Metadata of the chapter that will be visualized in SpringerLink

Book Title	Intelligent Data Communication Technologies and Internet of Things	
Series Title		
Chapter Title	CP-ABE Based Mobile Cloud Computing Application for Secure Data Sharing	
Copyright Year	2020	
Copyright HolderName	Springer Nature Switzerland AG	
Corresponding Author	Family Name	**Unki**
	Particle	
	Given Name	**Prakash H.**
	Prefix	
	Suffix	
	Role	
	Division	Department of Computer Science and Engineering, BLDEA's V.P. Dr. P.G. Halakatti College of Engineering and Technology
	Organization	Visvesvaraya, Technological University
	Address	Vijayapur, Belagavi, 586103, Karnataka, India
	Email	prakashhunki@gmail.com
Author	Family Name	**Kattimani**
	Particle	
	Given Name	**Suvarna L.**
	Prefix	
	Suffix	
	Role	
	Division	Department of Computer Science and Engineering, BLDEA's V.P. Dr. P.G. Halakatti College of Engineering and Technology
	Organization	Visvesvaraya, Technological University
	Address	Vijayapur, Belagavi, 586103, Karnataka, India
	Email	suvarnaky1977@gmail.com
Author	Family Name	**Kirankumar**
	Particle	
	Given Name	**B. G.**
	Prefix	
	Suffix	
	Role	
	Division	Department of Computer Science and Engineering, BLDEA's V.P. Dr. P.G. Halakatti College of Engineering and Technology
	Organization	Visvesvaraya, Technological University
	Address	Vijayapur, Belagavi, 586103, Karnataka, India
	Email	bgkiran16@gmail.com

Abstract

Due to the increased availability of internet and smart phones, mobile cloud computing becomes more popular in recent years. Maintaining security in mobile clouds is the most challenging issue because mobile devices are having limited computational resources and most of the operations are done through the

internet. Therefore, it is necessary to safeguard data access from unauthorized access. In this paper Ciphertext based Attribute-Based Encryption is implemented. It offers better data security and privacy using efficient access control and privilege management. and we have measured the performance of Key Policy Based-ABE and Cipher Text Policy Based-ABE, results show that Cipher Text Policy-Based ABE takes less time to perform encryption, key generation, decryption and offers better security compared to KP-ABE.

Keywords KP-ABE - CP-ABE - Mobile cloud computing - Access policy

CP-ABE Based Mobile Cloud Computing Application for Secure Data Sharing

Prakash H. Unki(✉), Suvarna L. Kattimani, and B. G. Kirankumar

Department of Computer Science and Engineering, BLDEA's V.P. Dr. P.G. Halakatti College of Engineering and Technology, Visvesvaraya, Technological University, Vijayapur, Belagavi 586103, Karnataka, India
prakashhunki@gmail.com, suvarnakyl977@gmail.com, bgkiranl6@gmail.com

Abstract. Due to the increased availability of internet and smart phones, mobile cloud computing becomes more popular in recent years. Maintaining security in mobile clouds is the most challenging issue because mobile devices are having limited computational resources and most of the operations are done through the internet. Therefore, it is necessary to safeguard data access from unauthorized access. In this paper Ciphertext based Attribute-Based Encryption is implemented. It offers better data security and privacy using efficient access control and privilege management. and we have measured the performance of Key Policy Based-ABE and Cipher Text Policy Based-ABE, results show that Cipher Text Policy-Based ABE takes less time to perform encryption, key generation, decryption and offers better security compared to KP-ABE.

AQ1

AQ2

Keywords: KP-ABE · CP-ABE · Mobile cloud computing · Access policy

1 Introduction

Nowadays the mobile cloud applications are very popular due to its globally available internet and advancement in smartphone technology. Mobile cloud is a new computing technology delivers unlimited storage and other computational resources for their clients based on their needs or payment on the go access mode. Some of the applications and services are freely available in the public cloud, where users can have access to these applications up to some time limit or storage limit, the problem in this free application and services are trustworthiness of data is not guaranteed because all users in the public cloud have access to the cloud data .these situations lead to data security and privacy attacks. Hence to handle these issues some of the security algorithms need to be adopted in mobile clouds. There are several security standards available like KP-ABE, CP-ABE, SDS, Homomorphic algorithm, etc. but these security standards are developed for High computational devices and cloud servers. To apply these in the mobile cloud require little modifications because the mobile devices are the lack of storage and computing power capabilities. In such cases, it is required to utilize fewer resources on the mobile side. and heavy computational operations should be outsourced to the proxy server. It effectively reduces the computational overhead at the mobile cloud. KP-ABE and CP-ABE standards suitable for mobile cloud computing, but

