Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhanced Large Universe Ciphertext Policy Attribute Based Encryption

Aparna C Bhadran
M.Tech Student, KMEA,
CSE Department & MG University, Kerala, India

Maria Joy
Assistant Professor, KMEA,
CSE Department & MG University, Kerala, India

Abstract— Security is needed to be ensured when messages are to be shared among different users through an untrusted medium. In the military environment, the confidential information needs to be transmitted between the users that belongs to different ranks. The information that has to be transmitted needs to be encrypted to protect the data from an unauthorized access. There are various methods to encrypt the data like identity-based encryption, Attribute based encryption (ABE), Key policy attribute based encryption (KP-ABE), and cipher text policy attribute based encryption (CP-ABE). In CP-ABE the access policies are associated with cipher text and attributes are associated with the key. The decryption is possible only if attribute matches with the access policy. The large universe, traceability and blocking properties are added to CP-ABE. Traceability property traces the malicious user who tries to access the encrypted data without proper decryption key and pin code. Blocking property blocks the illegal user who has been traced as a malicious user. Large universe property supports a flexible number of attributes to the system. The decryption key and pin code which are needed to decrypt the data are sent to the receiver via email. When the pin code that is given by the receiver is invalid that receiver is blocked. Admin can activate the blocked user if wanted for one time. But if the user again gives invalid pin code the corresponding user is blocked and cannot again enter the system.

Keywords— Attribute based encryption, Cipher text policy attribute based encryption, Large universe, Traceability, Blocking

I. INTRODUCTION

Computer Security is a technique used to ensure that the data stored in the computer is not compromised. There are various methods to ensure security like password, data encryption etc. Data encryption means encrypting the data into another form which can be decrypted only by decryption key.

The military communication had the greatest influence on encryption. A thorough understanding encryption helps people to develop better ways to protect valuable information because the technology has become faster and more efficient.

In the attribute based encryption, the secret key and cipher text depends upon the attributes. The identity of the user is described by a set of attribute. For example, the student pursuing a master degree in computer science in the year 2015 has attributes {computer_science, masters, 2015}.

Attribute Based Encryption can be categorized by the small universe and large universe construction. In small universe construction, the attributes are fixed at system setup, attribute size is polynomially bounded and public parameter size grows linearly with the attributes. In the large universe construction, the attributes are not fixed at system setup and attribute size is not polynomially bounded.

Goyle et al proposed two complementary forms of ABE: Key policy attribute based encryption[7](KP-ABE),Cipher text policy attribute based encryption(CP-ABE)[2].An access policy is a policy that specifies the types of users that have permission to read the data. In KP-ABE decryption keys are issued based on access policy and cipher text are illustrated with attributes. In CP-ABE decryption keys are issued depending upon attribute set and the sender can specify access policy.

II. RELATED WORKS

Whitfield Diffie and Martin Hellman introduced the concept of public key encryption [3], the sender and receiver use different keys for their encryption and decryption respectively. The sender encrypts with receiver's public key and receiver decrypt it with receiver's private key.

Shamir proposed Identity based encryption [4][5], the sender encrypts the message using receiver's public key. The public key can be openly known information like email id, designation etc. The resulting cipher text is passed through a communication channel to the receiver. The receiver gets the private key from the private key generator (PKG).The PKG uses receiver's public key along with some random seed to generate receiver's private key. The receiver can decrypt the cipher text using this private key.

Sahai and Waters introduced Fuzzy identity based encryption (FIBE) [6].It is a variation of Identity based encryption. FIBE is intended for multicasting. The multicast messages can be decrypted by all the users that have predetermined set

of attributes. The encryption and decryption key are developed using a set of attributes. The message encrypted using the key w can be decrypted using the secret key w' only if w and w' have at least d attributes in common where d is a predefined threshold value. It can be done in 2 ways:

1) Identity based encryption scheme that uses biometric identities. The message is encrypted using the biometric of the user such as fingerprint or iris scan. The receiver gets the private key from the private key generator by giving receiver side biometric along with some random seed. The message can be decrypted using this private key.

2) Sahai and Waters proposed attributes based encryption (ABE) [7].In ABE the access control is provided by public key cryptography. The main aim is to provide security, fine grained access control, flexibility. Both the secret key and cipher text are related with a set of attributes. If the threshold number of attributes between the cipher text and the secret key of the user overlaps then the user can decrypt the cipher text. ABE is mainly used in one-to-many encryption where the cipher text are implemented not for a particular user instead it is applicable to more than one user. Goyal, Pandey, Sahai and Waters proposed two concept of attribute based encryption: a. Key policy attribute based encryption (KP-ABE) b. Cipher text policy attribute based encryption (CP-ABE).

