ISSN: 0975- 3583, 0976-2833 VOL 10, ISSUE 01, 2019

Improving Revocation Scheme in Cloud Storage using Multi-Authority ABE

DR. KOPPARTHI SURESH[1]
[1]Professor & Principal, Bhimavaram Institute of Engineering and Technology, Bhimavaram, AP, India,
E-mail: sureshkgrl@gmail.com.

Abstract: Traditional system in cryptography allows just sharing of keys between the sender and receiver, for such a technique only the signature storage is provided for the user's public key. But as the number of users increases, it's became a challenging job to have such a certificate storage as well as key distribution, to overcome this Identity Based Encryption (IBE) was proposed, but again it had created the time consuming environment as it was supporting only to one-to-one communication. After IBE Attribute Based encryption (ABE) made possibility to provide multicast communication between users but it was limited to only key policy based encryption as well as could not provide the revocation phenomenon for keys. So this paper aims to develop an existing system using MAMM (Multiple Authority Multiple Mediator) with the use of distributed CP-ABE(Cipher Policy ABE) which enhances the revocation and improves the performance.

Keywords: Cipher-text, Distributed Cipher-text policy, Encryption, Multi-Authority, Multi-Authority Single Mediator.

INTRODUCTION

Data privacy is the most important feature in today's computer world. In traditional system, data security had done through encryption and decryption using certificates that binds user's keys. Shamir[1] proposed new concept of Identity Based Encryption (IBE) where instead of using the certificates, he had used the user's own id (example: SelfID).To provide an encryption in multicast manner, Fuzzy IBE[3] have been proposed that leads to an Attribute based encryption (ABE), that could encrypts the document for all the users having set of attributes. The level of access control has been maintained for users as well, these all were carried out by single authority. When the numbers of users were huge, multi-authority had a challenging for doing such work. Multi-Authority Attribute Based Encryption had proposed where services provided were almost for distributed system so, Cipher–policy based encryption technique of cryptography was used. The management of all these attributes/keys was done through the concept called Revocation‖ which basically proves the expiration for using the level of access that maintains the higher level of data privacy in encryption. Many solutions were proposed and implemented on revocation as well. The existing work extends to make improvement in revocation techniques. IBE scheme was proposed first to eliminate the certificate storage, where as Attribute Base Encryption proposed new security technology that motivates to survey on best encryption techniques for leveled data privacy. Existing work contains problems of using cipher-text Policy Attribute-Based Encryption (CP-ABE) which allows encrypting data under an access policy, specified as a logical combination of attributes. Such cipher-texts can be decrypted by anyone with a set of attributes that fits the policy. This work can be extended using distributed policy along with multiple mediators Further Section 2 consists literature survey followed by research methodology in Section 3 and Section 4 consists implementation details then conclusion.

RELATED WORK

A. Identity Based Encryption

Shamir [1] proposed a new concept called as an Identity Based Encryption (IBE) in 1998 where the practical implementation was done in 2001.He had simplified an issue of certificate storage. The scheme was an ideal for the closed group of users such as multinational companies, large banks since the headquarters of the corporation can serve as key generation centers. An Identity-based encryption (IBE) is an exciting alternative to public-key encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI). The senders using an IBE do not necessarily look up for the public keys and the corresponding certificates of the receivers, the identities (e.g. emails or Self ID) of the latter are sufficient to encrypt. This scheme had created a transparent environment to the users, when Alice sends mail to Bob at bob@lab.comshe just encrypts her message using the public key string\bob@lab.com". There is no need for Alice to obtain Bob's public key certificate. When Bob receives the encrypted mail he contacts with Private Key Generator (PKG) which is the third party. Bob authenticates himself to the PKG and obtains his private key from the PKG. Bob can then read his e-mail. Unlike the existing secure e-mail infrastructure, Alice can send encrypted mail to Bob even if Bob has not yet setup his public key certificate. In identity-based e-mail systems the PKG contains Bob's private key [2]. Such a Diffie-Hellman or EIGamal. The possible construction of pairing as bilinear map was carried out from two groups sayG1 and G2.When groups and pairings are clearly decided then for showing it (P, Q) are used. Pairings used was nice idea that solved the difficulties of discrete algorithm and rules out the simpler bilinear map for cryptosystem. The group G1 is selected as points on elliptic curves over function Fq. The order of G1 was chosen as prime l. When l=q, there exist anadaptive pairing that sends G1 to the additive group G2 = (Fq,+). For such a pairing a key parameter is used which is called as security parameter. When this r (security parameter) was small, the pairing was computed efficiently [6].