J. Hemanth et al. (Eds.): ICICI 2019, LNDECT 38, pp. 1–7, 2020.
https://doi.org/10.1007/978-3-030-34080-3_64

CP-ABE offer more benefits compare to KP-ABE in terms of security, less time taken for encryption and key generation and decryption, overall it reduces the communication cost and provides better access control facility. In this paper, we developed the prototype CP-ABE Based Mobile cloud computing application for secure data sharing. It implements CP-ABE algorithm [1] to guarantee the security and privacy and also it offers efficient privilege management feature to handle access control.

2 Existing System

KP-ABE Scheme has four function Setup, encryption, key-Generation, Decryption

(a) Setup (R_n, P_k, M_k): Setup function uses uniform random numbers Rn to produces the master key and public key.
(b) Encryption (Msg, $U_{Attributes}$, Public $_{key}$): Data Authority performs Encryption, it generates the ciphertext using the user attributes and Original message M, public key.
(c) Key Generation ($U_{Attributes}$, Public $_{Key}$, Master $_{Key}$): trusted authority creates secret keys using user attributes and public key and master key.
(d) Decryption (C_T, S_K): User performs the decryption using Cipher text and secret key of the user.

Significant problems of KP-ABE algorithm [1] in cloud computing has several restrictions to adopt, in this scheme First limitation is, actual data owner has no control to choose who can be able to decrypt the data. Second, it increases communication overhead when more attributes are added to the control tree. Its access policy is not suitable for mobile cloud devices.

3 Proposed System

Sahai and Waters [1] implemented the Attribute Based Encryption which is initially produced from the Identity Based Encryption (IBE). IBE is adopted in broadcasting systems. Basically, ABE is classified into two schemes Key policy based-ABE and Cipher Text Based-ABE. In KP-ABE encryption algorithm access policy is enclosed with data user key. In CP-ABE algorithm [10] access control procedure is enclosed with encrypted message. CP-ABE is commonly used in real time cloud application because it has better control over access control policy and data owner has an option design his own access policy based on number of attributes. Only authorized user whose attributes match with access control procedure can decrypt the original data.

The Cipher Text Policy-ABE Algorithm comprises of four functions they are explained in the following sections.

1. **Setup**- It accepts security parameters k and produces master key (MK) and public key (PK). Mixture of master key and public keys are used to generate Secret key.
2. **Encrypt**- This function performs encryption using public key, message, access control tree to generate Cipher Text (CT).

3. **Key Generation-** It accepts input of User Attributes and Master key (MK) to produce Secret Key (SK).
4. **Decrypt**- This function accepts Secret key (SK) and Cipher text (CT) to produce decrypted data.

3.1 Overview

The CP-ABE Based Mobile cloud computing application for secure data sharing framework is shown in Fig. 1. Data owner (DO): Data owner encrypt data then upload the data onto mobile cloud storage. and DO is govern the access strategy and its attributes.

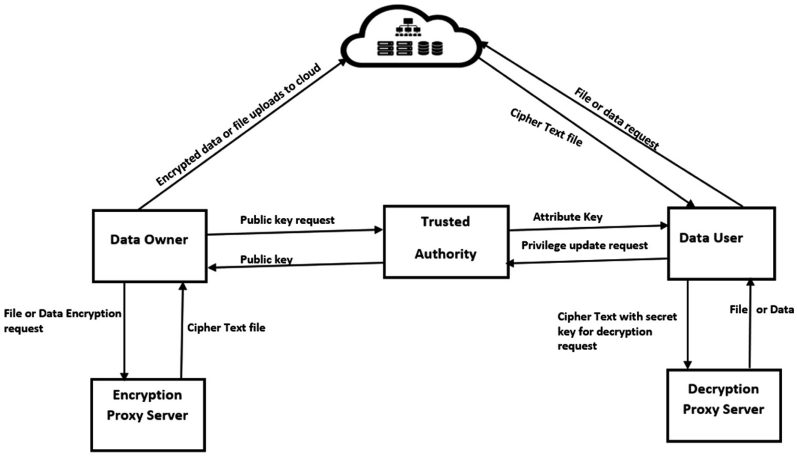

Fig. 1. CP-ABE based mobile cloud computing for secure data sharing framework

Data Users (DU): Data User is used to retrieve data from the mobile cloud environments.
Trusted Authority (TA): TA is performing the role of key generation and distribution. Overall operations of this framework will be explained in the following paragraph.

