International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 15
May 2018

Secure LDSS : Effective reduction of overhead for sharing data in mobile cloud environments.

Md Mudassir Ghori[1] and Md Ateeq Ur Rahman[2],

[1]*Research Scholar, Dept. of Computer Science & Engineering,*
SCET, Hyderabad, India
shadan.16081d7812@gmail.com
[2]*Professor and Head, Dept. of Computer Science & Engineering,*
SCET, Hyderabad, India
shadan.authors1@gmail.com

Abstract - With the recognition of cloud computing, mobile devices will store/retrieve personal information from anyplace at any time. Consequently, the information security downside in mobile cloud becomes more and more severe and prevents more development of mobile cloud. There square measure substantial studies that are conducted to boost 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 procedure overhead square measure in nice want for mobile cloud applications. during this paper, we tend to propose a light-weight information sharing theme (LDSS) for mobile cloud computing. It adopts CP-ABE, AN access management technology utilized in traditional cloud atmosphere, however changes the structure of access management tree to create it appropriate for mobile cloud environments. LDSS moves an oversized portion of the procedure intensive access management tree transformation in CP-ABE from mobile devices to external proxy servers. what is more, to scale back the user revocation price, 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 scale back the overhead on the mobile device facet once users square measure sharing information in mobile cloud environments.

Index Terms—mobile cloud computing, data encryption, access control, user revocation.

I. INTRODUCTION

With the event of cloud computing and therefore the quality of sensible mobile devices, individuals are step by step obtaining familiar with a brand new era of knowledge sharing model during which the info is keep on the cloud and therefore the mobile devices ar wont to store/retrieve the info from the cloud. Typically, mobile devices solely have restricted space for storing and computing power. On the contrary, the cloud has huge quantity of resources. In such a state of affairs, to realize the satisfactory performance, it's essential to use the resources provided by the cloud service supplier (CSP) to store and share the info.

Nowadays, numerous cloud mobile applications are wide used. In these applications, individuals (data owners) will transfer their photos, videos, documents and alternative files to the cloud and share these information with people (data users) they wish to share. CSPs additionally offer information management practicality for information homeowners. Since personal information files are sensitive, information homeowners are allowed to decide on whether or not to form their information files public or will solely be shared with specific information users. Clearly, information privacy of the non-public sensitive information could be a huge concern for several information homeowners.

The progressive privilege management/access management mechanisms provided by the CSP are either not sufficient or not terribly convenient. they can not meet all the necessities of knowledge homeowners. First, once individuals transfer their information files onto the cloud, they're deed the info in a very place wherever is out of their management, and therefore the CSP could spy on user information for its business interests and/or alternative reasons. Second, individuals need to send secret to every information user if they solely wish to share the encrypted information with bound users, that is extremely cumbersome.

To modify the privilege management, {the information|the info|the information} owner will divide data users into totally different teams and send secret to the teams that they need to share the info. However, this approach needs fine-grained access management. In each cases, secret management could be a huge issue.

Apparently, to unravel the higher than issues, personal sensitive information ought to be encrypted before uploaded onto the cloud in order that the info is secure against the CSP. However, the info secret writing brings new issues. a way to offer economical access management mechanism on ciphertext secret writing in order that solely the approved users will access the plaintext information is difficult. additionally, system should provide information homeowners effective user privilege management capability, so that they will grant/revoke information access privileges simply on the info users. There are substantial researches on the difficulty of knowledge 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 information are encrypted before uploaded to the Cloud. Third, user authorization on bound information is achieved through encryption/decryption key distribution. In general, we are able to divide these approaches into four categories: easy ciphertext access management, hierarchic access management, access management supported totally homomorphic secret writing [1][2] and access management supported attribute-basedencryption (ABE). of these proposals are designed for non-mobile cloud atmosphere. They consume great deal of storage and computation resources, that aren't on the market for mobile devices. consistent with the experimental leads to, the fundamental ABE operations take for much longer time on mobile devices than laptop computer or desktop computers. it's a minimum of twenty seven times longer to execute on a sensible phone than a private laptop (PC). this suggests that an secret writing operation that takes one minute on a computer can take regarding 0.5 an hour to end on a mobile device.