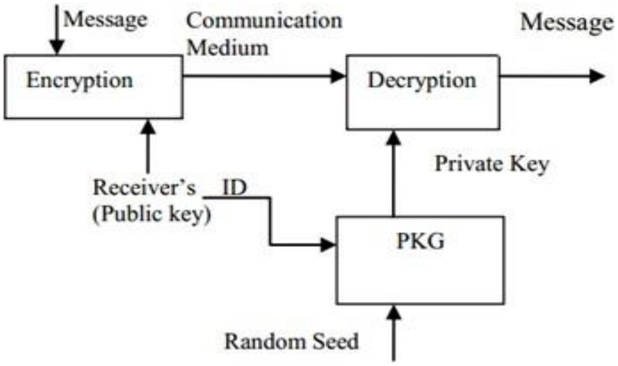

Fig.1. Identity Based Encryption [1].

Fig.1 shown below gives the basic view of an Identity Based Encryption. The message is encrypted under the key, transmitted as cipher-text through the exposed channel, and decrypted under the key. The choice of keys is based on truly random variable say k. The encryption key is the user's identity and the decryption key is derived. So here unlike traditional system the separate key channel between users was eliminated, and is replaced by a single interaction with key generation center when the recipient first joins the network[2]. Shamir implemented a way to provide the more secure system through IBE. An identity-based encryption scheme E specified is used. IBE in other way have some limitations which didn't make fully satisfactory work in Encryption of message as it is only limited for one to one communication to provide error tolerance property, new approach is proposed by Sanahi and Waters in 2005 called Fuzzy Identity Based Encryption (FIBE).

B. Fuzzy Identity Based Encryption

Multicast communication was possible concept proposed (FIBE) by Sahani [3] from IBE which had to two exciting applications. The first was an IBE that used biometric identities and second it could be used for multicast communication. In fuzzy IBE [3][4] identity of a user is viewed as a set of attributes. The name ―attributes‖ given such that numbers of attributes for each user are located so as to maintain the access level. It had given an idea that how an IBE system encrypts to multiple hierarchical-identities in a collusion-resistant manner implies a forward secure Hierarchical IBE scheme, e.g. {company, division, department}. It has shown that how their techniques for resisting collusion attacks were useful in attribute-based encryption. Fuzzy IBE was based on the set of attributes for which the implementation of group of bilinear group was required. Now as group structure was required for the pairing of elements which is a bilinear map [10], the better option forthis was proposed by V. Miller [5] in 1985 that is the use of elliptic curves which had an arithmetic structure as well as it is better to fit for solving the problems of traditional system.

Problem occurred when the value became large [3][7]. Two pairings types are defined on elliptic curves that are Weil pairing and Tate pairing. At some value of r Weil pairing was unable to reach the optimum value. On the other hand Tate pairing was used that provided an optimum solution as well has had less cost. For this reason, Frey, Muller and Ruck[8][9][10]proposed in to use it as a replacement for the Weil pairing. Hence the construction of pairing is done as bilinear map on elliptic curve to select a set of attributes. The preliminaries regarding to the security parameter used on elliptic curve for proper pairing as bilinear map, the multicast communication is possibly carried outthrough the set of attributes for users hence as variant to the Fuzzy IBE further leads to more advanced Attribute based IBE. For the set of attributes for user, an authority was required in any ways to make the management between the attributes a single authority attributes or multi authority attributes was used depending on the data. Single authority attributes can be easily managed between the users and providers [14][15] but the single authority had some problems such as inefficiency, non scalability and non applicability which were the open problems proposed by M. Pirretti [16], by Shucheng Yu [17],by V.Goyal[18] respectively. The most challenging and interesting job was to manage the security for multi-authority attributes as there were many applications which requires multiple authorities. A student registered with courses across multiple departments may have attributes associated with each of these departments. Designing a multi-authority ABE scheme was an interesting open problem first proposed by Sahani andWaters in [4] and later solved by Melissa Chase[13] in 2007.

