Application of Antenna Arrays to Mobile Communications,Part I:Performance Improvement, Feasiblity and Systems Consideration

A seminar report submitted

to

MANIPAL UNIVERSITY

For Partial Fulfillment of the Requirement for the

Award of the Degree

of

Bachelor of Technology

in

Information Technology

by

Manali Goel
Reg. No. 130911306

Department of Information and Communication Technology
MANIPAL INSTITUTE OF TECHNOLOGY
(A constituent Institute of Manipal University)
MANIPAL - 576 104, KARNATAKA, INDIA

October 2016

Abstract

In several distributed systems a user can only access data if user has certain set of credentials or attributes. One method to enforce such policy is to employ a trusted server to store the data and mediate access control. However if server storing the data is compromised then the confidentiality of the data is compromised. Therefore we use Cipher text-Policy Attribute-Based Encryption[1]. Shared files generally have hierarchical structure which is not explored in Cipher text-Policy Attribute-Based Encryption.

This article describes an efficient file hierarchy attribute-based encryption scheme to explore hierarchical structure of shared files in cloud computing.This scheme helps to reduce the computational complexity. Firstly system definition and basic construction of the file hierarchy attribute-based encryption scheme is proposed that is based on four operations Setup,Key Generation,Encrypt,Decrypt.Then improvement in scheme is proposed and finally using theoretical analysis and experimental simulation the proposed scheme is proved to be highly efficient in terms of encryption and decryption.

1 Introduction

Now days people are storing,accessing and sharing their information such as documents, files, data, photos and videos in cloud rather than storing the information locally on a hard disk,removal media,etc. As the technology is expanding the need to protect data from leaking encryption techniques are used. First step to protect data is to ensure authorization. Attribute-based encryption scheme ensures authorization. This scheme is public key encryption in which the secret key of a user and cipher text are dependent on the attributes.In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.
There are two types of attribute based encryption scheme :
1) Key-Policy Attribute-Based Encryption (KP-ABE)
2) Cipher text-Policy Attribute-Based Encryption (CP-ABE)

1.1 Cipher Text-Policy Attribute-Based Encryption Scheme

In cipher text-policy attribute-based encryption (CP-ABE) a users private-key is associated with a set of attributes and a cipher text specifies an access policy over a defined universe of attributes within the system. A user will be ale to decrypt a cipher text, if and only if his attributes satisfy the policy of the respective cipher text. In CP-ABE scheme each file information is encrypted by different access policies based on the actual need even though files are in same hierarchical structure.

1.2 File Hierarchy Attribute-Based Encryption Scheme

Using File Hierarchy Attribute-Based Encryption Scheme(FH-CP-ABE)[2] we can encrypt multiple hierarchical files with one integrated access structure. Also by this method there is low storage cost and computational complexity in terms of encryption and decryption.

1.3 Data Sharing In Cloud Computing

In cloud computing[3, 4] we have four actors: authority,cloud service provider,data owner and user.
1) Authority: It is completely trusted party in Cloud Computing and accepts enrollment from the user.
2) Cloud Service Provider: It provide multiple Services to the Client.
3) Data Owner: It encrypts the data to be shared/store on cloud and sends the encrypted data to cloud service provider.
4) User: Downloads and decrypts the cipher text from cloud service provider.