V. Goyal, O.Pandey, A. Sahai, and B. Waters proposed KP-ABE [7] [8]. The attribute policies are related to key and data is related with attributes. The data can be decrypted only if the key that is related to the policy are satisfied with the data that are related to the attributes. The sender encrypts the data with a set of attributes by using a public key. The user can decrypt the data only if the access tree structure satisfies the data attribute. It supports user secret key, accountability and provides fine grained access. The limitations of this method is that the sender cannot decide who can decrypt the message. It can only choose attributes for the data and does not provide scalability and accountability.

Sahai et al proposed CP-ABE [2]. The attribute policies are related with the data and attributes are related with the keys. The decryption is possible only if the keys that are related to attributes matches with attribute policies that are related to the data. The cipher text is related with an access tree structure and the secret key is inserted in the set of attributes. Each user is related with the set of attributes. The secret keys are generated based on the user's attribute. The message is encrypted based on the access structure. The cipher text can be decrypted only if the attributes matches with the access structure. The data that is encrypted is stored securely and the encrypted data is confidential against collusion attack. The practical issue of CP-ABE is the lack of solution to identify an illegitimate user. The access policies are associated with cipher text so it does not contain exact identities of receivers.

III. BACKGROUND

A. Access policy:

Access policy is a policy that defines what kind of users or type of users have the permission to access the documents. For example, in an academic setting the mark sheets of a class may be accessible only to the professor handling the course and some teacher assistance (TAs) of that course. Such a policy can be expressed in terms of a predicate as:

((Professor $\wedge$ CS dept) $\vee$ (M.tech student $\wedge$ CS-410 TA $\wedge$ CS dept)).

The access structure A will have the legal set of attributes that is used to represent the user. If the user in the system has the legal set of attributes then he can decrypt the cipher text otherwise, he can't retrieve any information.

B. Prime Order Bilinear Group:

Let G and G_T be two multiplicative cyclic groups of prime order p. Let g be a generator of G. Let e:GxG $\rightarrow G_T$ be the bilinear map. The bilinear map has the following properties:

a. Bilinearity:

$e(u^a,u^b)=e(u,v)^{ab}$ $\square u,v \in G$ and $a,b \in Z_p$

b. Non-degeneracy:

$e(g,g) \neq 1$

c. Symmetric:

$e(g^a,g^b)=e(g,g)^{ab}=e(g^b,g^a)$.

G is a bilinear map if the group operations in G and bilinear map e: GxG $\rightarrow G_T$ can be calculated efficiently.

IV. PROPOSED SYSTEM

In military different users that belong to different ranks needs to communicate with each other to transfer the confidential data. Table I shows some of the ranks of the officers in the army.

Table II Ranks in army

Priority	**Rank**
1	Field Marshal
2	General
3	Lieutenant General
4	Major General
5	Brigadier
6	Colonel
7	Lieutenant Colonel
8	Major

When a new user wants to enter the system the corresponding request is send to his immediately top priority user as shown in Fig. 1. The top priority user can either activate or deactivate the request. If the top priority user activates the request then the requested user can enter the system. If the top priority user deactivates the request then the user cannot enter the system.

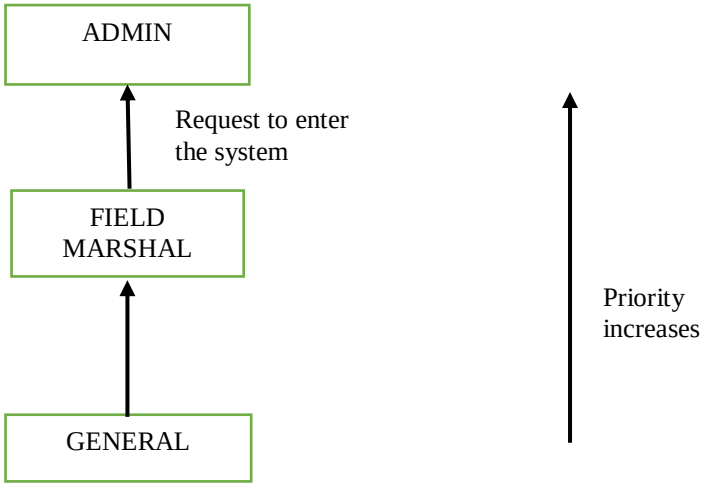

Fig. 1 Request to enter the system

First the document has to be uploaded by the sender to send the document to the receiver. After file uploading, the document will be encrypted and send to the receiver. The secret key and pin code will be generated when the encrypted data is sent to the receiver. This secret key and pin code will be sent to the receiver through email. If the receiver gives valid secret key and pin code then they can decrypt and document. If the pin code is invalid that user will be temporarily blocked and cannot enter the system. The blocked user can send the unblocking request to the admin. The admin can unblock the user if wanted. After unblocking if the user again gives invalid pin code then that user will be blocked for permanently as shown in Fig. 2.