IMPLEMENTATION METHODOLOGY

The encryption/decryption techniques for any informationor message consist of a structure followed by an algorithm. Ithad implemented sequentially followed by algorithmic steps given below [23].

A. Multi-Authority ABE

In [13] ABE scheme is explained. It is given that theuniverse of attributes can be partitioned into K disjoint sets where it is assumed. Each will be monitored by a different authority. It also has one trusted central authority that does not monitor any attributes. Note: In the following we use Au to denote the attribute set of user u and AC to denote the

Improving Revocation Scheme in Cloud Storage using Multi-Authority ABE attribute set of a cipher-text. Aku and Ak C are the attributes handled by authority k in the attribute sets of the user and the cipher-text respectively. A Multi-Authority ABE system is composed of K attribute authorities and one central authority.Each attribute authority is also assigned a value dk. Thesystem uses the following algorithms:

Setup: A randomized algorithm which must be run by some trusted party (e.g. central authority) takes as input the security parameter. Outputs a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key which will be used by the central authority.

Attribute Key Generation: A randomized algorithm run by an attribute authority. Takes as input the authority's secret key, the authority's value dk, a user's GID, and a set of attributes in the authority's domain AkC. (We will assume that the user's claim of these attributes has been verified before this algorithm is run). Output secret key for the user.

Central Key Generation: A randomized algorithm runs by the central authority. Takes as input the master secret key anda user's GID and outputs secret key for the user.

Encryption: A randomized algorithm runs by a sender. Takes as input a set of attributes for each authority, a message, and the system public key outputs the cipher-text.

Decryption: A deterministic algorithm runs by a user. Takes as input a cipher-text, which was encrypted under attribute setAC and decryption keys for an attribute set Au. Outputs amessage m if $|AkC\cap Aku| > dk$for all authorities k. Multi authority along with revocation scheme was implemented whose last step nothing but MASM (Multiple Authority Single Mediator) was proposed by Riddhi Mankad et al [23].

B. MASM

When multi-authority ABE was implemented along with revocation, this scheme was used by [23] as their proposed work in encryption of data where it was consisting of a central authority (TA), multiple authorities and a mediator that was so called as MASM (Multiple Authority Single Mediator). Every authority has its own set of attributes that are independent on other authority attributes. The mathematical form of such scheme is given as follows [23]:

Global Setup: GP, GS: The trusted authority (TA) will choose a bilinear group G of prime order p. Let g be the generator and e(g, g) ->G1 be a bilinear map defined on G1. Let H: {0, 1}*->G be a hash function that maps global identity, GID to a group element and H1: {0, 1}*->G that maps string attribute to a group element. Pick two random exponents α, β R Zp. The TA generates the global public parameters GP = {G, g, (h = gβ),e(g, g)α} and GS = {β , gα }.

The hash functions H,H1 are known only to the authorities. **Authority Setup (GP,Ui)->**PKj, SKj: Each authority ioutputs its own public key , PKj and secret key, SKj. Forattribute jUi, choose random exponent bj ϵRZn , PKj={[H1(j)]bj,gbj}

SKj={bj}

UserKeyGen(GID,GP, GS)->K0: The trusted authority uses GID and returns the base component of user's(with global Identifier GID)secret key using global secret component GSas below:

K0=g{(α+γ)/β} Where r=H (GID) andrϵZp.

