ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Review Paper on Enhancing Flexibility for ABE through the Use of Cipher Policy Scheme with Multiple Mediators

Ms. Sartale Mrinalini.*, Prof. Tidake Bharat
*Student Pursuing M.E. in Computer Networks from FIT,Khopi,Pune, India
P.G. Co-ordinator at Department of Computer Engineering, FIT,Khopi,Pune, India

Abstract

Traditional cryptography system shares the keys between senders and receivers for encryption and decryption purpose to achieve the data security, where these key sharing was done through the certificate exchange and signature storage. But it did not scale well as number of users get increased key distribution and signature storage was the great challenge. To overcome this problem of traditional cryptography system Identity Based Encryption has been proposed, where instead of IDs itself were used for encryption, which again leads to the limitation of only one-to-one communication was possible. To solve this problem multicast communication can be made possible through the Attribute Based Encryption. Single mediator and key policy ABE was used, which was not so efficient and failed for providing revocation. So MAMM concept with CP-ABE was proposed which gives more security by multiple encryptions through hierarchical mediators. This system can be extended for the distributed system, where more security can be given to the data by using MAMM with CP-ABE in distributed environment.

Keywords: Cipher-text, Attributes, Multi-Auhtority, Multiple Mediators, Distributed Cipher-text police.

Introduction

In today's world of computer data privacy is important issue. Traditional cryptography provides the data security through the encryption and decryption using certificates which binds user's keys. Identity Based Encryption was proposed by Shamir[1] where ids(example: email id, name) are used instead of using the certificates. To overcome the limitation of one-to-one communication of IBE Fuzzy IBE[4] have been proposed which then leads for another system as Attribute based encryption (ABE). So multicast communication can be possible as number of users can decrypt the data if they have appropriate attributes. Access control to be maintained for user's by the single authority. But for more scalability there is a challenge of multi-authority. Multi-Authority Attribute Based Encryption[13] has used Cipher – policy based encryption cryptography technique. Dynamic level of access was maintained by using the key "Revocation" which manages the attributes and keys. For maintaining the access control through revocation in multi authority system Multi Authority Single Mediator concept was proposed. To achieve the more security the single mediator system was extended to the multi mediator system. Lots of encryption techniques were proposed and implemented still there is research problem of improved encryption technique.

Problem definition

To make the encryption system more flexible by using multi authority. And to give the more security to the data by multiple encryptions through multiple mediators. To make possible this for Multi-Authority Multi-Mediator system in distributed version of Ciphertext Policy ABE. To make the distributed environment more secure, efficient and applicable and to maintain the access control.

Perspective solution

As the existing system is not applicable for distributed environment. The Multi-Authority Multi-Mediator concept can be implemented for distributed version of CP-ABE.

Related work and literature survey

Identity Based Encryption:-

Shamir[1] has suggested the technique for simplifying certificate management in e-mail systems. If Alice wants to send mail to Bob at bob@job.com then encryption can be done by using bob@job.com as a public key. There is no requirement of checking the public key certificate of the bob to Alice. Bob can decrypt that mail by taking the private key from PKG by authenticating himself to PKG. For the implementation of this technique Shamir has proposed several IBE schemes. But none of the techniques were efficient. So Dan Boneh and Matthew Franklin

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

proposed the fully functional identity-based encryption scheme. The proposed technique was based on computational Diffie-Hellman assumption. To make the master-key more secure, master key is distributed. So robustness of PKG is achieved. This IBE system uses bilinear map as e:G1*G1 G2, where G1 and G2 are two groups. Boneh et al.[3] used Weil pairing on elliptic curves as such a map. This technique of IBE is application in several cases. The public key revocation can be achieved. The certificates contain the field of expiration date. Like that IBE done this by Alice encrypt the mail which is sent to Bob by using his public key and expiration date field is added there as bob@job.com||current _date. Another application is user credentials can be managed by simply adding one more field of credential. Delegation of decryption keys is also possible in IBE. Delegation example can be as: delegation to a laptop. If Alice encrypts mail to Bob by using the current date for the encryption key, Then instead of keeping master key, Bob can simply keep the keys of some days on his laptop if he will not be there for decryption. So master key will not be compromised. Identity based encryption scheme consists of four algorithms as: Setup, Extract, Encrypt and Decrypt. Where in Setup security and system parameters are decided and master key formation is done. Extract creates private key from parameters, master key and arbitrary ID {0, 1}*. Encrypt converts a message into ciphertext and decryption gives the original message back by Decryption algorithm. Boneh et al. has given the chosen ciphertext security for identity-based systems. This chosen ciphertext security has used the random oracle model. IBE has the limitation as it is only applicable for one-to-one communication. To overcome this problem Amit Sahai and Brent Waters introduced a technique Fuzzy IBE. Another limitation of Boneh et al. is it uses random oracle model.