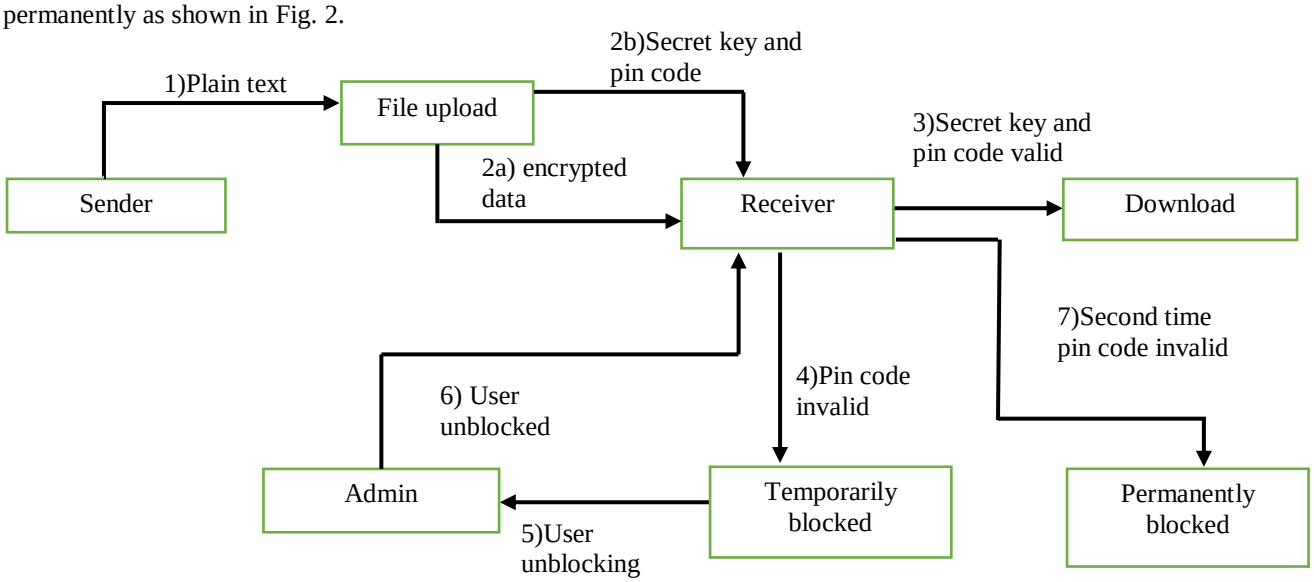

Fig. 2 Block diagram of proposed system

A. Algorithms

Proposed method uses 5 algorithms [2]:

1) Setup:

Input: Security parameter

Output: Public parameter (PK), Master secret key (MK)

The algorithm will choose a bilinear group G_0 of prime order p with generator g. Then choose two random exponents $\alpha,\beta \in Z_p$. Then computes $h = g^{\beta}$, $f = g^{1/\beta}$.PK = G_0,g, h, f, e(g,g) $^{\alpha}$ MK = (β,g^{α}).

2) KeyGen:

Input: Master secret key (MSK), Set of attributes (S).

Output: private key (SK)

The algorithm first chooses a random $r \in Z_p$, and then random $r_j \in Z_p$ for each attribute $j \in S$. Then it computes the key as:

$$SK = \{D = g^{(\alpha+r)/\beta},\ \forall j \in S: D_j = g^{r} \cdot H(j)^{r_j},\ D'_j = g^{r_j}\}$$

3) Encrypt :

Input: Public parameter (pp), Plaintext (m), Access structure (A).

Output: Cipher text

The encryption algorithm encrypts a message M under the tree access structure A. The algorithm first chooses a polynomial q_x for each node x (including the leaves) in the tree A. These polynomials are chosen in the following way in a top down manner, starting from the root node R. For each node x in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$.

Starting with the root node R the algorithm chooses a random $s \in Z_p$ and sets $q_R(0)$ =s. Then, it chooses d_R other points of the polynomial q_R randomly to define it completely. For any other node x, it sets $q_x(0) = q_{parent(x)}(index(x))$ and chooses d_x other points randomly to completely define q_x. Let, Y be the set of leaf nodes in A. The cipher text is then constructed by giving the tree access structure A and computing

$$CT = (A, \tilde{C} = Me(g, g)^{\alpha s}, C = h^s, \forall y \in Y : C_y = g^{q_y(0)}, C'_y = H(att(y))^{q_y(0)})$$

4) Delegate:

Input: Secret key (SK), subset of attributes ($\tilde{S} \subseteq S$).