AttributeKeyGen (GID, GP,j,SKj)->Kuj, Kmj: User request for attribute component of secret key for attribute j to respective authority i. This authority makes confirmation about j Uiand computes r=H(GID). Then it chooses aj randomly and makes keys as Kujand Kmjas ,
Kuj= g(r/bj) H1(j)(aj/bj), Kmj = g(aj / bj) Kujgiven to the user and Kmjis given to mediator.

Encrypt (M, T, PKj, GP) ->CT: Using access policy T sender encrypts the message M. It chooses the polynomial qx for each node in access tree having degree dx=tx -1 is the threshold value of node x. It sets the value of root node qR(0)

= s, where sϵRZp and R is root node. The remaining terms of polynomial are randomly chosen to make a polynomial qx of length t. For all other child node say z, it sets qz(0) = qz' where z' is parent node of z and algorithm continues assigning the values of similar fashion in a top down manner
.Let y ϵY be the set of leaf node and let att(y) be a functionthat returns the specific attribute to leaf node y. let j= att(y). It returns cipher text CT as CT={T, C0, C1,Cy,C'y}

M-Decrypt(CT, Kmj, y,GID)->C"y: The mediator takes the cipher text and performs partial decryption using its secret key component and user's (Receiver) GID, provided that the GID is not revoked. If the GID is revoked, then the associated authority needs to issue a new key to the user by performing ReUserKey step as explained. If GID is not revoked, the mediator outputs partially decrypted cipher text C‖y and sends it to the receiver. The mediator will stop issuing to the user if the user is revoked.

$$Cy = e (Cy , Kmj)$$

ReUserKey(newGID,GP)->K0:TA verifies the authenticity of the revoked user and issues a new base component of the secret key to him. Thereafter, the user requests for the attribute component of his secret key K0 from individualauthorities using AttributeKeyGen step.

$$K0= g (\alpha + \gamma \text{ new}) / \beta$$

Where rnew =H(newGID) and rnewϵZp. Thereafter, a user will request attribute component of his secret key by calling Attribute KeyGen function.

u-Decrypt(CT,Kuj,y,C"j)->A: The receiver takes cipher text, along with his secret key Kuj component and partially decrypted cipher-text, recovered from the mediator to compute C‖'y. as

$$C\|'=e(Cy, Kuj), e(Cy,Kuj)/e(C'y,Kmj)$$

Decrypt(CT,K0,A)->M: To retrieve the message M, the receiver needs certificate authority, K0 and A. The receiverd ecrypts message by feeding certificate authority, K0 and A into the decryption function. The decrypt function for this receiver would have failed had he been revoked or his secret key had not satisfied the policy.

$$e(C0,k0)/A = e(h, g(\alpha+\gamma/\beta) /e(g,g)rs$$

To retrieve M, $M= C_1 / e(C_0, K_0)/A=M.e(g,g)as/e(g,g)as=M$ MASM contains single mediator which further

inspires in
making more improvement in Revocation scheme as well as gives an idea about extending it as MAMM (Multiple Authority Multiple Mediator).

C. Key Revocation

Boneh and Franklin [3] was first suggested simpleRevocation‖ concept for IBE in random oracle [21] told about expiration date for keys for maintaining the access control. He had given example about key expiration in IBE such that Alice encrypts e-mail sent to Bob using the public key:
{bob@lab.com|| current-year}. Bob could use his private key during the current year only. Bob requires new private key once a year from the PKG. Alice did not need to obtain a new certificate from Bob every time Bobre freshes his private key. This approach was carried out by encrypting e-mail for Bob using {bob@gmail.com current date}. This forced Bob to obtain a new private key every day. This could be possible in a corporate PKI where the PKG was maintained by the corporation. This approach gives simple

key revocation technique: when Bob leaves the company and his key needs to be revoked, the corporate PKG is instructed to stop issuing private keys for Bob's e-mail address. As a result, Bob could no longer read his email. The interesting property was that Alice did not need to communicate with any third party certificate directory to obtain Bob's daily public key. Hence, identity based encryption was very efficient mechanism for implementing ephemeral public keys. Also this approach enabled Alice to send messages into the future: Bob would only be able to decrypt the e-mail on the date specified by Alice. A simple extension to the discussion above enabled to manage user credentials using the IBE system. Suppose Alice encrypts mail to Bob using the public key:\bob@company. com k current-year k clearance=secret". Then Bob will only be able to read the email if it has specific certified credentials. Appropriately, it is easy to revoke user credentials using the PKG. But PKG [25] was not a proper solution due to causing time consuming process.

