International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Data Storage in Cloud with Fine Grained Attribute Encryption

[1]Pakkala Vamshi, [2]Mr.B.Krishna
[1]PG Scholar, Department of CSE, Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana, Mail ID: vamshi3232@gmail.com@gmail.com
[2]Assistant Professor, Department of CSE, Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana, Mail ID:bandikrishna007@gmail.com

Abstract:

With the development of cloud computing, outsourcing data to cloud server attracts lots of attentions. To guarantee the security and achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used in cloud storage system. However, user revocation is the primary issue in ABE schemes. In this article, we provide a ciphertext-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys. Notably, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. We prove the security of our scheme under the divisible computation Diffie-Hellman (DCDH) assumption. The result of our experiment shows computation cost for local devices is relatively low and can be constant. Our scheme is suitable for resource constrained devices.

I. INTRODUCTION

In this project, we provide a cipher text-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as

it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys

II. RELATED WORKS

A.text-Policy Attribute-Based Encryption AUTHORS:Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng Wan In several distributed systems a user can able to access data if a user posses a certain set of credentials or attributes. Presently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server stores the data, which is compromised, then the confidentiality of the data will be compromised. In this paper, we present a process for realizing complex access control on encrypted data that we say Cipher text-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; [2] moreover, our systems are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to explain the encrypted data and built policies into user‟s keys; while in our system attributes are used to explain a user‟s credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our systems are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we ensure an implementation of our system and give performance measurements. [1] **B. Multi-Authority Attribute Based Encryption With Honest-But-Curious Central Authority AUTHORS: Vladimir Bozovic , Daniel Socek , Rainer Steinwandt , and Viktoria I. Villanyi**

An attribute based encryption scheme capable of handling M. JOTHIRMYI, KARPURAPU SUDHAKAR BABU International Journal of Advanced Technology and Innovative Research Volume. 09, IssueNo.03, March-2017, Pages: 0512-0517 multiple authorities were recently proposed by Chase. The scheme is built upon a single-authority attribute based encryption technique presented earlier by Sahai and Waters. [6]-[9] Chase‟s construction uses a trusted central authority that is inherently able to do decrypting arbitrary cipher texts created within the system. We present a multi-authority attribute based encryption technique in which only the set of recipients defined by the encrypting party can decrypt a

corresponding cipher text. The central authority is shown as "honest-but-curious": on the one hand it honestly follows the protocol, and on the other it is curious to decrypt arbitrary cipher texts thus violating the intent of the encrypting party. The advance scheme, which like its predecessors relies on the Bilinear DiffieHellman assumption, has a complexity comparable to that of Chase"s technique. We prove that our scheme is secure in the selective ID model and can tolerate an honest-but-curious central authority. Building on the proposal for multi-authority based attribute based encryption from; we constructed a scheme where the central authority is no longer capable of decrypting arbitrary cipher texts created within the system. In addition to viewing security in the selective ID model, we showed that the proposed system can able to tolerate an honest-but-curious central authority. Since both Chase"s scheme and the proposed scheme rely on the same hardness assumption, and have a comparable complexity, the new scheme seems a viable alternative to Chase"s construction. However, since the proposed method is capable of handling a curious yet honest central authority, the proposed scheme is suggested in applications where security against such a central authority is required. [9]

C. Decentralizing Attribute-Based Encryption AUTHORS: Allison Lewko, University of Texas at Austin alewko@cs.utexas.edu We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In this process, any party can become an authority and there is no requirement for any world coordination other than the innovation of an initial set of common reference parameters. A party can simply plays as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in forms of any Boolean formula over attributes issued from any chosen set of authorities [7]. Finally, our process does not require any central authority. In constructing our system, our largest technical hurdle is to create it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE technique authority "tied" together different components (representing different attributes) of a user"s private key by randomizing the key. But in our system each component will come from a potentially different authority, where we think no coordination between such authorities. We

create new techniques to tie key components together and prevent collusion issues between users with different global identifiers. We prove our system secure using the new dual system encryption methodology where the security proof works by first converting the challenge cipher text and private keys to a half-functional form and then arguing security. We follow a recent variant of the dual system proof scheme due to Lewko and Waters and build our system using bilinear groups of Composite order. We prove security under same static assumptions to the LW paper in the random oracle model. For illegal key sharing. And for the half trusted authority, it‟s illegal key (re-)distributing misconduct could be caught and prosecuted. Furthermore, we have provided an auditor to judge whether a malicious user is naive or framed by the authority. As far as we know, this is the first CP-ABE technique that simultaneously encourages white-box traceability, accountable authority, public auditing. We have also proved that the new system is total protection in the standard model. Note that there exists a stronger notion for traceability called black-box traceability. In black-box scenario, the malicious user can hide.

