International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Special Issue - NGEPT - 2019

Attribute based encryption for cloud Computing

Ms. Sona L Singh, Student, EPCET, Bangalore,India,sonaraksha.ls@gmail.com

Prof. Nandini Gowda P, Assistant professor, Bangalore, India,nandini.epcet@gmail.com

Ms. Archana Pandey, Student, EPCET, Bangalore, India,archanapandey686856@ gmail.com

Abstract-The Attribute-Based Encryption is used in mobile cloud storage to protect data from malicious users. It is necessary for ABE scheme to achieve attribute revocation as the attribute will keep on changing. Keyword search is also required for mobile cloud storage. For resource constrained mobile device is used for computational efficiency. Data owner and user can generate the keyword index and search trapdoor by using keyword search. To reduce the computational load of decryption on user side by using decryption technology. RSABE scheme is secured against ciphertext policy.

Keywords —Attribute-based encryption, keyword search and mobile cloud storage.

I. INTRODUCTION

Portable mobile devices are widely favoured by users, followed bythe rapid growth of per capita holdings of mobile devices. Data storage and data processing are relatively limited for hot research area. Mobile users canoutsource their data to the cloud sever through the mobilenetworks so as to store or share it with users. One of the main concerns is to maintain the confidentiality of outsourced data. The data stored in cloud its very far from data-owner physical control so it is vulnerable for unauthorized access. The integrity for shared data is also a security consideration for solving remote possession checking protocol. Sahai and Waters presented a new method for data encryption: attribute-based encryption (ABE), which is envisioned to be a promising cryptographic primitive to protect the data security and realize fine-grained access control in one-to-many communications. The user has access right for encrypted data. more and more attention has been paid to the revocation mechanism, for user's attributes can be changed dynamically in practice, in ABE scheme attribute revocation is a challenging issue.

Searchable encryption is such a technology which is used to provide more and more attention has been paid to the revocation mechanism, for user's attributes can be changed dynamically in practice.

The contributions of our scheme can be concluded as follows:

1.We construct an RSABE scheme, which supports attribute grant and keyword search.

2.The attribute authority securely delegates the most update tasks to cloud server.

3.The cloud server will return the search results only when the keywords and indexes are matched and the attributes set of user satisfies the access policy in ciphertext.

4.Each user has a delegated secret key for cloud server, so partial decryption operations can be outsourced to the cloud server.

5.RSABE scheme is proven to be selectively secure

in the security model.

II. RELATED WORK

A. ATTRIBUTE BASED ENCRYPTION

The ciphertext can only be decrypted only if there are at least *d* attributes overlap between the set of w and w', where *d* is the threshold parameter. The cipher text is associated with an access policy and the secret key is integrated with an attribute set, a secret key can decrypt a cipher text if and only if the attributes set satisfies the access policy, while the situation is inversed in KP-ABE schemes.

B. ATTRIBUTE-BASE DECRYPTION WITH ATTRIBUTE REVOCATION

The attribute revocation was first introduced by Pirretti each attribute was designated to an expiration date, thus authority centre are required to periodically reissue updated key.

CP-ABE schemes which enforced immediate attribute revocation by introducing asemi-trusted proxy server. This method transferred most of the workload of the authority to the proxy server, which greatly reduced the pressure of the authority.

C. KEYWORD SEARCH OVER ENCRYPTED DATA

SE is a cryptographic primitive that enables users to keywords over the encrypted data without leaking keywords information. This method transferred most of the workload of the authority to the proxy server, which greatly reduced the pressure of the authority.

D.*OUTSOURCED ENCRYPTION*

 DOI : 10.18231/2454-9150.2019.0582

Outsourced decryption technology can largely reduce the computational load of user side. A fine-grained access control scheme with outsourced key generation and decryption, where two secure cloud service providers are adopted to execute key-issuing and decryption respectivelyuser side.

III. *MATH*

A. BILINEAR MAP

Choose two multiplicative cyclic group G and G'of prime order p. Let g be a generator of G. A function e:G XG'is called a bilinear map.

B. DECISIONAL PARALLEL BILINEAR DIFFIE- HELLMAN EXPONENT ASSUMPTION

An algorithm βthat outputs $z \in \{0,1\}$has advantage €in solving *q*-parallel BDHE problem in G if-

$$|Pr [\beta (y, e(g, g^{a}) =0] - Pr [\beta (y, R) =0] | \geq €$$

C. BILINEAR DIFFIE-HELLMAN ASSUMPTION

We say the BDHassumption holds if no probabilistic polynomial time algorithm can solve the BDH problem with a non-negligibleprobability.