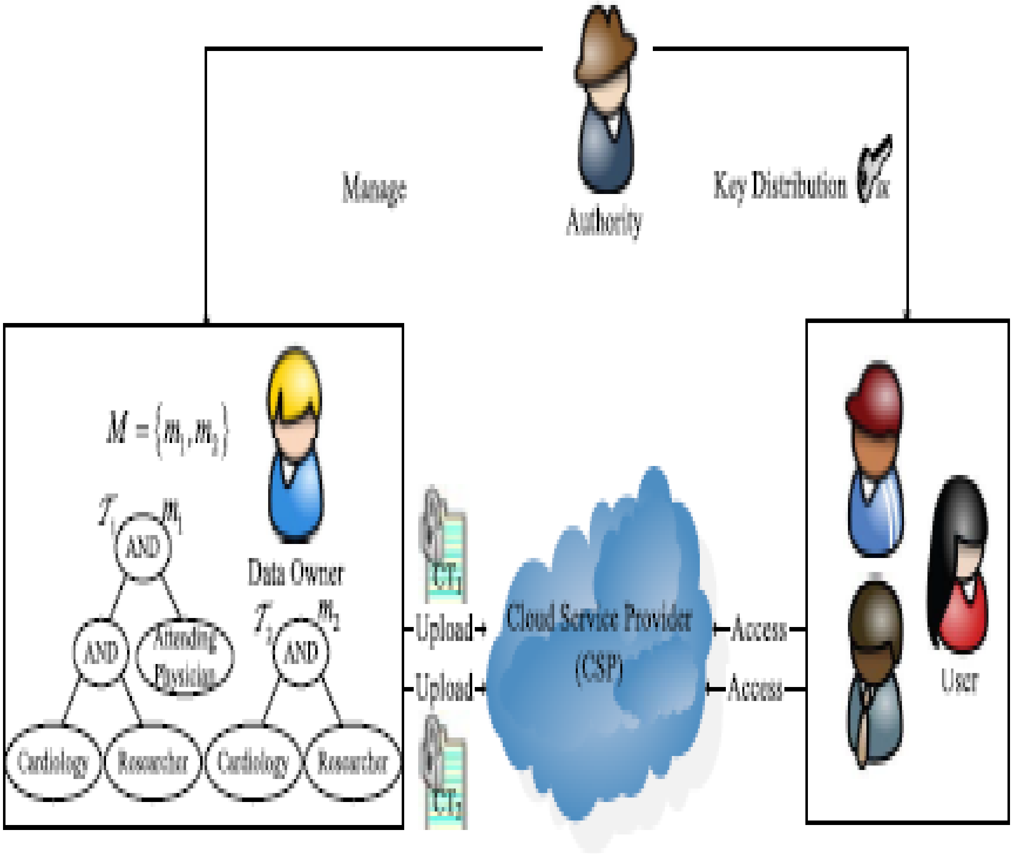


Fig. 1. An example of secure data sharing in cloud computing.

2 Preliminaries

In this section system definitions and basic constructions is described.

2.1 Access Structure

Access Structures are referred as qualified sets.It is used in security where multiple parties work together to obtain a resource.Using access structures people can provide digital signatures. Basically it describes which party should coordinate with whom to get the resources.

2.2 Bilinear Maps

Bilinear map is a function combining elements of two vector spaces to yield an element of a third vector space, and is linear in each of its arguments. Matrix multiplication is an example. In case of encryption Bilinear maps are basically used for pairing based cryptography. For this scheme bilinear maps should satisfy three properties like bilinearity, non-degeneracy and compuatability.

2.3 Hierarchical Access Tree

In this scheme T is the hierarchical tree that represents and access structure that is divided into different levels(k access levels).

Nodes of the tree are represented as (x, y) where x denotes the row number and y denotes the column number.

This access structure is made by using ”OR” and ”AND” gates.

num$_{\text{x, y}}$ defines the number of children of node(x, y)

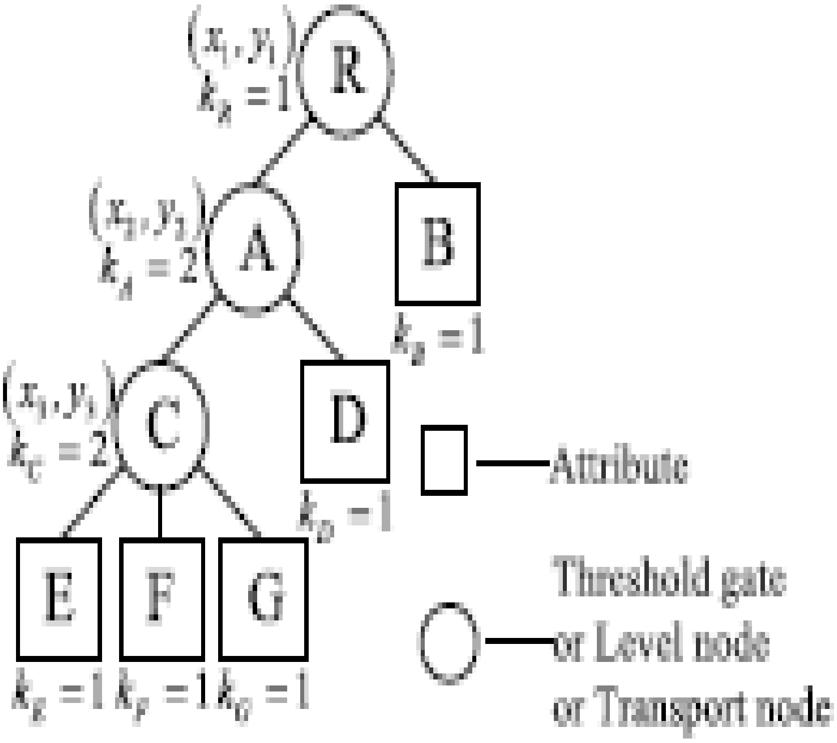
k$_{\text{x,y}}$ denotes the threshold value of node (x, y). If k$_{\text{x,y}}$ is 1 then node(x, y) is a non-leaf node and is an ”OR” gate but if k
textsubscriptx,y=num$_{\text{x,y}}$ then node (x, y) is a non-leaf node and ”AND” gate.