DO register with cloud and Trusted Authority cloud provides encrypted storage facility. And Trusted authority TA will generate the public key for data owner. DO states the policy that decides how access the data and encryption is outsourced to Encryption proxy server (EPS) to decrease the computational load at mobile cloud. EPS returns Encrypted data to data owner for uploading on to cloud. Trusted authority generates the keys and sends to data users and data owner.

Data user request the decrypted file from the cloud. if the access privileges match then request sent to cloud for access. else request will be sent to DO, meanwhile data owner has option to revoke the users from accessing the data. DO checks the user authenticity by verifying the access policy and his credentials if it found correct secret key will be shared through email-id. users decode the data or file with help of the secret key shared by data owner.

4 Proposed System Performance Analysis

In this section, we inspect the efficiency of proposed system CP-ABE Based Mobile cloud application for secure data sharing.

4.1 Experimental Settings

The test is performed on intel core i3 processor with 3.2 GHz CPU, 4 GB RAM, Windows 10 operating system and Prototype Application is developed in JAVA, JSP using NetBeans IDE, for data storage My SQL data base was used and for performance testing we used Apache JMeter application. Performance measure is evaluated by comparing the KP-ABE and CP - ABE schemes w.r.t security, time efficiency of Encryption and Key-Generation, Decryption.

Table 1. KP-ABE VS CP-ABE performance analysis (a) Encryption Time (b) Key-Generation Time (c) Decryption Time (d) Security ratio (f) Compative Analysis of KP-ABE and CP-ABE

Algorithm	File Size(MB)	Time (ms)
KP-ABE	100	93
CP-ABE	100	65

(a)

Algorithm	File Size(MB)	Time (ms)
KP-ABE	100	93
CP-ABE	100	65

(b)

Algorithm	Attributes	Time (secs)
KP-ABE	100	0.348
CP-ABE	100	0.251

(c)

Algorithms	Time (ms)
KP-ABE	80
CP-ABE	55

(d)

Algorithm	Security Performance in (%)
KP-ABE	60%
CP-ABE	92.91%

(e)

Parameters	**KP-ABE**	**CP-ABE**	**Analysis**
Encryption Time(ms)	93	65	**-28**
Decryption Time(sec)	0.348	0.251	**-0.09**
Key-Generation Time(ms)	80	55	**-25**
Security Performance in(%)	**60**	**92.91**	**32.91**

(f)