Furthermore, current solutions don't solve the user privilege amendment downside o.k.. Such an operation may lead to terribly high revocation value. this can be not applicable for mobile devices in addition. Clearly, there's no correct answer which may effectively solve the secure information sharing downside in mobile cloud. because the mobile cloud becomes a lot of and a lot of standard, providing an economical secure information sharing mechanism in mobile cloud is in imperative want.

To address this issue, during this paper, we have a tendency to propose a light-weight information Sharing theme (LDSS) for mobile cloud computing atmosphere.

The main contributions of LDSS are as follows:

(1) we have a tendency to style an algorithmic program referred to as LDSS-CP-ABE supported Attribute-Based secret writing (ABE) technique to supply economical access management over ciphertext.

(2) we have a tendency to use proxy servers for secret writing and secret writing operations. In our approach, machine intensive operations in ABE ar conducted on proxy servers, that greatly scale back the machine overhead on consumer aspect mobile devices. Meanwhile, in LDSS-CP-ABE, so as to take care of information privacy, a version attribute is additionally additional to the access structure.

The secret writing key format is changed in order that it will be sent to the proxy servers in a very secure means.

(3) we have a tendency to introduce lazy re-encryption and outline field of attributes to cut back the revocation overhead once handling the user revocation downside.

(4) Finally, we have a tendency to implement an information sharing model framework supported LDSS. The experiments show that LDSS will greatly scale back the overhead on the consumer aspect, that solely introduces a lowest extra value on the server aspect. Such an approach is useful to implement a practical information sharing security theme on mobile devices.

The results additionally show that LDSS has higher performance compared to the prevailing ABE based mostly access management schemes over ciphertext.

II. Related Works

With the growing quality of cloud computing, a lot of and a lot of enterprises ar migrating their collaboration platforms from in-enterprise systems to software system as a Service (SaaS) applications. whereas SaaS collaboration has various benefits, it additionally raises new security challenges. specifically, since SaaS collaboration is more and more used across enterprise boundaries, organizations ar involved that sensitive data is also leaked to outsiders because of their employees' unintended mistakes on data sharing. during this article, we tend to propose to mitigate the information leak drawback in SaaS collaboration systems by reducing human errors. designed on prime of the discretionary access management model in existing collaboration systems, we've designed a series of mechanisms to produce defense full against data leak. First, we tend to permit enterprises to code their structure security rules as necessary access management policies, therefore on impose coarse-grained restrictions on their employees' discretionary sharing selections. Second, we tend to style associate degree attribute-based recommender that means and prioritizes potential recipients for users' files, reducing errors within the decisions of recipients. Third, our system actively examines abnormal recipients entered by a file owner, providing the last line of defense before a file is shared. we've enforced a epitome of our answer and performed experiments on knowledge collected from real-world collaboration systems.

Cloud computing is associate degree rising paradigm that permits on-demand network access to a shared pool of resources while not requiring in depth management efforts on behalf of the purchasers that need these resources. It will be differentiated from alternative classical computing models by 5 major characteristics akin to on-demand self-service, broad network access, resource pooling, fast physical property and measured service . Since a cloud atmosphere involves multiple resources happiness to multiple purchasers interacting in complicated manners, correct access management to those resources is incredibly vital. As delineate in Fig. 1, access management needs addressing 3 nonorthogonal sub issues of authorization, authentication and social control.