parent$_{\text{x,y}}$ denotes the parent of the node (x, y).
transport nodes are those nodes that contain at least on non-leaf node as their children.

index$_{\text{x,y}}$ returns a unique value associated with the node (x, y).

TN-CT(A): It represents number of children of A that are transport nodes.

attribute set is the set of leaf nodes.



2.4 System Definition and Basic Construction

In this we assume data owner has k files with k access levels and M={$\mathrm{m_1}$, $\mathrm{m_2}$, ..., $\mathrm{m_k}$} are shared in cloud computing.

2.4.1 Encryption

In fig2 a data owner processes the files in the following manner:
1.)Data owner choose k content keys {$\mathrm{ck_1}$, $\mathrm{ck_2}$,.. , $\mathrm{ck_k}$} and encrypts files {$\mathrm{m_1}$, $\mathrm{m_2}$,..., $\mathrm{m_k}$} using symmetric encryption algorithm {DES,AES } .
2.)Cipher texts are denoted as $\mathrm{E_{ck}}$(M)={$\mathrm{E_{ck_1}}$($\mathrm{m_1}$),...,$\mathrm{E_{ck_k}}$($\mathrm{m_k}$)} 3.)Data owner encrypts {$\mathrm{ck_1}$, $\mathrm{ck_2}$,.. , $\mathrm{ck_k}$} using FH-CP-ABE encryption algorithm and obtains an integrated cipher text of content keys CT.

2.4.2 Decryption

1.)User decrypts the cipher text CT and obtain content key by using FH-CP-ABE decryption operation.
2.)Then, the user can obtain file by using symmetric decryption algorithm with content key.

2.4.3 FH-CP-ABE Scheme Operations

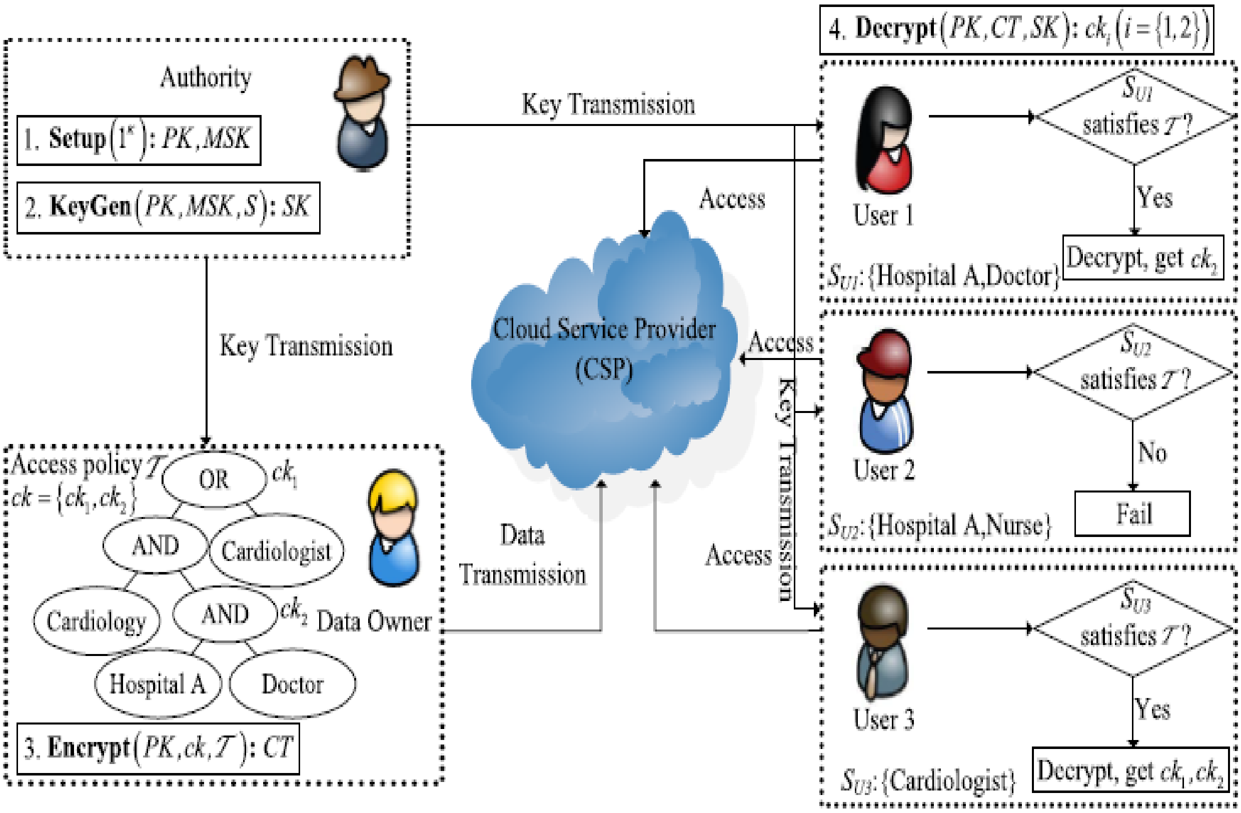
FH-CP-ABE consist of four operations: Setup,Key Generation, Encrypt and Decrypt

