IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

A Lightweight Secure knowledge Sharing theme for Mobile Cloud Computing

[1] D. Bhanu Pratap, [2] CH.D. Sunil Kumar, [3] K.Dumas Sam, [4] P.Goutham, [5] A.Raghavulu
[1][2][3][4][5] Narayana Engineering College, Gudur.

Abstract: With the recognition of cloud computing, mobile devices will store/retrieve personal knowledge from anyplace at any time. Consequently, the information security drawback in mobile cloud becomes additional and additional severe and prevents additional development of mobile cloud. There square measure substantial studies that are conducted to enhance the cloud security. However, most of them don't seem to be applicable for mobile cloud since mobile devices solely have restricted computing resources and power. Solutions with low process overhead square measure in nice want for mobile cloud applications. during this paper, we tend to propose a light-weight knowledge sharing theme (LDSS) for mobile cloud computing. It adopts CP-ABE, AN access management technology employed in traditional cloud surroundings, however changes the structure of access management tree to create it appropriate for mobile cloud environments. LDSS moves an outsized portion of the process intensive access management tree transformation in CP-ABE from mobile devices to external proxy servers. what is more, to cut back the user revocation value, it introduces attribute description fields to implement lazy-revocation, that could be a thorny issue in program based mostly CP-ABE systems. The experimental results show that LDSS will effectively cut back the overhead on the mobile device aspect once users square measure sharing knowledge in mobile cloud environments.

Index Terms—mobile cloud computing, encryption, access management, user revocation one

INTRODUCTION

ith the event of cloud computing and therefore the quality of good mobile devices, folks square measure bit by bit obtaining familiar with a replacement era of information sharing model during which the information is hold on on the cloud and therefore the mobile devices square measure accustomed store/retrieve the information from the cloud. Typically, mobile devices solely have restricted cupboard space and computing power. On the contrary, the cloud has monumental quantity of resources. In such a state of affairs, to attain the satisfactory performance, it's essential to use the resources provided by the cloud service supplier (CSP) to store and share the information.

Nowadays, numerous cloud mobile applications are wide used. In these applications, folks (data owners) will transfer their photos, videos, documents and different files to the cloud and share these knowledge with others (data users) they wish to share. CSPs conjointly offer knowledge management practicality for knowledge homeowners. Since personal knowledge files square measure sensitive, knowledge home owners square measure allowed to settle on whether or not to create their knowledge files public or will solely be shared with specific knowledge users. Clearly, knowledge privacy of the private sensitive knowledge could be a huge concern for several knowledge home owners.

The progressive privilege management/access management mechanisms provided by the CSP square measure either not adequate or not terribly convenient. They can not meet all the necessities of information homeowners. First, once folks transfer their knowledge files onto the cloud, they're going the information in a very place wherever is out of their management, and therefore the CSP might spy on user knowledge for its business interests and/or different reasons. Second, folks need to send arcanum to every knowledge user if they solely need to share the encrypted knowledge with sure users, that is incredibly cumbersome. To alter the privilege management, {the knowledge| the info| the information} owner will divide data users into completely different teams and send arcanum to the teams that they need to share the information. However, this approach needs fine-grained access management. In each cases, arcanum management could be a huge issue.

Apparently, to unravel the on top of issues, personal sensitive knowledge ought to be encrypted before uploaded onto the cloud so the information is secure against the CSP. However, the information cryptography brings new issues. the way to offer economical access management mechanism on cipher text secret writing so solely the licensed users will access the plaintext knowledge is difficult. Additionally, system should provide knowledge homeowners effective user privilege management capability, so that they will grant/revoke knowledge access privileges simply on the information

IFERP connecting engineers... developing research

users. There are substantial researches on the difficulty of information access management over ciphertext. In these researches, they need the subsequent common assumptions. First, the CSP is taken into account honest and curious. Second, all the sensitive knowledge square measure encrypted before uploaded to the Cloud. Third, user authorization on sure knowledge is achieved through encryption/decryption key distribution. In general, we will divide these approaches into four categories: straightforward ciphertext access management, hierarchal access management, access management supported absolutely homomorphic cryptography and access management supported attribute-based
Security Assumptions

2.2.1 Semi-trusted Server

LDSS is intended below a similar assumptions projected in zero that the CSP is honest however curious, which suggests that the CSP can reliably execute the operations requested by users, however it'll peek on what users have hold on within the cloud. The CSP can reliably store users' knowledge, undertake AN initial access management, update knowledge in keeping with users' requests. However, CSP might do malicious actions appreciate collusion with users to urge the information in plain text.

