





Materials Today: Proceedings

Volume 80, Part 3, 2023, Pages 3059-3063

Security on mobile cloud computing using cipher text policy and attribute based encryption scheme

Madireddy Swetha ^a  , M. Latha ^b

Show more 

 Share  Cite

<https://doi.org/10.1016/j.matpr.2021.06.462> 

[Get rights and content](#) 

Referred to by [5 NANO 2021 – EXPRESSION OF CONCERN – PART 5](#)
Materials Today: Proceedings, Volume 80, Part 3, 2023, Pages 1705

 [View PDF](#)

Abstract

Mobile Cloud Computing (MCC) is a new paradigm that has been emerged by the advances in the Cloud Computing for Mobile devices to access Cloud services. The data security challenges against the data thefting, deleting, corrupting, or exploiting are existed as the data storage and access to/from the cloud has been most popular. In order to handle these data security issues in the cloud and to provide protection for the data, some innovative encryption methods have been developed. One of such encryption methods is Attribute-Based Encryption (ABE) that has a more control on the data in cloud as which is accessed by whom. Since from the recent years, many of academic researchers have paying a widespread of attention on using advanced cryptographic techniques to securely store,

process, also share data over the untrusted cloud environment. One of the promising cryptographic techniques which can solve the open challenge of regulating the fine-grained access control of important data over the distributed cloud is the Cipher text Policy – Attribute Based Encryption (CP-ABE). Therefore, a survey of work is presented in this paper on different CP-ABE methods for the secure mobile cloud computing architecture. This paper presents some works that are focused on secure data storing, accessing and sharing using CP-ABE methods over the untrusted cloud environments. All the works that are studied are analyzed and compared with each other in the results to find the best out of it.

Introduction

The persistent access can be empowered by the distributed computing for the information resources. The information management systems such as remote information storage, calculation of outsourced label, etc. can provide cloud servers over distribute computing environment. Then such cloud servers are used along with the CP-ABE methods and Verifiable Delegation (VD) approaches in order to ensure the data protection and the undisputed status of the appointment [1]. Fig. 1. Fig. 2. Fig. 3. Fig. 4. Table 1.

Two types of attribute-based encryptions are there in which first one is the Key Policy-Attribute Based Encryption (KP-ABE) and second one is the Cipher text based-ABE (CP-ABE). The key dealer determines the access control model to be taken in the middle of KP-ABE framework instead of enciphering which limits that framework usage and incentive in sensible applications [2]. The cipher text in this CP-ABE scheme identified within actuality related to maintaining access structure. Then the all attributes are gathered to label every unopened secret key. The user can get an access to encrypted data file if and only if the privilege of his/her cipher text matches with the privilege of access control model's predefined cipher text. Obviously, this method is theoretically closer to the previous access control models.

On the other hand, the access control model for universal framework is the most ingrained type of category criteria in the middle of an ABE framework which the devices express a predetermined program [3]. Some of the previous methods addressed for the secure mobile cloud computing environment are surveyed and three of the works are presented in this paper. At last all the works are analyzed and compared in the result which may help the researchers who are doing works under finding the reliable security framework for the mobile cloud computing environment.

Access through your organization

Check access to the full text by signing in through your organization.

Access through **your organization**

Section snippets

A brief review of Cp-Abe

The private data to be shared to all data users is the wish of data owner. Suppose the cloud is utilized to save the data [4]. The data owner gives access to all data users to access the data rather than giving permission to individual data users. All the data users can only access data when they have proper attributes to access data of others or else cannot access the data. An Access Policy is applied by DO for this private data. If the attributes of the users and access policy are matched

RS-CP attribute based encryption scheme

A scalable, flexible and fine-grained access control method is developed and implemented with Cipher text Policy-Attribute Based Encryption (CP-ABE) like an effective cryptographic technique. But the computation cost, overhead of data owner and revocation are some of the challenges faced by the existed CP-ABE based techniques. Such challenges can be addressed in the paper [5] by proposing a Revocable Sliced-Cipher text Policy ABE (RS-CP ABE) in which splitting algorithm is applied. In this

Result analysis

In this result analysis section, all the results and performance evaluation of four papers that are surveyed in this paper are studied and then a comparison among those schemes can be carried out and a tabular form is given to show the comparison analysis. Here, in paper [5] the CP-ABE scheme is implemented in mobile cloud computing environment which provide a fine-grained access control. It uses a splitting algorithm with re-encryption in revocation scheme and key is updated when there is a

Conclusion

In general, one of the most widely used schemes to deal with the security challenges of data in the cloud environment is CP-ABE. This method has provided a finite level of scalability and flexibility to eliminate the requirement of data owners for managing every single request. Therefore, for this a fine-grained access control model is maintained by each data owner and they issue the access to the user if he/she had proper attributes. In this paper four papers that addressed this CP-ABE scheme

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

[Special issue articles](#) [Recommended articles](#)

References (15)

K Xue, J Hong and Y Xue, "TAFC: time and attribute factors combined access control for time-sensitive data in public...

C. Ma *et al.*

Scalable access control for privacy-aware media sharing

IEEE Transaction on Multi. Pp (2019)

Li J, Chen N and Y. Zhang, "Extended file hierarchy access control scheme with attribute-based encryption in cloud...

W. Li *et al.*

Unified fine-grained access control for personal health records in cloud computing

IEEE Journal of Biomedical on Health PP (2019)

L.A. Saidane *et al.*

Revocable Sliced CipherText Policy Attribute Based Encryption Scheme in Cloud Computing

15th Inter. Wirel. Comm. & Mobile Comput. Confe. (IWCMC) (2019)

Baocang Wang, Zhenhua Liu, Yan Liu and Jing Xu, "Updatable Ciphertext-Policy Attribute-Based Encryption Scheme With...

Q.i. Li *et al.*

Qi Li, Yinghui Zhang Jingjing Guo and Youliang Tian, "Efficient privacy-preserving access control of mobile multimedia data in cloud computing", IEEE

Access (2019)

There are more references available in the full text version of this article.

Cited by (0)

[View full text](#)

© 2021 Elsevier Ltd. All rights reserved. Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.



All content on this site: Copyright © 2024 Elsevier B.V., its licensors, and contributors. All rights are reserved, including those for text and data mining, AI training, and similar technologies. For all open access content, the Creative Commons licensing terms apply.