Output: New secret key ($\tilde{SK}$)

The algorithm chooses random $\tilde{r}$ and $\tilde{r}_k \ \forall k \in \tilde{S}$. Then creates new secret key:

$$\tilde{SK} = (\tilde{D} = Df^{\tilde{r}}, \forall k \in \tilde{S} : \tilde{D}_k = D_k g^{\tilde{r}} H(k)^{\tilde{r}_k}, \tilde{D}'_k = D'_k g^{\tilde{r}_k})$$

The resulting secret key $\tilde{SK}$ is a secret key for the set $\tilde{S}$.

5)Decrypt:

Inputs:Public parameter (PK),private key (SK), cipher text(CT).

Output: M

For decryption we need a recursive algorithm DecryptNode(CT,SK,x).It takes input as cipher text ,secret key and a node x from access structure A. If the node x is a leaf node then compute i=att(x) if $i \in S$ then DecryptNode(CT,SK,x)= $e(g,g)^{rq_x(0)}$ Otherwise DecryptNode(CT,SK,x)= $\perp$.

If the node x is a non-leaf node then for all node z that have children then it calls DecryptNode(CT,SK, z) and store output F_z. Let S_x be an arbitrary k_x-sized set of child nodes z such that $F_z \neq \perp$.If no such set exists then the node was not satisfied and function returns $\perp$.Otherwise it returns $F_x = e(g,g)^{rq_x(0)}$ and returns the result. Now the decrypt algorithm begins by calling the function on the root node R of the access tree A. If the tree is satisfied by S then compute T=DecryptNode(CT,SK,r)= $e(g,g)^{rq_R(0)} = e(g,g)^{rs}$.

The algorithm decrypts by calculating: $\tilde{C}/(e(C/D)/T) = \tilde{C}/(e(h^s, g^{(\alpha+r)/\beta})/e(g,g)^{rs}) = M$.

B. Key Sanity Check:

We are providing 2 level security to the information that is shared by the user. As a first level of security, we are comparing the secret key provided by the receiver with the generated secret key. If the comparison is successful then the document can be decrypted otherwise the decryption is not possible.

C. Trace:

As a second level of security, a pin code is which is unique is generated randomly and given to each receiver. Initially, the status of the user is initialized as 1.If the pin code provided by the receiver is invalid then the status of the receiver is updated to 2 and that receiver is temporarily blocked from the system. If the pin code is valid then the receiver can download the document. If needed the receiver can send the request for unblocking once to the admin. The admin can either activate or deactivate the receiver.

D. Block:

After unblocking if again the user provides invalid pin code the status of the receiver is updated to 3 and that receiver is permanently blocked.

V. CONCLUSIONS

In military confidential information needs to be exchanged between different users that belong to different rank. So for that enhanced large universe cipher text policy attribute based encryption is proposed with the properties of large universe where attributes need not be fixed at system setup, tracing property allows tracing of malicious user who tries to provide invalid key and blocking property will block the malicious user from further attack.

ACKNOWLEDGMENT

The authors would like to sincerely thank the editors and anonymous reviewers for their valuable comments.

REFERENCES

[1] Jianting Ning, Xiaolei Dong, Zhenfu Cao "*White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible attributes*"in Information Forensics and Security, IEEE Transactions on June 2015.

[2] Bethencourt,J. Carnegie Mellon Univ., Pittsburgh, PA Sahai, A. ; Waters, B. *"Ciphertext-Policy Attribute-Based Encryption*" in Security and Privacy, 2007. SP '07. IEEE Symposium on 20-23 May 2007,pages 321-334

[3] W.Diffie "*The first ten years of public-key cryptography*" in Proceedings of the IEEE ,76:560-577,1988.

[4] Carl Youngblood "*An Introduction to Identity-based Cryptography*"CSEP 590T in March 2005

[5] A. Shamir "*Identity-based Cryptosystems and Signature Schemes*", Proceedings of CRYPTO '84, LNCS 196, pages 47-53, Springer-Verlag, 1984.

[6] Amit Sahai and Brent Waters "*Fuzzy identity-based encryption"* in EUROCRYPT, pages 457–473, 2005

[7] 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.

[8] Nuttapong Attrapadung, Benoît Libert, and Elie De Panafieu. "Expressive key-policy attribute-based encryption with constant-size ciphertexts" In Public Key Cryptography–PKC 2011, pages 90–108. Springer, 2011