Setup This operation takes a security parameter k as input and outputs public key PK and master secret key MSK.

Key Generation The operation inputs PK,MSK and a set of attributes S and creates a secret key SK .

Encrypt The operation inputs PK,$\{ck_1, ck_2, .. , ck_k\}$ and a hierarchical access tree A and creates an integrated cipher text of content keys CT.

Decrypt The algorithm inputs PK, CT which includes an integrated access structure A, SK described by a set of attributes S. If S matches A all content keys can be decrypted. Then corresponding files can be decrypted with content keys by symmetric description algorithm.



4. Decrypt(PK, CT, SK): $ck_i (i = \{1,2\})$
Authority
1. Setup(1^κ): PK, MSK
2. KeyGen(PK, MSK, S): SK
Key Transmission
Access
Key Transmission
Cloud Service Provider (CSP)
Access
Key Transmission
Data Transmission
Access
Access policy $\mathcal{T}$
$ck = \{ck_1, ck_2\}$
OR
ck_1
AND
Cardiologist
Cardiology
AND
ck_2
Data Owner
Hospital A
Doctor
3. Encrypt$(PK, ck, \mathcal{T})$: CT
User 1
S_{U1} satisfies $\mathcal{T}$?
Yes
S_{U1}:{Hospital A,Doctor}
Decrypt, get ck_1
User 2
S_{U2} satisfies $\mathcal{T}$?
No
S_{U2}:{Hospital A,Nurse}
Fail
User 3
S_{U3} satisfies $\mathcal{T}$?
Yes
S_{U3}:{Cardiologist}
Decrypt, get ck_1, ck_2

Fig 2: An example of FH-CP-ABE scheme in cloud computing

3 The Proposed FH-CP-ABE Scheme

3.1 Scheme Construction

1) Setup :

$$PK = \{\mathbb{G}_0, g, h = g^{\beta}, e(g,g)^{\alpha}\}$$
$$MSK = \{g^{\alpha}, \beta\}$$

where PK=Public Key MSK=Master Secrey Key

2)Key Generation:

$$SK = \left\{ \begin{array}{l} D = g^{\alpha} \cdot h^{r}, \\ \forall j \in S : D_j = g^{r} \cdot H_1(j)^{r_j}, D'_j = h^{r_j} \end{array} \right\}$$

where SK is Secret Key

3)Encrypt Operation:

$$\tilde{C}_i = ck_i e(g,g)^{\alpha s_i}, \quad C'_i = g^{s_i}$$

$$C_{(x,y)} = h^{q_{(x,y)}(0)}$$
$$C'_{(x,y)} = H_1(att(x,y))^{q_{(x,y)}(0)}$$

$$\hat{C}_{(x,y),j} = \left\{ \begin{array}{l} e(g,g)^{\alpha \cdot (q_{(x,y)}(0) + q_{child_j}(0))} \\ \cdot H_2(e(g,g)^{\alpha q_{(x,y)}(0)}) \end{array} \right\}$$

$$CT = \{T, \tilde{C}_i, C'_i, C_{(x,y)}, C'_{(x,y)}, \hat{C}_{(x,y),j}\}$$

where CT is integrated cipher text of content keys

4)Decrypt Operation:

