ISSN 2395-1621

Survey On Efficient user revocation for dynamic groups using cloud

[#1]V.A.Patil, [#2]Pratiksha Kute, [#3]Pritam Pardeshi, [#4]Smrutigandha Pathare

[1]vikasapatil123@gmail.com,
[2]pratiksha.kute1996@gmail.com,
[3]pritampardeshi729@gmail.com,
[4]smruti7gandha@gmail.com

[#1]Assistant Professor, Department of Computer engineering,
[#234]Students, Department of Computer engineering,

SITS Narhe Pune India.

ABSTRACT

The advent of cloud computing makes outsourcing storage becomes a rising trend, which promotes the secure remote data auditing a hot topic that appeared in search literature. Recently some research consider the problem public data integrity of the secure and integrity for audit shared dynamic data. However, these schemes are still not secure against the storage server collusion cloud and revoked group users during user revocation in practical cloud storage system. In this paper, we figure on collusion attack in the exiting scheme and provide an efficient public Integrity system audit with the secure user group revocation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme on the basic of our scheme definition. Our scheme supports the public checking and efficient user revocation and also some interesting properties, such as confidence, efficiency, count ability and traceability of secure group revocation of the user. Finally, security and experimental analysis show that, compared with its relevant schemes our scheme is also secure and efficient.

Keywords: **Public integrity auditing, dynamic data, group signature, privacy-preservation, shared data, Amazon cloud**

ARTICLE INFO

Article History

Received: 28st November 2016

Received in revised form :

28th November 2016

Accepted: 1st December 2016

Published online :

15th December 2016

I. INTRODUCTION

Cloud services providers offer users efficient and scalable data storage services with a much low marginal cost than traditional approach. It is routine for users to take advantage of cloud storage services to share data with other in a group, as data sharing is a standard feature on most cloud storage offerings, including Drop box, iCloud and Google Drive [4].

Digital signatures are becoming a fact of life. They are used in more and more products and protocols and one can a large amount of literature dealing with their applications find, variants and security. A digital group signature scheme addresses a group, perhaps a dynamic process, including users are called players (or simply embers) and most of the time a group of center(also called group leader), which is the authority with ability to "open" a signature in case of later dispute, and to and reveal the identity the actual signer. The structure of the underlying group is said to be dynamic if the number of users can increased by registering and adding new members[2].A scheme is publicly variables means capable check the integrity of data check can be achieved not only by the data owners, but also by any third party auditor. However the dynamic schemes above focus on the cases where there is a data owner and only the owner of the data may change data. To support multiple user data operation, Wan get al proposed a data integrity based on the signature of the ring. In the diagram, the user revocation problem is not considered and the audits cost is linear in the size of the group and data. To further improve the system and previous support group user revocation, Wang et al. designed a scheme based on proxy re-signatures. However, the plan assumes that the private and authenticated channels exist between each pare entities and there is no collusion between them. Also, the auditing cost of the scheme is linear to the group size. Another attempt to improve the previous scheme and to the scheme efficient, scalable and collusion resistant is

© 2016, IERJ All Rights Reserved

Yuan and Yu, who designed a dynamic public integrity auditing scheme with group user revocation [1].

II. PROPOSED SYSTEM

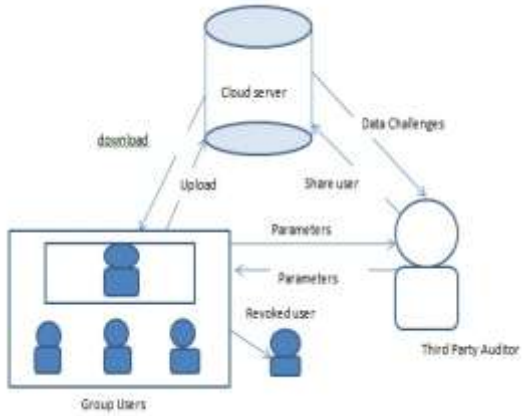

Fig.1.Proposed System

In proposed system, we found out the solution for revocation by providing 'Get Key' option on e-mail, by using SHA-1 algorithm.

