{array}\right\} \longrightarrow \text{Access denied, } A_{mv} \neq A_{mu}$$

The decryption key K_d can be generated by combining K_m and K_a, Without finding salt value it is not possible to get the decryption key.
$K_m + K_a \rightarrow K_d$

$$(K_m + K_a) \oplus A_{mk} \rightarrow \neg K_s$$

$$(\neg (K_m + K_a) \oplus A_{mk}) \vee ((K_m + K_a) \oplus \neg A_{mk}) = K_s$$

$$S_v \oplus A_{mk} \Rightarrow \neg K_s$$

$$(\neg S_v \oplus A_{mk}) \vee (S_v \oplus \neg A_{mk}) \Rightarrow K_s$$

$$K_d = A_{mk} + S_v$$

$$K_d = K_s$$

$$K_s = K_e$$

$$K_e = K_d$$

The following flow chart shows the decryption process

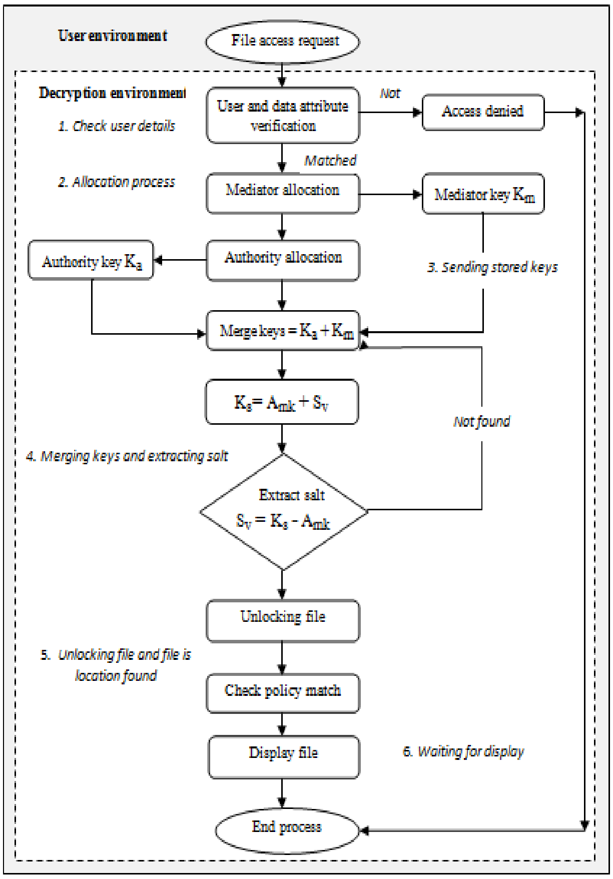

Figure 3. Decryption chart

IV. CONCLUSION

To enhance the security level, the previously existing cryptographic techniques such as attribute based encryption, cipher text are not sufficient. The proposed system improves the level of security by increasing the level of encryption. Here both the user and data attributes are utilized in secret key generation which avoids user attribute leak problem. To make the secret key more strong and unbreakable, salt method is added into DCP-ABE-M. So that, it will be difficult for an attacker to break the system. Since the entire secret key is not stored anywhere in the system, it will be difficult for an attacker to get the entire secret key. Hence the proposed system is more efficient and has unbreakable security than the previously existing schemes.

V. REFERENCES

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494. Heidelberg, Germany: Springer-Verlag, 2005, pp. 457–473.

[2] M. Chase and S. S. Chow, “Improving privacy and security in multiauthority attribute-based encryption,” in Proc. 16th ACM Conf. CCS, 2009, pp. 121–130.

[3] M. Chase, “Multi-authority attribute based encryption,” in Theory of Cryptography 2007, (Lecture Notes in Computer Science), vol. 4392. Heidelberg, Germany: Springer-Verlag, pp. 515– 534.