If (x, y) is a leaf node decrypt in the following way:

$$\begin{aligned} DecryptNode(CT, SK, (x, y)) &= \frac{e(D_i, C_{(x,y)})}{e(D_i', C_{(x,y)}')} \\ &= \frac{e(g^r H_1(i)^{r_i}, h^{q_{(x,y)}(0)})}{e(h^{r_i}, H_1(att(x, y)^{q_{(x,y)}(0)}))} \\ &= e(g, g)^{r\beta q_{(x,y)}(0)} \end{aligned}$$

If (x, y) is a non-leaf node decrypt in the following way:

$$\begin{aligned} F_{(x,y)} &= \prod_{z \in S_{(x,y)}} F_z^{\Delta_{i,S'_{(x,y)}}(0)} \\ &= \prod_{z \in S_{(x,y)}} (e(g, g)^{r \cdot \beta q_z(0)})^{\Delta_{i,S'_{(x,y)}}(0)} \\ &= \prod_{z \in S_{(x,y)}} (e(g, g)^{r \cdot \beta q_{(x,y)}(i)})^{\Delta_{i,S'_{(x,y)}}(0)} \\ &= e(g, g)^{r \cdot \beta q_{(x,y)}(0)} \end{aligned}$$

Procedure to decrypt is :

$$\begin{aligned} A_i &= DecryptNode(CT, SK, (x_i, y_i)) \\ &= e(g, g)^{r\beta q_{(x_i,y_i)}(0)} \\ &= e(g, g)^{r\beta s_i} (i \in [1, k]) \end{aligned}$$

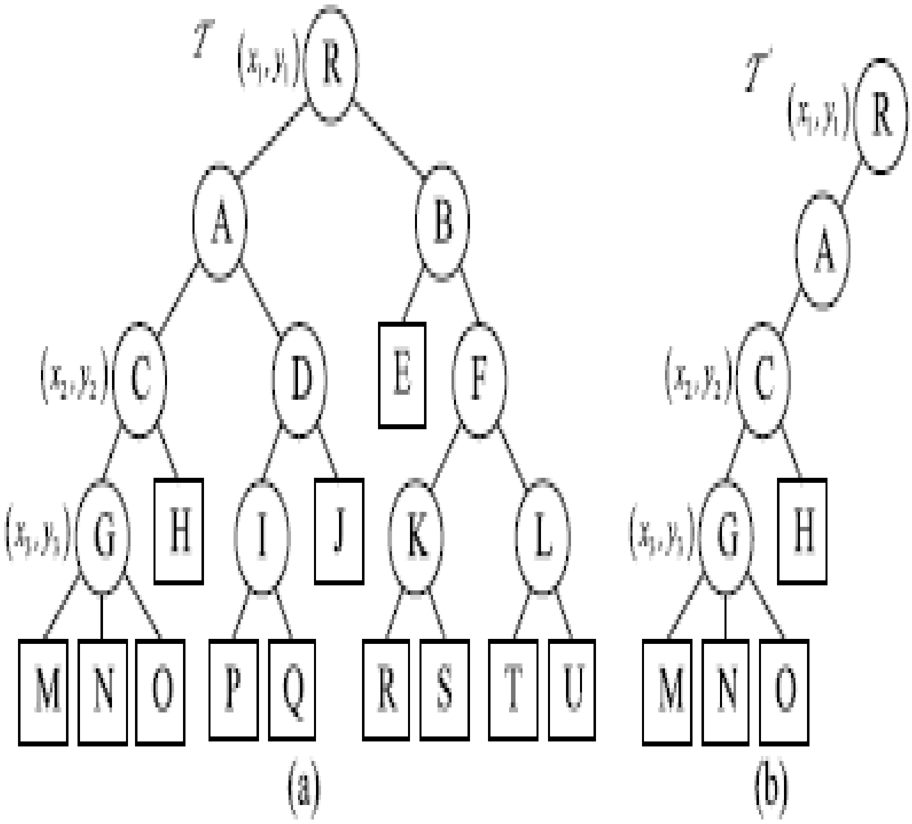
$$\begin{aligned} F_i &= \frac{e(C_i', D)}{A_i} \\ &= \frac{e(g^{s_i}, g^{\alpha} \cdot g^{\beta r})}{e(g, g)^{r\beta s_i}} \\ &= e(g, g)^{\alpha s_i} (i \in [1, k]) \end{aligned}$$

$$\frac{\tilde{C}_i}{F_i} = \frac{ck_i e(g, g)^{\alpha s_i}}{e(g, g)^{\alpha s_i}} = ck_i (i \in [1, k])$$

after this last step is to decrypt the encrypted files using content keys {ck$_1$, ck$_2$,.. , ck$_k$} using any symmetric decryption algorithm like AES, DES, etc