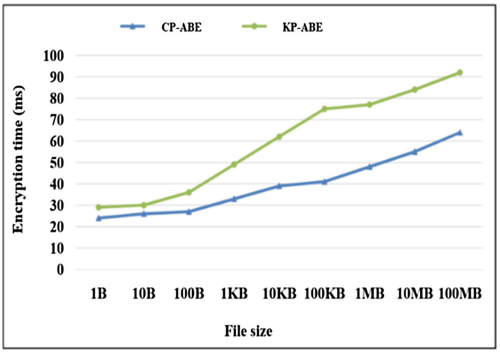

Fig. 2. Encryption time analysis

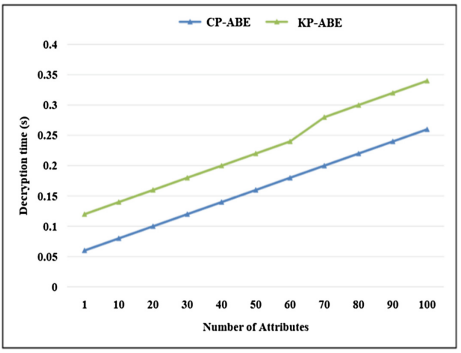

Fig. 3. Decryption time analysis

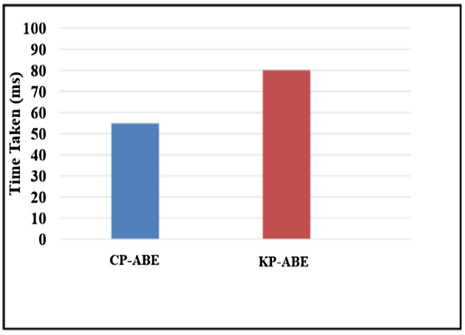

Fig. 4. Key generation time analysis

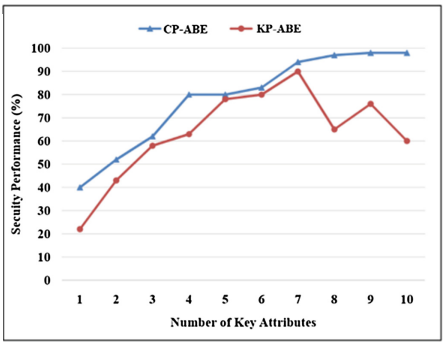

Fig. 5. Security performance analysis

4.2 Experimental Results

4.2.1 Encryption Time

The analysis of encryption time with varying file size. The increase in file size gradually increases the encryption time. In existing KP-ABE, the encryption time is more for maximum file sizes. But, the proposed CP-ABE offered the minimum time requirement as shown in Table 1(a). The graphical illustration of comparison between proposed CP-ABE and KP-ABE is depicted in Fig. 2 The encryption time for maximum file size (100 MB) the encryption time will be 93 ms and 65 ms respectively. the encryption time for CP-ABE is 65 ms which is less compared to KP-ABE Method. AQ3

4.2.2 Decryption Time

The proposed CP-ABE offered the minimum time compared to KP-ABE Algorithm as shown in Table 1(c). Fig. 3 shows the visual representation of decryption time analysis with the number of attributes. The proposed CP-ABE consumes 0.251 s for and for the maximum attributes (100) the CP-ABE and KP-ABE offers 0.251 and 0.348 s respectively. Hence, the proposed CP-ABE offers 90 ms lesser decryption time than the KP-ABE for minimum and maximum attributes respectively.

4.2.3 Key Generation Time

The proposed CP-ABE offered the minimum time compared to KP-ABE Algorithm as shown in Table 1(b).the comparative analysis is graphically presented in the following Fig. 4 The time required for key generation in KP-ABE method and proposed CP-ABE are 80 and 55-mile seconds respectively. From the comparative analysis, the proposed CP-ABE offered 25 ms reduction compared to existing methods respectively.

4.2.4 Security Analysis

The proposed CP-ABE offered the better amount of security compared KP-ABE Algorithm as shown in Table 1(e). The graphical representation of comparative analysis between the security performance and minimum number of attributes is illustrated in Fig. 5 The proposed CP-ABE offered the better security performance compared to the existing methodologies for the maximum number of attributes. For the maximum attribute of 14, the security performance for CP-ABE is 92.91 which is maximum compared to KP-ABE method.

5 Conclusion

In this paper, we have implemented CP-ABE Based Mobile Cloud Application for a secured data sharing. Our formulated results optimize time and security progressively. The performance of proposed CP-ABE is improved in terms of encryption time, decryption time, key generation time and security ratio respectively. The resultant values are −28, 0.09, −25, 32.91. Both KP-ABE and CP-ABE Results are shown quantitively and qualitatively by state-of-the-art algorithms. Our proposed methodology increases the time efficiency in mobile cloud and offers better secure data sharing. In the future it would be interesting to apply the method for the increased file size and incorporates the mobile cloud domain knowledge.

References

1. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute based encryption. In: IEEE Symposium Security and Privacy, Oakland, CA (2007)
2. Tysowski, P.K., Hasan, M.A.: Cloud-hosted key sharing towards secure and scalable mobile applications in clouds. In: 2013 International Conference on Computing, Networking and Communications (ICNC), San Diego, CA (2013)
3. Gupta, C.P., Sharma, I.: A fully homomorphic encryption scheme with symmetric keys with application to private data processing in clouds. In: 2013 Fourth International Conference on the Network of the Future (NoF), Pohang (2013)
4. Jin, Y., Tian, C., He, H., Wang, F.: A secure and lightweight data access control scheme for mobile cloud computing. In: 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, Dalian, pp. 172–179 (2015)
5. Yasumura, Y., Imabayashi, H., Yamana, H.: Attribute-based proxy re-encryption method for revocation in cloud storage: reduction of communication cost at re-encryption. In: 2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA), Shanghai, pp. 312–318 (2018)