Fuzzy Identity Based Encryption:-Amit Sahai and Brent Waters[4] has introduced another type of IBE which is nothing but Fuzzy IBE. It does not use random oracle model for it's construction and avoids this limitation of IBE.In Fuzzy IBE, identities are set of descriptive attributes instead of string of characters. If user have the secret key for the identity x then he can decrypt the encrypted ciphertext with x' public key, where x and x' should be within certain distance of each other. So certain amount of error tolerance is tolerated in this system.

Fuzzy IBE has two applications. IBE using biometric identities is one of them. Here the identity is formed by attributes which are biometrics of user. So encryption is done using biometric identity. It has the advantage as when one want his private key for decryption, he has to authenticate to the authority by presenting supplementary documents or credentials. These documents could be subject to forgery. So instead of these documents biometric gives clear identities of a user for verification. Another application of Fuzzy IBE is attribute based encryption. Here the encrypted data is for all the users having certain set of attributes. So number of users can decrypt the data if they have the matching attributes. Amit Sahai and Brent Waters have given the security against collusion attack, so group of users can not combine their keys to decrypt the data if they are unable to decrypt it alone.

For implementation of Fuzzy IBE group of bilinear group was required, where bilinear map is required for the pairing of elements. So another approach was proposed by V. Miller [5] in 1985 to use the elliptic curves which had removed the problems Diffie-Hellman or EIGamal like of traditional systems. Implementing and managing for single authority attributes was easy between the users and providers. But single authority system had limitations as it was not scalable, efficient and not applicable. So it this open problem was proposed by M. Pirretti [16], by Shucheng Yu [17], by V. Goyal [18]. So multi-authority system should be used, but managing the security in multi-authority was challenging. This problem was solved by Melissa Chase [13] in 2007.

Multi Authority Based Encryption:-
In single authority attribute based encryption only one authority was responsible to manage all the attributes, where multi authority based encryption[13] portioned the universe of attributes in some disjoint sets. So sender specifies the X attributes to each authority, which will be monitored by that authority. So to decrypt the message user must have fX attributes from each and every authority. The problem of collision of authorities was solved by Sahani and Water. Suppose for decryption of one ciphertext, attributes from authority 'a' and authority 'b' are required. If 'A' has all the needed attributes from authority 'a' and 'B' has all the needed attributes from authority 'b', still they should not be able to combine their individual keys for decryption. To achieve this concept the GID technique was used, where GID was global identifier so one user can not argue on another user's identifier. All

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

authorities checks the GID of each user. By using this technique collision can be avoided. To maintain the secrecy secret keys provided were easily re-randomized in single authority. But in multi authority based encryption the secrets were divided among multiple authorities. So to maintain the secrecy each authority acts as PRF, which is nothing but pseudorandom function. It randomizes the secret keys given out. Although the secret keys for each user appeared completely random they were derived deterministically. So for the key generation the PRF was computed on the user's GID and then the computed result was used as a secret key. Here uniqueness of outputs of PRFs were maintained at each user. By using the PRF along with GID each authority works independently and the collision is impossible. But as the users are dynamic, their key updation to maintain the access control was important.

MASM:-
To achieve the better access control Boneh and Franklin was first suggested the concept called as "Revocation" over IBE which has used expiration date in keys. Proxy re-encryption technique was in CP-ABE where proxy servers were used. But there was a problem regarding to the proxy servers that the servers can be dishonest. Also these servers could be compromised. This problem was partially solved in 2011, where proxy re-keying concept was proposed. But the problem of inefficiency and non scalability was still there. So to overcome these problems Riddhi Mankad[23] in 2012 proposed the system where multi authority encryption technique was combined with revocation concept. For this technique one mediator was responsible for partial decryption. If the match for GID not found at mediator or it was revoked then mediator returns null.

MAMM:-
To achieve more security the approach of multiple mediators with multiple authority was proposed in 2014[26], where final data can be extracted through the number of decryptions by number of mediators. So the data was highly secure. As previous scheme has provided facility for static data environment, multi-mediator has given the facility for dynamic data environment. After the authorities setup the data can be encrypted by number of mediator's collaboration. And at the decryption side the data would be partially decrypted by multiple mediators and then fully by the user.

Proposed work
Multi-Authority Multiple Mediator system gives more flexibility to Attribute Based Encryption and more data security. These features can be extended for the distributed version of Cipher-text Policy Attribute Based Encryption. So the proposed work is to enhance the flexibility in distributed environment for Attribute Based Encryption through the use of Cipher Policy by using multiple mediators. By this distributed environment can be made more secure. And the efficiency, scalability and applicability will be enhanced.