Authorization, that is expressed in terms of associate degree access management model, specifies the resources that require to be protected, what forms of accesses (operations) ar doable on these resources, and UN agency is allowed access to those resources. (2) Authentication, that is laid out in terms of protocols, addresses the matter of deciding UN agency is attempting to access a protected resource. (3) social control involves ensuring that associate degree entity that's allowed to access bound resources, gets to access these resources once requested, which associate degree entity that's not allowed is denied access. In clouds, these 3 aspects of access management ar achieved by the cooperation of 4 practical modules: one. Policy Administration purpose (PAP): PAP could be a repository for the authorization policies that ar expressed in terms of the actions. Subjects (i.e., human users, devices, processes, organizations, etc.) will withstand varied objects within the system. The authorization policies ar basically associate degree representation of the access management model tailored towards the organization. it's the most part for the authorization portion of access management. 2. Policy data purpose (PIP): PIP is that the module that combination the knowledge to judge associate degree authorization policy. it's the most part accountable for achieving authentication. 3. Policy call purpose (PDP): PDP gets relevant data from the PIP associate degreed consults the PAP to reach a choice whether or not to grant or deny an access request. 4. Policy social control purpose (PEP): ginger receives access requests from subjects within the external world, sends them to the PDP for analysis, and once receiving the grant or deny response from the PDP, ensures that the suitable action is taken.

The distinctive characteristics of cloud computing introduce novel challenges to every of the 3 aspects of access management, specifically to authorization. to start with, multi-tenancy ends up in the co-residency of machines (e.g., virtual machines (VMs) and info engines) and alternative resources (e.g., hardware or storage) owned by completely different purchasers within the same privileged position within the cloud. Tenant, client or user is usually utilized in cloud computing expression to mean consumer. we'll use these 3 terms interchangeably.

This makes security vulnerabilities at the cloud infrastructure level significantly crucial to the cloud atmosphere. A guest package (OS) will exploit vulnerabilities within the hypervisor [31] and run processes on alternative guests or the host. One such exploit was incontestible in a very recent work wherever the interior cloud infrastructure was mapped to spot wherever a target virtual machine (VM) is probably going to reside so that data was wont to mount cross-VM side-channel attacks to extract sensitive data from the target VM. In short, security breaches akin to unauthorized connections, unauthorized leak of data, unmonitored login makes an attempt, malware propagation etc., will arise in one consumer and doubtless propagate to a different simply.

It is, therefore, vitally vital that correct authorization policies use for the protection of tenant resources from un-authorized revelation and modification,segregation of tenants from each other, and isolation of computation, storage and network resources of the cloud supplier from tenants. A cloud-computing atmosphere being massively ascendable and elastic, is inherently terribly dynamic. This makes the matter of providing correct access management in clouds even more difficult. The accessing entities could amendment, resources requiring protection is also created or changed, associate degreed associate degree entity's access to resources could amendment throughout the course of an application execution. Users may have to dynamically acquire different permissions from different domains supported the services they have. Cloud collaboration will doubtless unfold across enterprise boundaries wherever interactions among entities usually occur in unexpected manners. The access-requesting entity might not be best-known beforehand by the access-granting entity

2.1 Existing System

The progressive privilege management/access management mechanisms provided by the CSP square measure either not adequate or not terribly convenient. they cannot meet all the necessities of knowledge house owners.

When individuals transfer their knowledge files onto the cloud, they're deed the info in a very place wherever is out of their management, and also the CSP might spy on user knowledge for its industrial interests and/or alternative reasons.

Second, individuals ought to send word to every knowledge user if they solely need to share the encrypted knowledge with bound users, that is extremely cumbersome. To modify the privilege management, data owner will divide data users into totally different teams and send word to the teams that they need to share the info. However, this approach needs fine-grained access management. In each cases, word management could be a massive issue.

III. PROPOSED SYSTEM

We style an algorithmic rule referred to as LDSS-CP-ABE supported Attribute-Based encoding (ABE) technique to supply economical access management over ciphertext.

We use proxy servers for encoding and decipherment operations. In our approach, procedure intensive operations in ABE area unit conducted on proxy servers, that greatly cut back the procedure overhead on consumer facet mobile devices. Meanwhile, in LDSS-CP-ABE, so as to keep up information privacy, a version attribute is additionally added to the access structure. The decipherment key format is changed so it is sent to the proxy servers in a very secure manner.