Vipul Goyal[3] proposed an IBE scheme with efficient revocation by combining binary tree data structures with FIBE. His techniques were again applicable to only KP-ABE rather than CP-ABE. Another approach towards revocation in CP-ABE was proxy re-encryption technique that made use of the proxy servers [17].The proxy servers could be dishonest or could be compromised and hence the scheme was not very secure. In2011, with the aim of providing encryption based access control in social networks the authors in [22] proposed the concept of proxy re-keying for minimizing the trust on proxy servers to enable efficient revocation. These approaches were limited to revoking a predefined number of attributes also providing the limitation of existing approaches for revocation in ABE includes inefficiency [3][16], non-scalability [17],unreliability and non-applicability to CP- ABE. Furthermore in2012 Riddhi Mankadet al [25] were combined the multi authority scheme with revocation concept where she implemented the combinations of authority and mediator with final combination proposed was MASM [25] (Multi-authority Single Mediator) which eliminated the problem about revocation of previous scheme. It is still unable to problem regarding advanced revocation concepts.

CIPHER-TEXT POLICY ATTRIBUTE BASEDENCRYPTION (CP-ABE)

The logical combination of attributes was used by the traditional CP-ABE (Cipher-text Policy Attribute Based Encryption) scheme. Such cipher-texts can be easily decrypted by anyone as set of attributes that fits the policy. This overall survey up to Multi-authority attribute based Encryption along with Revocation mainly focused on combining the Multi Authority attribute scheme with revocation. But as it was first model proving combined scheme and hence includes some problems regarding the improvement in revocation techniques due to the use of single mediator. Distributed version of CPABE (DABE) scheme allows to extend this single mediator scheme to multiple mediator (Multiple Authority Multiple Mediator) so that the problem of mediator compromising is avoided. The multiple parties are responsible to keep the track of number of arbitrary secrets keys. Distribute CP-ABE contains such multiple attribute authorities to distribute secret keys. So, algorithm for such a scheme is possibly used in multiple mediator which gives basic mathematical steps as is given below.

Setup: The initial step gives global setup to produce thePkand Mk as an output.

CreateUser (Pk,Mk,u): This function takes input from global setup as Pk, Mk and user name u and outputs the public user key PKu which is used by the attribute authoritiesto issue the secret attribute key for u SKu. This key is used todecrypt the cipher-texts.

CreateAuthority(Pk,a): This is executed by attribute authority with identifier a and creates secret authority key Ska.

RequestAttributePk(Pk,A, SKa): This provides the public attribute key when attribute authorities executed the request by checking the condition as whether A equals a and generates the key PKA otherwise outputs NULL.

RequestAttrbuteSK(Pk,A,Ska,u,Pku): This step check all the conditions of above step and additionally checks whether user u with public key PKu is eligible of attribute A. If condition is true then this step outputs SKA ,u for user u otherwise the algorithm outputs NULL.

Improving Revocation Scheme in Cloud Storage using Multi-Authority ABE

Encrypt(Pk,M,A,Pka1,PkAN): This step takes an input Pk, M, access policy A, Pk and public keys PKA1, , PK An and generates the output as cipher-text CT.

Decrypt: This step takes input as SKu, SKA1,u,...., SK Anand generates output M.

CONCLUSION AND FUTURE SCOPE

Literature survey is done based on existing techniques and their implementation which gives an idea that there are still limitations in existing system. This paper shows that algorithm for MASM is implemented which further gives possible construction for MAMM (Multiple Authority Multiple Mediator).Also it can be possibly implemented using distributed version of CP-ABE. So all these approaches gives idea about more scope in encryption techniques under the distributed environment which provides a brief knowledge about future work in the same to enhance the revocation and improves the performance specifically in the area of cloud computing.