Scope of work
Proposed technique extends the MAMM technique for the distributed version of cipher policy ABE. So it will enhance the flexibility for distributed system. This work can be extended for cloud system. So the security and efficiency of data security in cloud system can be increased. For more security multiple mediators can be used in cloud system also with multi-authority and CP-ABE techniques.

Conclusion
On the basis of existing techniques Literature survey is done and they give an idea that there are still some limitations in it. MAMM system was implemented for more security which can be possibly extended using distributed version of CP-ABE. So all these techniques give an idea that there is more scope in encryption techniques for the distributed systems and can be extended in the area of cloud computing.

References
1. Adi Shamir, "Identity Based Cryptosystems and Signature schemes" Department of Applied mathematics, 1998.
2. Alexandra Boldyreva∗,Vipul Goyal, "Identity-based Encryption with Efficient Revocation" .2008.
3. D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing". In CRYPTO, pages 213–229, 2001.
4. A. Sahai and B.Waters, "Fuzzy identity based encryption," Advances in Cryptology Eurocrypt,LNCS, Springer, vol. 3494, pp. 457–473, 2005.
5. V. Miller,"Use of elliptic curves in cryptography". In H. Williams, editor, Advancesin Cryptology — CRYPTO'85, volume 218 of Lecture Notes in Computer. Sci., pages417–428. Springer, 1986.
6. Antoine Joux,"The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems". Lecture Notes in Computer Science,Edited by G. Goos, J. Hartmanis, and J. van Leeuwen.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

7. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weilpairing". In C. Boyd, editor, Proceedings of ASIACRYPT'2001, volume 2248 of Lecture Notesin Computer. Sci., pages 514–532. Springer, 2001.
8. P. Barreto, H. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing basedcryptosystems. Cryptology 2002.Number 2002/008.
9. G. Frey, M. Muller, and H.-G. Ruck, "The Tate pairing and the discrete logarithmapplied to elliptic curve cryptosystems". IEEE Transactions on Information Theory,45(5):1717–1718, 1999.
10. S. D. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate pairing". Volume, 2002.
11. Piyi Yang, Zhenfu Cao and Xiaolei Dong, "Fuzzy identity based signature," Available at http://eprint.iacr.org/2008/002, 2008.
12. Allison Lewko and Brent Waters, "Decentralizing attribute-based encryption," K.G. Paterson(Ed.): Eurocrypt 2011, LNCS, vol. 6632, pp. 568–588, 2011.
13. Chase, M.: "Multi-authority attribute-based encryption". The Fourth Theory Of cryptography Conference (TCC 2007), LNCS. 4392, 513{534 (2007).
14. Waters,B.: "Ciphertext policy attribute based encryption an expressive, Efficient,and provably secure realization". PKC 2011, LNCS, Springer Heidelberg. 6571, (2011)
15. Luan, I., Milan, P., Svetla, N., Pieter, H., Willem, J.: Mediated ciphertext Policyattribute-based encryption and its application. WISA 2009, LNCS, Springers, Ver- lag. 5932, 309{323 (2009)
16. Pirretti, M., Traynor, P, McDaniel, P, Waters,B.: "Secure attribute-based Systems". ACM CCS'06. 6377, 111{118 (2006).
17. Shucheng, Yu, CongWang, Kui, R., and Wenjing,Lou:"Attribute based data Sharing with attribute revocation". ASIACCS10. (2010).
18. Alexandra, B., Vipul, G., Virendra, K.: "Identity-based encryption with Efficient revocation". CCS. (2008).
19. Melissa chase "Multi-authority Attribute Based Encryption", Computer Science Department Brown University Providence, RI 02912.
20. V.Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute based encryption for fine Grained access control of encrypted data." ACM Conference on Computer and Communications Security, pp. 88–98, 2006.
21. Bethencourt John, Sahai Amit, Waters Brent, "Ciphertext-policy attribute-Based encryption," IEEE Symposium on Security and Privacy, pp. 321–334, 2007.
22. Sonia Jahid, Prateek Mittal,Nikita Borisov, "Easier: Encryption-based access Control in social networks with efficient revocation," ASIACCS11, March 2011.
23. Riddhi mankad, Devesh Jinwala "Investigating multi authority attribute based Encryption with revocation", NIT Surat, 2012
24. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for Designing efficient protocols. InACM conference on Computer and Communications Security (ACM CCS), pages 62{73, 1993.
25. Vipul Goyal," Reducing Trust in the PKG in Identity BasedCryptosystems" Department of Computer Science, University of California,Los Angeles, CRYPTO 2007, LNCS 4622, pp. 430–447, 2007.
26. Rasal Shraddha* and Tidke Bharat, "Enhancing Flexibility for ABE through the Use of Cipher Policy Scheme with Multiple Mediators" Department of Computer Science, Pune University, Maharashtra, India rasalshraddha@hotmail.com © Springer International Publishing Switzerland 2015