D. LINEAR SECRET SHARING SCHEME

1)The shares for each party form a vector over Zp.

2) There exists a share-generating matrix M for Π,

where M has l rows and n columns. For all i=l,2,..,l.

III. FRAMEWORK AND SECURITY MODEL

A. FRAMEWORK

RSABE scheme includes four entities:

1) ***Attribute Authority****:* AA is in charge of the revoking and entitling user's attributes on the basis of his dynamical role.

2*) **Data Owners*:** Its data-owners responsibility to put data onto cloud. The owner extracts keywords set from the file and establishes keywords index.

3) ***Cloud server***: It is responsible for data storage and provides data access services. Once it receives an access request from a user, the Cloud server performs the retrieval operation with the submitted search trapdoor.

4) ***Users*:** A user can access data files by providing a search a trapdoor generated with keyword and secret key.

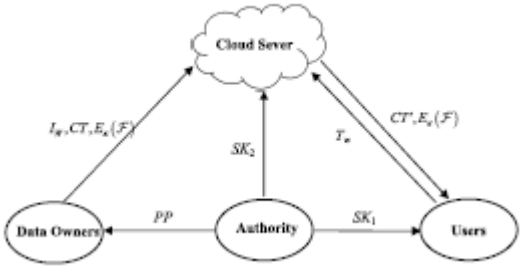

Figure 1. Framework of RSABE Scheme

The framework of RSABE scheme is shown in Fig. 1;

1)*Setup(λ)*: The setup algorithm is run by attribute authority. It takes λ as input and MK as an output.

2)*KeyGen*: The secret key generation algorithm is run by AA. It takes as inputsthe master key MK, an attribute set S_{uid} that describesthe user uid and the corresponding attribute version keys.

3)*KeyIndex:* This is run by the data owner. The inputs are the public parameters PPand a keyword set Wof the shared data file, then outputs the keywords index I_W.

4)*Encrypt:* The encrypt algorithm is run by data owner, it takes input as PP and outputs a cyphertext CT.

5)*Trapdoor* $(w; SK_1) \rightarrow T_w$. This algorithm is run by user.

6)Test: This algorithm is run by cloud server, and outputs 1 if matched and 0 otherwise.

7)*PreDecrypt:* This algorithm also depends on CS.

8)*PostDecrypt:* This algorithm is run by user.

IV. OUR CONSTRUCTION

In this paper we have issue with keyword search, attribute grant and attribute revocation. Our solution reduces computational and storage overload to the user side. Its responsibility of user to store secret key. RSABE scheme has advantages of low computation and storage capacity. There are five steps in construction those are as follows:

A) *SYSTEM SETUP*

By calling algorithm setup AA gets initialized. It chooses bilinear map e: G X G→G', where G and G' are multiplicative cyclic group.

It randomly chooses numbers:

MK={a , ā}

where a is used for data encryption and ā is for keyword search

B) *KEY GENERATION*

It is the responsibility of AA to assign unique identity to users.

KeyGen uses MK as a master key in key generation algorithm. It chooses number as:

 DOI : 10.18231/2454-9150.2019.0582

a=a1+a2 mod p

C) *DATA OUTSOURCING*

When a file F is outsourced from data owner to cloud server following steps are required:

Step 1: keyword index building

We need to send data file to other user so we need to call KeyIndex algorithm.

KeyIndex (PP, W) →Iw: the input is PP and set of keywords are W={w1,w2,…….wn}.

Step 2: data decryption

Data file F is encrypted by data owner to process symmetric keys.

D*) KEYWORD SEARCH*

when data user wants to download any encrypted file.

Step 1: Trapdoor generation

The user generates trapdoor keyword w.

Step 2*:* search data by CS

By calling algorithm Test CS is performed.

E) *DATA DECRYPTION*

It consists of two steps:

Step 1: Decryption by CS

If the output of the previous Test algorithm is 1, which

means that the keyword index is matched with the keywordtrapdoor, the CS partially decrypts the corresponding ciphertext *CT* by calling the algorithm PreDecrpt.

Step2: decryption by user

When the user *uid* receives the search results from the CS,it further decrypts the partially decrypted ciphertext *CT*0 bycalling the algorithm PostDecrpt.

V. *PERFORMANCE ANALYSIS*

The performance analysis is measured in terms of computation cost, storage overhead and communication cost.

A. *COMPUTATION COST*

On a Windows system with an Intel Core i7 CPU at3.60GHz and 8.00 GB RAM our proposed RSABE scheme simulation is used.