In above figure, there is user member, one data owner, admin and third party auditor is present. Data owner is responsible for creating various group and function of data owner is to upload and download the data. At the time of uploading data owner generates one private key. TPA provides function like data challenges and securely sharing of data between use member. Revocation having two ways, first self revocation and second is through admin. If any person revoked from group and he/she wants to access his own file present on cloud server then he/she doesn't access files directly. For accessing files he/she have to take permission of TPA. If TPA gives permission to access files at that time TPA generate one key named as 'GET KEY'. By using that GET KEY user can access his/her own files.

For generation of GET KEY, we are using SHA-1 algorithm. GET KEY is a combination of user-id and password. Also exploration on secure and efficient data shared integrate audit for multi-user operation for cipher text database. By incorporating primitives commitment winner asymmetric group key agreement and group signature, we propose an efficient data audit system while providing at the same time a new features, such as traceability and count ability. We provide the security and analysis of the effectiveness of our system, and the analysis results show that our scheme is secure and efficient.

III. LITERATURE SURVEY

The coming of the distributed computing makes stockpiling outsourcing turn into a rising pattern, which advances the protected remote information inspecting a hotly debated issue that showed up in the examination writing. As of late some exploration consider the issue of secure and effective open information up rightness examining for shared element information. Security against the collusion attack from the cloud storage server and revoked group users. More time cost and length of key is greater[1]. Bunch marks are an exceptionally valuable primitive in cryptography, permitting an individual from a gathering to sign messages secretly in the interest of the gathering. Such marks must be mysterious and unlikable, however bunch power must have the capacity to open them if there should arise an occurrence of debate. The security of our component is formally demonstrated, and also the hidden gathering mark plan. To delete members from a group without compromising their past signatures or changing the group public key. Obtaining members revocation with constant size signatures remains an open problem[2].

The I/O information requests of these applications get higher as they get bigger. With a specific end goal to enhance execution of these applications can utilize parallel document frameworks. PVFS2 is a free parallel document framework created by a multi-foundation group of parallel I/O, systems administration and capacity specialists. The exploratory results demonstrate the predominance that exists on a neighborhood document framework contrasted with a parallel record framework where information is gotten to remotely. More cost for data backup and data stores [3]. With cloud information administrations, it is typical for information to be put away in the cloud, as well as shared over various clients. A few instruments have been intended to permit both information proprietors and open verifiers to proficiently review cloud information honesty without recovering the whole information from the cloud server. In any case, open reviewing on the respectability of imparted information to these current systems will unavoidably uncover private data personality protection to open verifiers. It support batch auditing. Designing an efficient public auditing mechanism with the capabilities of preserving identity privacy and supporting traceability is still problem [4].

IV. FUTURE WORK

To improve performance and fault tolerance. Length of key is smaller and less time cost. There are two

© 2016, IERJ All Rights Reserved

interesting problems we will continue to look to our future work. One of them is traceability, which means the ability to group manager(e.g. the original user) to reveal the identity signer on the basis of verification of the metadata in some special situations.

V. CONCLUSIONS

In this paper, we propose a system which provides efficient group user revocation. In group user revocation we can provide one GET KEY by using SHA-1 algorithm. By using GET KEY revoked person can access their files from cloud server.

Also data owner is responsible for generating one private key at the time of uploading the data. To solve the problem of verifiable outsourcing storage. We propose a system to achieve safe and effective data integrity auditing for share dynamic data with multi-user modification and group sig-natures with user revocation are adopt to achieve the data integrity auditing of remote data. We provide an analysis of the security of our system, and it shows that our scheme provide data confidentiality for users of the group, and it is also secure against the collusion attack from the cloud storage server and revoked group users.

REFERENCES

[1] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", .IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015.

[2] Emmanuel Bresson and Jacques Stern "Efficient Revocation in Group Signatures" Springer-Verlag Berlin Heidelberg 2001

[3] Hugo E. Camacho, J. Alfredo Brambila, Alfredo Peña, José M. Vargas "A Cloud Environment for Backup and Data Storage " 2014 INTERNATIONAL CONFERENCE ON (CONIELECOMP)

[4] Boyang Wang, Baochun Li,Hui Li, "Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014

© 2016, IERJ All Rights Reserved