We introduce re-encryption and outline field of attributes to cut back the revocation overhead once addressing the user revocation downside.

IV. System Architecture

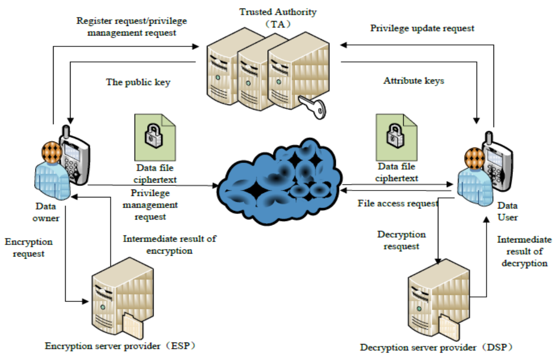
Trusted Authority (TA)
Register request/privilege management request
Privilege update request
The public key
Attribute keys
Data file ciphertext
Privilege management request
Data file ciphertext
File access request
Data owner
Data User
Encryption request
Intermediate result of encryption
Decryption resquest
Intermediate result of decryption
Encryption server provider (ESP)
Decryption server provider (DSP)

Figure 1: System Architecture of the Proposed System

We propose LDSS, a framework of light-weight data-sharing theme in mobile cloud (see Fig. 1). it's the subsequent six parts.

(1) knowledge Owner (DO): DO uploads knowledge to the mobile cloud and share it with friends. DO determines the access management policies.

(2) knowledge User (DU): DU retrieves knowledge from the mobile cloud.

(3) Trust Authority (TA): Ta is liable for generating and distributing attribute keys.

(4) cryptography Service supplier (ESP): ESP provides encryption operations for DO.

(5) decoding Service supplier (DSP): DSP provides knowledge decoding operations for DU.

(6) Cloud Service supplier (CSP): CSP stores the info for DO. It reliably executes the operations requested by DO, whereas it's going to peek over knowledge that DO has hold on within the cloud.

As shown in Fig. 1, a DO sends knowledge to the cloud. Since the cloud isn't credible, knowledge needs to be encrypted before it's uploaded. The DO defines access management policy within the style of access management tree (refer to Definition a pair of in Section three.2) on records to assign that attributes a DU ought to acquire if he desires to access a definite knowledge file. In LDSS, knowledge files ar all encrypted with the radially symmetrical cryptography mechanism, and also the radially symmetrical key for {data cryptography|encoding|encryption} is additionally encrypted mistreatment attribute based mostly encryption (ABE). The access management policy is embedded within the ciphertext of the radially symmetrical key. solely a DU UN agency obtains attribute keys that satisfy the access management policy will decipher the ciphertext and retrieve the radially symmetrical key. because the cryptography and decoding ar each computationally intensive, they introduce serious burden for mobile users. to alleviate the overhead on the shopper aspect mobile devices, cryptography service supplier (ESP) and decoding service supplier (DSP) ar used. each the cryptography service supplier and also the decoding service supplier are semi-trusted. we have a tendency to modify the normal CP-ABE formula and style Associate in Nursing LDSS-CP-ABE formula to make sure the info privacy once outsourcing process tasks to ESP and DSP.

V. CONCLUSION

In recent years, several studies on access management in cloud square measure supported attribute-based coding rule (ABE). However, ancient ABE isn't appropriate 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 handle this issue. It introduces a completely 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 scale back the overhead on users' aspect in mobile cloud. within the future work, we'll style new approaches to make sure knowledge integrity. To additional faucet the potential of mobile cloud, we'll additionally study the way to do ciphertext retrieval over existing knowledge sharing schemes.

References

[1] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.
[2] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011.
[3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.
[4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013.
[5] Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009.
[6] Maheshwari U, Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage. in: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation-Volume 4. USENIX Association, pp. 10-12, 2000.
[7] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.
[8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.
[9] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350-364
[10] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012.