The implementation is done by Pairing-based cryptography. Anelliptic curve of 160-bit is used for bilinear map. The size of group elements is 1024 bit and base field size is 512 bits. The computation cost is evaluated in terms of system-setup, key-generation, encryption, decryption, and secret key.

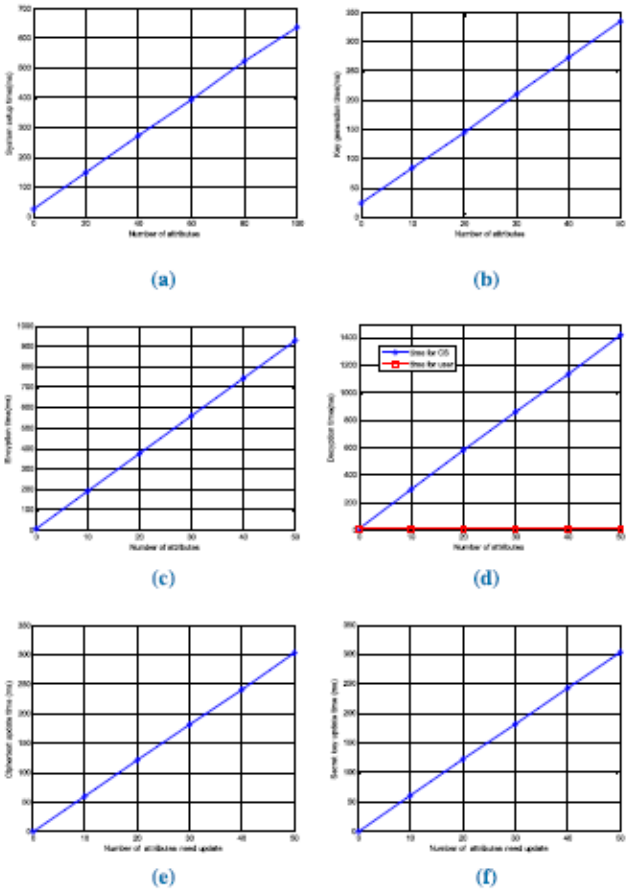

Figure 2. Performance evaluation on RSABE (a) System setup (b) Key-generation (c) Encryption (d) Decryption (e) Ciphertext update (f) Secret key update.

Fig. 2(a) describes time cost of setup, Fig. 2(b) describes key-generation and Fig. 2(c) describes encryption. Time cost linearly increase with the number of attributes in universe, secret keys and ciphertexts.

Fig. 3(d), the time cost of decryption at user side is bounded by a small constant, since most decryption task is outsourced to CS. Fig. 3(e) and Fig. 3(f) show that the time cost is linear with the number of revoked attributes.

B. *STORAGE OVERHEAD*

It is important factors that needs to be considered in mobile cloud storage. The storage overhead on the CS is remarkably increased that doesn't produce much effect on mobile cloud storage.

C. *COMMUNICATION COST*

Communication cost of owner is relatively increased as we add keywords index. Focuses on reducing the user's communication costs. the communication cost between user and the authority.

VI. CONCLUSION

An attribute-based encryption scheme for mobile cloud storage supports attribute grant, attribute revocation and keyword search. Our solution enhances computational efficiency for outsourced decryption technology. RSABE is

 DOI : 10.18231/2454-9150.2019.0582

more secured and can be applied to many cloud storage systems. To consider the situation of multi-authority which is more accordant with practical circumstances

REFERENCES

[1] N. Fernando, S. W.Loke, and W. Rahayu, " Mobile cloud computing: A survey,"*Future Generat. Comput. Syst.*,vol.29, no.1,pp.84 106, 2013.

[2] J. Li, H. Yan, and Y.Zhang, " Certificateless public intergity checking of group shared data on cloud storage,"*IEEE Trans.Service Comput*, to be published, doi: 10.1109/TSC.2018.2789893.

[3] A. Sahai and B. Waters, " Fuzzy identity-based encryption," in *Advances in cryptology - EUROCRYPT*, R. Cramer, Ed. Berlin, Germany: Springer, 2005,pp.457 473

[4] J. Hur andD.K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems."*IEEE Trans.Parallel Distrib.Syst*, vol. 22, no. 7, pp. 1214 1221, Jul. 2011.

[5] L. Zu, Z. Lou, and J. Li, " New ciphertext-policy attribute- based encryption- with efficient revocation," in proc. *IEEE Int. Conf. Comput. Inf. Technol.(CIT)*,SEP.2014,pp.281 287.

 DOI : 10.18231/2454-9150.2019.0582