3.2 Efficient Scheme of FH-CP-ABE

In Efficient Scheme of FH-CB-ABE we remove the unwanted transport nodes in order to reduce the computational complexity and storage cost. In the below figure a) part represents the 3 level access structure where we have 9 eligible children threshold gates that are related to transport nodes but using this scheme we reduce these 9 eligible children threshold gates to 3 threshold gates as in b) because nodes B, D, and F do not carry any information regarding the level node.



3.3 Scheme Features

1) Computation Cost For Data Owner:
As in this scheme we are using a single integrated access structure for the encryption of files therefore here the cost for encryption reduces and hence the efficiency of the data owner is improved.
2) Computation Cost For User: Using this scheme the user can decrypt all his authorization files using secret key only once and also the bi linear pairing operation of each common node is also computed only once. Therefore by using this scheme the decryption cost is also reduced.

4 Security Analysis

Here two aspects are considered firstly the confidentiality of file cipher text and secondly the confidentiality of content keys that are used for encryption of files.

This scheme also proves that no polynomial adversary can selectively break the proposed system.

$$
\begin{aligned}
Adv_{\mathcal{S}} = {} & \frac{1}{2}Pr[\mathcal{B}(g, g^{a}, g^{b}, g^{c}, T = e(g, g)^{abc}) = 0] \\
& + \frac{1}{2}Pr[\mathcal{B}(g, g^{a}, g^{b}, g^{c}, T = R) = 0] - \frac{1}{2} \\
= {} & \frac{1}{2} \cdot (\frac{1}{2} + \varepsilon) + \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} \\
= {} & \frac{\varepsilon}{2}
\end{aligned}
$$

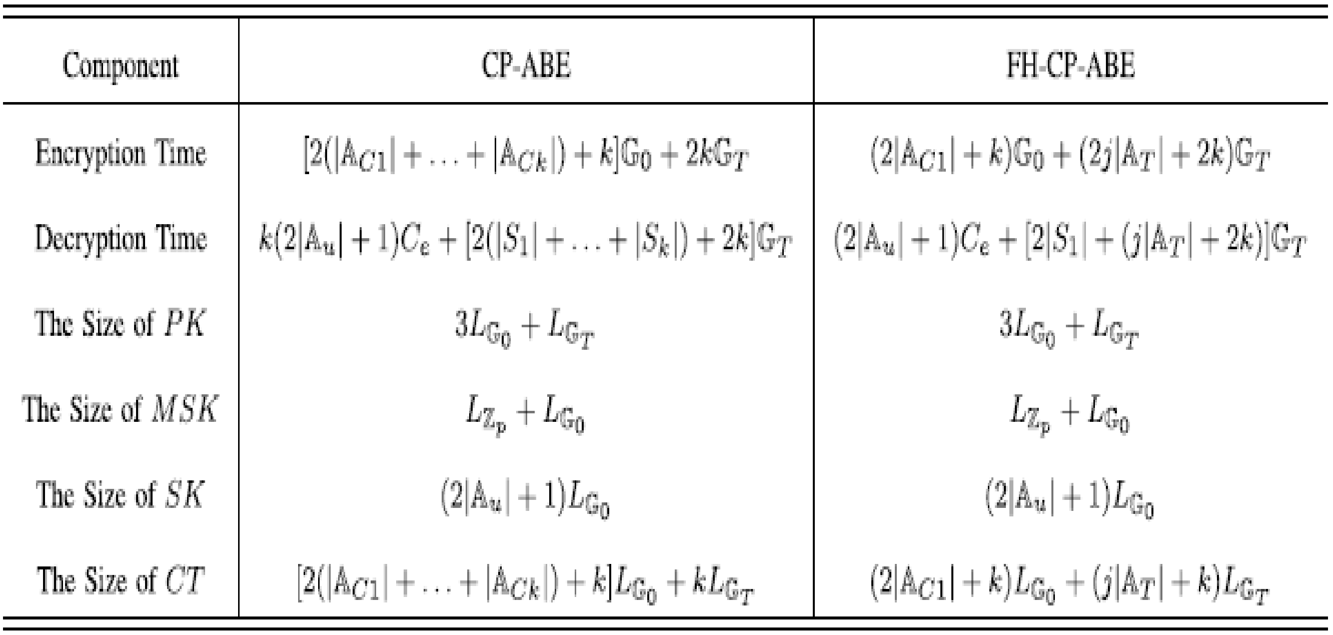
5 Performance Analysis

This section describes the efficiency of the proposed scheme by theoretical and practical analysis.