[4] A. Lewko and B. Waters, “Decentralizing attributebased encryption,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6632. Heid.elberg, Germany: Springer-Verlag, 2011, pp. 568–588.

[5] Varsha Thanaji Mulik, Shinu A, Suraj Rasal. [2016] Privacy Preserving Through Mediator in Decentralized Ciphertext policy Attribute Based Encryption, IJRET: International Journal of Research in Engineering and Technology, 05 (06) | June.

[6] Varsha Thanaji Mulik, Shinu A, Suraj Rasal. [2016] A Survey on Improving Privacy and Security in Decentralized Cipher Text-Policy Attribute-Based Encryption, IJAECS: International Journal of Advances in Electronics and Computer Science, vol. 03 (05) | May.

[7] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In CRYPTO, pages213–229, 2001

[8] D. Boneh and X. Boyen. “Secure identity based encryption without random oracles”. In CRYPTO, pages 443-459, 2004.

[9] D. Boneh and X. Boyen. “Efficient selective-id secure identity based encryption without random oracles”. In EUROCRYPT, pages 223 - 238, 2004.

[10] Adi Shamir‖Identity Based Cryptosystems and Signature schemes‖ Departments of applied mathematics, 1998.

[11] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494. Heidelberg, Germany: Springer-Verlag, 2005, pp. 457–473.

[12] J. Herranz, F. Laguillaumie, and C. Ràfols, “Constant size cipher texts in threshold attribute-based encryption,” in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6056. Heidelberg, Germany: Springer-Verlag, 2010, pp. 19–34.

[13] R.Ostrovsky, A. Sahai, and B. Waters, “Attribute based encryption with non-monotonic access structures,” in Proc. 14th ACM Conf. CCS, 2007, pp. 195–203.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. CCS, 2006, pp. 89–98.

[15] H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure threshold multi authority attribute based encryption without a central authority,” in Progress in Cryptology (Lecture Notes in Computer Science), vol. 5365. Heidelberg, Germany: Springer-Verlag, 2008, pp. 426–436. 678 ieee transactions on information forensics and security, vol. 10, no. 3, march 2015.

[16] Kan Yang, student member, ieee, and xiaohua jia, fellow, ieee. (july 2014). expressive, efficient, and revocable data access control

for multi-authority cloud storage. ieee transactions on parallel and distributed systems. vol. 25, no. 7 (1), 1735-1744

[17] J.Bethencourt, A. Sahai, and B. Waters, “Cipher text policy attribute based encryption,” in Proc. IEEE Symp. SP, May 2007, pp. 321–334.

[18] H. Qian, J. Li, and Y. Zhang, “Privacy-preserving decentralized cipher text-policy attribute-based encryption with fully hidden access structure,” in Information and Communications Security (Lecture Notes in Computer Science), vol. 8233. Heidelberg, Germany: Springer-Verlag, 2013, pp. 363–372.

[19] J. Han, W. Susilo, Y. Mu, and J. Yan, “Privacy preserving decentralized key-policy attribute based encryption,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2162, Nov. 2012.

[20] Jinguang han, member, ieee, willy susilo, senior member, ieee, yi mu, senior member, ieee, jianying zhou, and man ho allen au, member, ieee. (march 2015). improving privacy and security in decentralized ciphertext-policy attribute-based encryption. ieee transactions on information forensics and security. vol. 10, no. 3 (1), 665-678.

[21] Suraj Rasal, Karan Saxena ,Sanya Relan. (2016/5). OTP Processing using UABE & DABE with Session Management. *International Journal of Advanced Research in Computer Science and Software Engineering*. 6 (5), 57-59.

[22] Varsha S Rasal, Suraj U Rasal, Shraddha T Shelar. (2016/10). ENHANCING PRIVACY AND SECURITY THROUGH MEDIATOR USING DCP-ABE WITH OTP. *IIOAB-Institute of Integrative Omics and Applied Biotechnology* . 7 (1), 277-283.