D. Accountable Authority Cipher text-Policy Attributethe decryption algorithm by tweaking it, as well as the Based Encryption with White-Box Traceability and Public Auditing in the Cloud AUTHORS: Jianting Nin, Xiaolei Dong, Zhenfu Cao and Lifei Wei [3] As a sophisticated mechanism for secure well-grained access control, cipher text-policy attribute-based encryption (CP-ABE) is a highly promising solution for commercial applications like cloud computing. But there still exists one major issue awaiting to be solved, that is, the prevention of key abuse. The existing CP-ABE systems missed this critical functionality, hindering the wide utilization and commercial application of CP-ABE systems to date. Here we address two practical problems about the key abuse of CP-ABE: The key escrow problem of the half-trusted authority; and, The malicious key delegation problem of the users. For the semitrusted authority, its misconduct (i.e., illegal key (re-)distribution) should be caught and prosecuted. And for a user, his/her malicious conduct (i.e., illegal key sharing) need be traced. We affirmatively solve these two key abuse issues by proposing the first accountable authority CP-ABE with white box traceability that supports policies expressed in any monotone

access structures. And we provide an auditor to judge publicly whether a suspected user is guilty or is framed by the authority. In this process, we addressed two practical problems about the key abuse of CP-ABE in the cloud, and have presented an accountable authority CPABE technique supporting white-box traceability and public auditing. Specifically, the proposed system could trace the spiteful users decryption key. And in this case, the advanced system with white-box traceability in this paper will fail since both the decryption key and decryption algorithm are not good. In our future work, we will focus on constructing an accountable authority CP-ABE technique which is blackbox traceability and public auditing. [3]

III. SCOPE

It provides data security and achieves flexible &finegrained file access control . It handles revocation efficiently. It is collusion attack proof system. It fulfills the client's requirement cost effectively. It is high in performance. It is robust and reliable system

IV. PROPOSED SYSTEM:

In this system, we focus on designing a CP-ABE scheme with efficient user revocation for cloud storage system. We aim to model collusion attack performed by revoked users cooperating with existing users. Furthermore, we construct an efficient user revocation CP-ABE scheme through improving the existing scheme and prove our scheme is CPA secure under the selective model. To solve existing security issue, we embed a certificate into each user's private key. In this way, each user's group secret key is different from others and bound together with his private key associated with attributes. To reduce users' computation burdens, we introduce two cloud service providers named encryption-cloud service provider (E-CSP) and decryption-cloud service provider (DCSP). The duty of E-CSP is to perform outsourced encryption operation and D-CSP is to perform outsourced decryption operation.

IMPLEMENTATION MODULES:

Data Owner(DO)

Data User(DU)

Group Manager(GM)

Auditor Cloud Storage Server(CSS)

MODULES DESCRIPTION:

Data Owner (DO): In this module includes the Data Owner first register his

details and login. Next The Owner gives the request to Group Manager for Group Certificate. After receive the certificate DO can Upload a file to the Cloud and the file encrypted by the CP-ABE Algorithm. The Data Owner can also view the Files details and File contents in a Encrypted format. The Data Owner can only View his Group Files.

Data User (DU): In this module includes the Data User first register his details and login. Next The User gives the request to Group Manager for Group Certificate. After receive the certificate DU can View a file Details. If Data User wants to download the file means DU send the request to the Auditor for Secret Key of downloading permission. Auditor sends the Secret Key to Data User Mail id. Data User can download the file by using the Secret Key. Data User view and download his Group files only.

Group Manager (GM): In this Module Group Manager response Data Owner and Data User Group Certificate requests. Group Manager sends the Group Certificates to the DO and DU. Group Manager done the Users Revocation Process. Once the User is Revoked by GM then the user not able to access the files in the group and the user is unauthorized to login.

Auditor: In this Module the Auditor can view the Uploaded file details and Auditor response the Data Users Secret Key Requests for Downloading process. Auditor sends the Secret Key to the Data Users Mail id. Without this secret key Data User Cannot able to download the files.

Cloud Storage Server (CSS) : The Cloud Storage Server can view the Data Users and Data Owners Details.CSS can also view the File Details .and CSS view the revoked Users Details.

V. CONCLUSION

We provided a formal definition and security model-ABE with user revocation. We also constructed a concrete CP-ABE International Journal of Engineering Science and Computing, September 2017 14853 http://ijesc.org/ scheme which is CPA secure based on DCDH assumption. To resist collusion attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key through combining their private keys. Additionally, we outsource operations with high computation cost to reduce the user's computation burdens. Through applying the technique of outsource, computation cost for local devices is much lower and relatively

fixed. The results of our experiment show that our scheme is efficient for resource constrained devices.

REFERENCE:

[1]. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," EUROCRYPT'05, LNCS, vol. 3494, pp. 457-473, 2005.

[2]. J.Bethencourt, A.Sahai and B.Waters, "Ciphertext-Policy Attribute-Based Encryption,"Proc. IEEE Symposium on Security and Privacy, pp.321-334, May 2007, doi: 10.1109/SP. 2007.11

. [3]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "AttributeBased En-cryption for Fine-Grained Access Control of Encrypted Data,"Proc.13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89-98, 2006, doi: 10. 1145 /1180405.1180418.

[4]. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal of Computing, vol. 32, no. 3,pp. 586-615, 2003.

[5]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation,"Proc.15th ACM conference on Computer and communications security (CCS' 08),pp. 417- 426, 2008.

AUTHOR'SPROFILE:

Pakkala Vamshi,
PG Scholar, Department of CSE, Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana, Mail ID: vamshi3232@gmail.com@gmail.com

Mr.B.Krishna
Assistant Professor, Department of CSE, Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana, Mail ID:bandikrishna007@gmail.com