5.1 Theoretical Analysis

TABLE I

COMPARISONS OF THE FEATURES OF CP-ABE WITH FH-CP-ABE ($M = \{m_1, \ldots, m_k\}$)



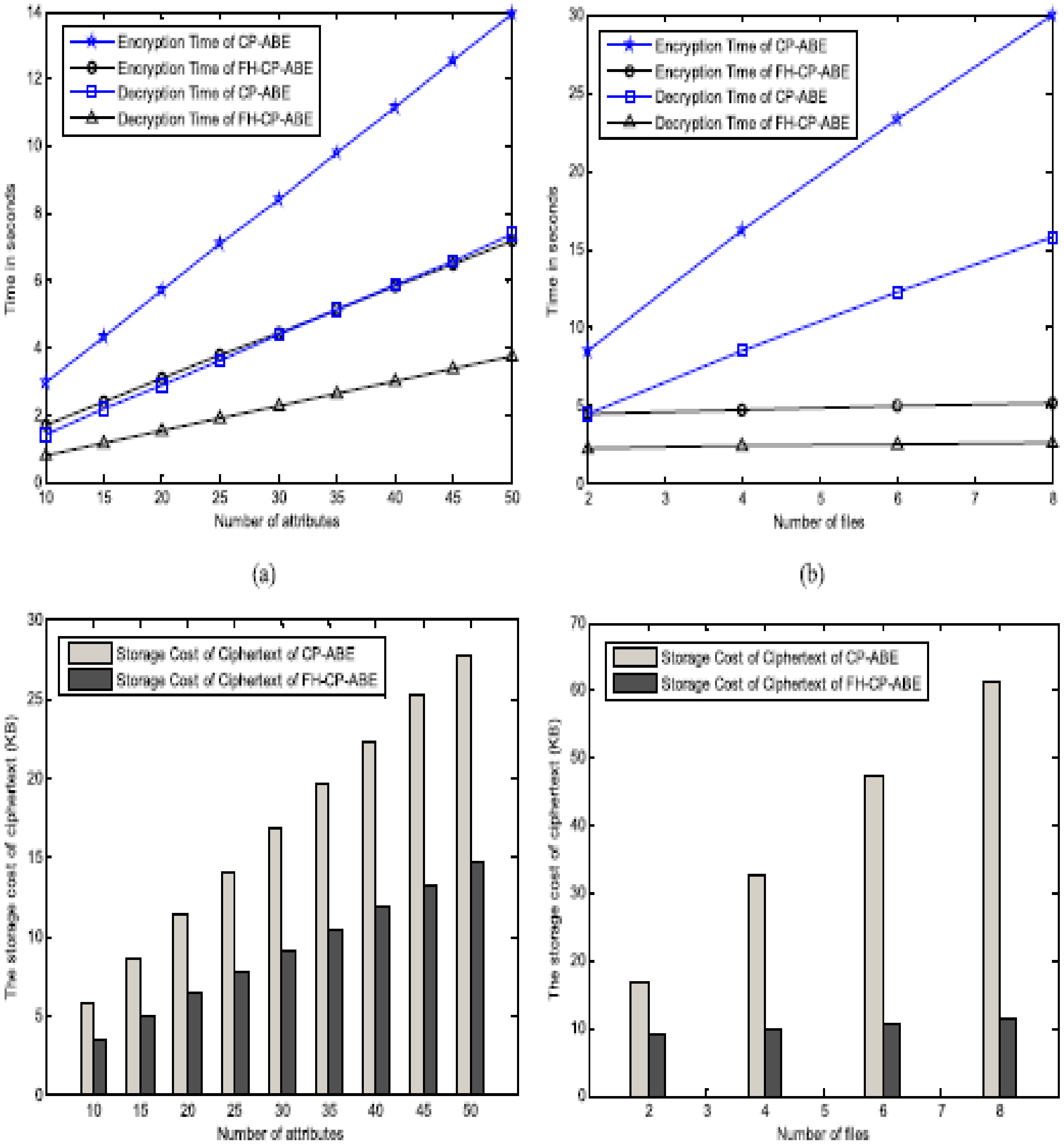
Component	CP-ABE	FH-CP-ABE
Encryption Time	$[2(\lvert\mathbb{A}_{C1}\rvert + \ldots + \lvert\mathbb{A}_{Ck}\rvert) + k]\mathbb{G}_0 + 2k\mathbb{G}_T$	$(2\lvert\mathbb{A}_{C1}\rvert + k)\mathbb{G}_0 + (2j\lvert\mathbb{A}_T\rvert + 2k)\mathbb{G}_T$
Decryption Time	$k(2\lvert\mathbb{A}_u\rvert + 1)C_e + [2(\lvert S_1\rvert + \ldots + \lvert S_k\rvert) + 2k]\mathbb{G}_T$	$(2\lvert\mathbb{A}_u\rvert + 1)C_e + [2\lvert S_1\rvert + (j\lvert\mathbb{A}_T\rvert + 2k)]\mathbb{G}_T$
The Size of PK	$3L_{\mathbb{G}_0} + L_{\mathbb{G}_T}$	$3L_{\mathbb{G}_0} + L_{\mathbb{G}_T}$
The Size of MSK	$L_{\mathbb{Z}_p} + L_{\mathbb{G}_0}$	$L_{\mathbb{Z}_p} + L_{\mathbb{G}_0}$
The Size of SK	$(2\lvert\mathbb{A}_u\rvert + 1)L_{\mathbb{G}_0}$	$(2\lvert\mathbb{A}_u\rvert + 1)L_{\mathbb{G}_0}$
The Size of CT	$[2(\lvert\mathbb{A}_{C1}\rvert + \ldots + \lvert\mathbb{A}_{Ck}\rvert) + k]L_{\mathbb{G}_0} + kL_{\mathbb{G}_T}$	$(2\lvert\mathbb{A}_{C1}\rvert + k)L_{\mathbb{G}_0} + (j\lvert\mathbb{A}_T\rvert + k)L_{\mathbb{G}_T}$