AQ4

6. Liu, X., Zhang, Y., Wang, B., Yan, J.: Mona: secure multi-owner data sharing for dynamic groups in the cloud. IEEE Trans. Parallel Distrib. Syst. **24**(6), 1182–1191 (2015)
7. Chu, C.K., Sherman, S., Chow, M., Tzeng, W.G., Zhou, J., Deng, R.H.: Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Trans. Parallel Distrib. Syst. **25**(2), 468–477 (2014)
8. Fu, A., Yu, S., Zhang, Y., Wang, H., Huang, C.: NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users. IEEE (99), 1 (2017)
9. Alansari, S., Paci, F., Margheri, A., Sassone, V.: Privacy-preserving access control in cloud federations. In: 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, CA, pp. 757–760 (2017)
10. Anup, R.N., et al.: Attribute-based encryption techniques in cloud computing security: an overview. Int. J. Comput. Trends Technol. **4**(3), 419–422 (2013). ISSN 2231-2803
11. Praveena, A., Smys, S.: Ensuring data security in cloud based social networks. In: 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA) 20 April 2017, vol. 2, pp. 289–295. IEEE (2017)
12. Sridhar, S., Smys, S.: A survey on cloud security ıssues and challenges with possible measures. In: International Conference on Inventive Research in Engineering and Technology 2016 , vol. 4 (2016)

AQ6

Author Query Form

Book ID : **482990_1_En**

Chapter No : **64**

Please ensure you fill out your response to the queries raised below and return this form along with your corrections.

Dear Author,

During the process of typesetting your chapter, the following queries have arisen. Please check your typeset proof carefully against the queries listed below and mark the necessary changes either directly on the proof/online grid or in the 'Author's response' area provided below

Query Refs.	Details Required	Author's Response
AQ1	This is to inform you that corresponding author has been identified as per the information available in the Copyright form.	
AQ2	As per Springer style, the name of an author is presented with the abbreviated initials first and then the expanded names. Accordingly, we have transposed author names "Kirankumar B.G" so that it will appear in the final proof as: Prakash H. Unki, Suvarna L. Kattimani , B. G. Kirankumar (in Chapter First page) P. H. Unki et al. (in Running heads). Please confirm if this is fine.	
AQ3	Please note that the figures/tables are renumbered to ensure sequential order of citations. Please check and confirm the change.	
AQ4	References [2–9, 11, 12] are given in the list but not cited in the text. Please cite them in text or delete them from the list.	
AQ5	As Ref. [8] and [10] are same, we have deleted the duplicate reference and renumbered accordingly. Please check and confirm.	
AQ6	Kindly provide complete detail for Ref. [8].	

MARKED PROOF

Please correct and return this set

Please use the proof correction marks shown below for all alterations and corrections. If you wish to return your proof by fax you should ensure that all amendments are written clearly in dark ink and are made well within the page margins.

Instruction to printer	*Textual mark*	*Marginal mark*
Leave unchanged	··· under matter to remain	New matter followed by
Insert in text the matter indicated in the margin		or (x2)
Delete	through single character, rule or underline or through all characters to be deleted	or (x2)
Substitute character or substitute part of one or more word(s)	through letter or through characters	new character or new characters
Change to italics	under matter to be changed	
Change to capitals	under matter to be changed	
Change to small capitals	under matter to be changed	
Change to bold type	under matter to be changed	
Change to bold italic	under matter to be changed	
Change to lower case	Encircle matter to be changed	
Change italic to upright type	(As above)	
Change bold to non-bold type	(As above)	
Insert 'superior' character	through character or where required	or under character e.g. or
Insert 'inferior' character	(As above)	over character e.g.
Insert full stop	(As above)	
Insert comma	(As above)	
Insert single quotation marks	(As above)	or and/or or
Insert double quotation marks	(As above)	or and/or or
Insert hyphen	(As above)	
Start new paragraph		
No new paragraph		
Transpose		
Close up	linking characters	
Insert or substitute space between characters or words	through character or where required	
Reduce space between characters or words	between characters or words affected	