In LDSS, proxy cryptography server and proxy secret writing server square measure introduced to help users to cipher and rewrite knowledge so user-side overhead is reduced. In essence, proxy servers are machines within the cloud. Thus, we tend to take into account that they're honest however curious even as the CSP.

2.2.2 trust worthy Authority

In this paper, to create LDSS possible in follow, a trustworthy authority (TA) is introduced. it's accountable of generating public and personal keys, and distributing attribute keys to users. With this mechanism, users will share and access knowledge while not being alert to the cryptography and secret writing operations.

We assume atomic number 73 is entirely credible, and a trustworthy channel exists between the atomic number 73 and each user. The very fact that a trustworthy channel exists doesn't mean that the information is shared through the trustworthy channel, for the information is in a very great amount. Atomic number 73 is barely accustomed transfer keys (in alittle amount) firmly between users. Additionally, it's requested that atomic number 73 is on-line all the time as a result of knowledge users might access knowledge at any time and wish atomic number 73 to update attribute keys.

Encryption (ABE) of these proposals square measure designed for non-mobile cloud surroundings. They consume great amount of storage and computation resources, that don't seem to be accessible for mobile devices. In keeping with the experimental leads to, the fundamental ABE operations take for much longer time on mobile devices than portable computer or desktop computers. It's a minimum of twenty seven times longer to execute on a wise phone than a private laptop (PC). This suggests that AN cryptography operation that takes one minute on a computer can take concerning 0.5 AN hour to end on a mobile device. What is more, current solutions don't solve the user privilege modification drawback all right. Such AN operation may lead to terribly high revocation value. This is often not applicable for mobile devices similarly. Clearly, there's no correct resolution which might effectively solve the secure knowledge sharing drawback in mobile cloud. Because the mobile cloud becomes additional and additional in style, providing AN economical secure knowledge sharing mechanism in mobile cloud is in imperative want.

To address this issue, during this paper, we tend to propose a light-weight knowledge Sharing theme (LDSS) for mobile cloud computing surroundings.

The main contributions of LDSS square measure as follows:

(1) We tend to style AN rule referred to as LDSS-CP-ABE supported Attribute-Based cryptography (ABE) technique to supply economical access management over ciphertext.

(2) We tend to use proxy servers for cryptography and secret writing operations. In our approach, process intensive operations in ABE square measure conducted on proxy servers, that greatly cut back the process overhead on shopper aspect mobile devices. Meanwhile, in LDSS-CP-ABE, so as to take care of knowledge privacy, a version attribute is additionally additional to the access structure. The secret writing key format is changed so it is sent to the proxy servers in a very secure approach.

(3)We tend to introduce lazy re-encryption and outline field of attributes to cut back the revocation overhead once addressing the user revocation drawback.

(4) Finally, we tend to implement an information sharing epitome framework supported LDSS. The experiments show that LDSS will greatly cut back the overhead on the shopper aspect,that solely introduces a smallest extra value on the server aspect. Such AN approach is useful to implement a practical knowledge sharing security the meon mobile devices. The results conjointly show that

LDSS has higher performance compared to the prevailing ABE based mostly access management schemes over ciphertext.

The rest of this paper is organized as follows. Section a pair of presents some elementary ideas in secure mobile cloud knowledge sharing and therefore the security premise. Section three provides the elaborated style of LDSS. Section four and five provide the security assessment and performance analysis, severally. Section sixpresents connected works. Finally, Section seven concludes our work with the longer term work.

2 PRELIMINARIES AND ASSUMPTIONS

In this section, we tend to initial shortly gift the technique preliminaries closely involving LDSS, and so gift the system model and a few security assumptions in LDSS.