REFERENCES

[1] AdiShamir,‖Identity Based Cryptosystems andSignatureschemes‖ Departments of appliedmathematics, 1998.

[2] Alexandra Boldyreva,VipulGoyal, Identity-basedEncryption with Efficient Revocation‖,2008.

[3] D. Boneh and M.K Franklin, ―Identity-basedencryptionfrom the weil pairing‖. CRYPTO, pages 213–229, 2001.

[4]Sahai and B.Waters, Fuzzy identity based encryption,Advances in Cryptology Eu-rocrypt,LNCS, Springer, vol.3494, pp. 457–473, 2005.

[5] V. Miller, ―Use of elliptic curves in cryptography‖.In H.Williams, editor, Advances in Cryptology—CRYPTO'85, volume 218 of Lecture Notes inComputer. Sci., pages 417–428. Springer, 1986.

[6] Antoine Joux, The Weil and Tate Pairings asBuilding Blocks for Public Key Cryptosystems‖.Computer Science, Edited by G. Goos, J. Hartmanis,and J. van Leeuwen.

[7] Boneh, B. Lynn, and H. Shacham, ―Short signatures from the Weil pairing‖. In C. Boyd, editor,Proceedings of ASIACRYPT'2001, volume 2248 ofLecture Notes in Computer. Sci., pages 514–532.Springer, 2001.

[8]P.Barreto, H. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing based cryptosystems.Cryptology 2002.Number 2002/008.

[9]G. Frey, M. Muller, and H.-G. Ruck, ―The Tatepairing and the discrete logarithm applied to ellipticcurve cryptosystems‖. IEEE Transactions onInformation Theory, 45(5):1717–1718, 1999.

[10] S. D. Galbraith, K. Harrison, and D. Soldera, Implementing the Tate pairing‖. Springer-Verlag,2002.

[11]Piyi Yang, Zhenfu Cao and Xiaolei Dong, ―Fuzzy identity based signature,‖ 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-basedencryption‖. The Fourth Theory Of cryptography

ISSN: 0975- 3583, 0976-2833 VOL 10, ISSUE 01, 2019

Conference (TCC 2007), LNCS.4392,513{534(2007).

[14] Waters, B.:Cipher-text policy attribute based encryption an expressive, Efficient, and provablysecure realization‖. PKC 2011, LNCS, SpringerHeidelberg.6571, (2011).

[15] Luan, I., Milan, P., Svetla, N., Pieter, H., Willem, J.:Mediated cipher-text Policy attribute-basedencryption 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, Cong Wang, Kui, R., and Wenjing,Lou: ―Attribute based data Sharing with attributerevocation‖. ASIACCS10. (2010).

[18]Alexandra, B., Vipul, G., Virendra, K.: Identity basedencryption with Efficient revocation‖. CCS.(2008).

[19] Melissa chase―Multi-authority AttributeBasedEncryption‖, Computer Science Department Brown UniversityProvidence, RI 02912.

[20]V. Goyal, O. Pandey, A. Sahai, B. Waters,―Attribute based encryption for fine Grained accesscontrol of encrypted data.‖ ACM Conference onComputer and Communications Security, pp. 88–98,2006.

[21] Bethencourt John, SahaiAmit, 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 networkswith efficient revocation,‖ ASIACCS11, Marc2011.

[23] Riddhimankad, DeveshJinwala ―Investigatingmulti authority attribute-based Encryption withrevocation‖, NIT Surat, 2012.

[24] M. Bellare and P. Rogaway. Random oracles arepractical: A paradigm for Designing efficientprotocols. In ACM conference on Computer andCommunications Security (ACM CCS), pages62{73, 1993.

[25] VipulGoyal,‖ Reducing Trust in the PKG inIdentity Based Cryptosystems‖ Department ofComputer Science,University of California, LosAngeles, CRYPTO 2007, LNCS4622, pp.