As shown in the above Table1 the length of the Public Key,Master Secret Key and Secret Key is same in both the algorithms but as j is relatively small in FH-CP-ABE Scheme the encryption algorithm is small in FH-CP-ABE Scheme.Hence, theoretically FH-CP-ABE scheme is better than CP-ABE scheme.

5.2 Experimental Results

The experiments are conducted using Java and all the results are average of more than 10 trials. Two results were observed firstly the scheme reduces the cost of encryption and decryption and secondly the scheme reduces the storage cost.

The experimental results we plotted and graph a) shows the reduction in computational cost of encryption and decryption whereas graph c) shows storage cost of cipher text for various attributes.



(a)

(b)

(c)

(d)

6 Conclusion

In this paper we have extended the CP-ABE scheme and introduced a new scheme FH-CP-ABE which saves the time and computational cost for encryption and decryption also it reduces storage spaces needed for encryption and decryption.This scheme is proved to be secure under DBDH assumptions.Also by using this scheme the user can decrypt all files at once and this scheme provide authorization that is needed for secure transfer of data in cloud computing.

In this scheme keys are not user specific they are generated by trusted third party hence any future user can also decrypt the message using the desired attributes and key.As trusted third party is generating the keys authorization is guaranteed here and it becomes difficult for unauthorized users to decrypt the contents of the files.

Also this scheme helps in the encryption of hierarchical files with a single integrated structure and the cipher text components related to attributes.Therefore this scheme efficiently share the hierarchical files in cloud computing.

References

[1] A. S. J. Bethencourt and B. Waters, “Ciphertext-policy attributebased encryption,” *IEEE Symposium on security and Privacy*, May 2007.

[2] M. I. J. K. L. M. I. J. Y. J. C. Shulan Wang, Junwei Zhou and W. Xie, “An efficient file hierarchy attribute-based encryption scheme in cloud computing,” *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. 11,No.6, JUNE 2016.

[3] J. H. J.-K. L. J. X. C.-K. Chu, W.-T. Zhu and J. Zhou, “Security concerns in popular cloud storage services,” *IEEE Pervasive Comput.*, vol. vol. 12, no. 4, Oct./Dec. 2013.

[4] J. L. D. S. W.-J. M. T. Jiang, X. Chen and J. Liu, “Timer: Secure and reliable cloud storage against data re-outsourcing,” *Proc. 10th Int. Conf. Inf. Secur. Pract. Exper*, vol. vol. 8434, May 2014.