2.1 Preliminary Techniques

2.1.1 Additive Pairing

In our implementation, we tend to typically take as a bunch consisting points on AN elliptic curve, as a increasing subgroup of a finite field, e as a Weil or the poet pairing supported AN elliptic curve over a finite field. Additional descriptions on however these parameters square measure outlined and generated is found in.

2.1.2 Attribute-Based cryptography

Attribute-based cryptography (ABE) is projected by Sahai and Waters [29]. it's derived from the Identity-Based cryptography (IBE) and is especially appropriate for one-to-many knowledge sharing eventualities in a very distributed and open cloud surroundings. Attribute-based cryptography is split into 2 categories: one is that the Ciphertext-Policy Attribute based mostly cryptography (CP-ABE), during which the access management policy is embedded into ciphertext; the opposite one is Key- Policy Attribute based mostly cryptography (KP-ABE), during which the access management policy is embedded within the user's key attributes. In real applications, CP-ABE is additional appropriate since it resembles role-based access management. In CP-ABE, {the knowledge| the info |the information} owner styles the access management policy and assigns attributes to data users. A user will rewrite the information properly if the user's attributes satisfy the access management policy.

2.1.3 Secret Sharing theme

S Shamir secret sharing theme [30] is employed to shield secret info. It is explained as below. Assume that p could be a prime quantity, the key info to share is . Divide k into n pieces through the following steps: p Z K k = ∈

(1) indiscriminately choose one (t-1)-order polynomial , and let .] [...) (0 1 1 1x Z a x a x a x h p t t ∈ + + + = – – k a= 0

(2) choose n non-zero and distinct parts Xi from Zp, calculate . n i xhyi i ≤ ≤ = 1)

(3) Distribute as shares and publish the corresponding.) 1(ni yi ≤ ≤ n xxx,...,, 2 1

Computational Overhead with completely different CP-ABE Schemes

DO's overhead in several ABE schemes is shown in Table four. As shown in Table four, in existing programs, the overhead on mobile user DU's aspect is proportional to the quantity of attributes in access management policy. In LDSS, the overhead could be a little constant worth.

Measurement of process Overhead of LDSS

We live the process overhead of LDSS through experiments. The results square measure as follows.

(1) Registration value

The average registration time for one user is 50ms.

(2) Authorization value

The time required for authorization is proportional to the quantity of attributes in hand by DU. Fig. seven shows the time required for user authorization once the quantity of attributes in hand by user is a pair of,4,8,16,32.

As is seen in Fig. 7, the time of authorization is proportional to the quantity of attributes in each BSW CP-ABE and LDSS.

In each eventualities, the authorization time remains below 1s once the quantity of attributes rises to thirty two. Authorization time in LDSS is simply slightly longer as a result of it introduces the version attribute.

CONCLUSION AND FUTURE WORK

In recent years, several studies on access management in cloud square measure supported attribute-based cryptography rule (ABE). However, ancient ABE isn'tappropriate for mobile cloud as a result of it's computationally intensive and mobile devices solely have restricted resources. during this paper, we tend to propose LDSS to deal with this issue. It introduces a unique LDSS-CP-ABE rule to migrate major computation overhead from mobile devices onto proxy servers, therefore it will solve the secure knowledge sharing drawback in mobile cloud. The experimental results show that LDSS will guarantee knowledge privacy in mobile cloud and cut back the overhead on users' aspect in mobile cloud. within the future work, we are going to style new approaches to confirm knowledge integrity. To additional faucet the potential of mobile cloud, we are going to conjointly study the way to do ciphertext retrieval over existing knowledge sharing schemes.

REFERENCES

[1] upper crust C, Halevi S. Implementing gentry's fully-homomorphic cryptography theme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.
[2] Brakerski Z, Vaikuntanathan V. economical absolutely homomorphic cryptography from (standard) LWE. in: continuing of IEEE conference on Foundations of engineering. California, USA: IEEE press, pp. 97-106, Oct. 2011.
[3] Qihua Wang, Hongxia Jin. "Data run mitigation for discertionary access management together clouds". the sixteenth ACM conference on Access management Models and Technologies (SACMAT), pp.103-122, Jun. 201

IFERP connecting engineers... developing research