Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

Possession of Dynamic Group-Oriented Provable Data in the Cloud

Mrs Anuradha Anumolu [1] , Miss. P. Aswini [2]

#1 Associate Professor and Head in the department of AI & IT at DVR & Dr HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District.

#2 MCA student in the Department of computer applications at DVR & DR. HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR District.

ABSTRACT_ As a significant security property of distributed storage, information respectability has not been adequately concentrated under the multi essayist model, where a gathering of clients work on shared documents cooperatively and any gathering part can refresh the information by change, inclusion, and erasure tasks. Existing works under such multi-author model would bring enormous capacity cost to the outsider verifiers. Moreover, as far as we could possibly know, none of the current works for shared records upholds completely unique tasks, which infers that clients can't openly play out the update activities.

The first public auditing scheme for shared data that achieves constant storage costs for verifiers and supports fully dynamic operations is presented in this paper. Our plan, named Implores, is helped by another worldview for distant information honesty checking. We proposed a novel cryptographic primitive known as permission-based signature and an authenticated structure called blockless Merkle tree to put the new paradigm into practice. Extensive testing shows that PRAYS is just as effective as the other, less useful options. PRAYS is, in our opinion, a significant step toward the creation of practical multiwriter cloud storage systems**..**

1.INTRODUCTION

CLOUD storage is an appealing paradigm for both individuals and businesses because it provides on-demand, ubiquitous access to a pool of configurable remote storage resources. Alongside this comfort, information uprightness turns into a main pressing issue about capacity re-appropriating, particularly taking into account stage disappointments and human mistakes [1], [2], [3]. To ensure information trustworthiness in distributed storage administrations, numerous applicable cryptographic natives have been proposed [4], [5], [6], [7], [8]. By validating and assigning a cryptographic tag to each data block in a file, these primitives typically make it possible for a verifier—the owner of the data or a special third party—to examine the integrity of remote data without downloading the entire file, thereby lowering the cost of communication. These primitives, on the other hand, are restricted to the single-writer model, in which only the owner of the data can update it in the cloud. However, in today's cloud platforms, the multi-writer model, in which a group of users can update shared files for collaboration, is becoming increasingly popular as online collaboration expands. In the case of dynamically shared data, maintaining data integrity in multi-writer cloud storage becomes an urgent challenge. The paradigm for the single-writer model, in which each data block is signed with a user's private key, is simply applied by the majority of current solutions that use the multi-writer model. All data blocks signed by a revoked user must be resigned by another, unrevoked user or the cloud server [9, 10], [11]. Since the quantity of information blocks is tremendous in the cloud (e.g., 1 TB information can have 2:68 108 information blocks with each block of size 4 kB), these sorts of techniques are wasteful practically speaking..

2.LITERATURE SURVEY

1. “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,”

AUTHORS: B. Wang, B. Li, and H. Li,

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

2. “Security Challenges for the Public Cloud,”

AUTHORS: K. Ren, C. Wang, and Q. Wang,

In this talk, I will first discuss a number of pressing security challenges in Cloud Computing, including data service outsourcing security and secure computation outsourcing. Then, I will focus on data storage security in Cloud Computing. As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging. In this talk, I will present our recent research efforts towards storage outsourcing security in cloud computing and describe both our technical approaches and security & performance evaluations.

3. "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,"

AUTHORS: C. Wang, Q. Wang, K. Ren, and W. Lou

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed.

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

3.PROPOSED SYSTEM

Following in the footsteps of provable data possession [4, 15], we present a dynamic group-oriented provable data possession scheme known as PRAYS that incorporates all of the aforementioned characteristics. PRAYS benefits from a new paradigm in comparison to other solutions, such as generating the tags and then building the structure: building the construction and afterward creating the tag. The following is a summary of our principal contributions.

1) A customized, authenticated structure known as a blockless Merkle tree is displayed by the system. The proposed structure outperforms the conventional Merkle tree by enabling blockless verification—that is, checking the integrity of remote data without downloading the challenged data blocks—through a complex procedure for each data block.

2) A brand-new cryptographic primitive known as a permission-based signature is proposed by the system. The first cryptographic primitive that combines offline traceability with anonymity is the permission-based signature. Additionally, this primitive could be utilized on its own in additional privacy-preserving applications.

3) The permission-based signature and the blockless Merkle tree serve as the foundation for the system's PRAYS design. Apparently, Supplicates is the main provable information ownership plot under the multi-essayist model that upholds completely unique tasks as well as consistent examining metadata.

4) A comprehensive security analysis and evaluation of the proposed scheme are carried out by the system. That's what the outcomes exhibit, contrasted and existing solutions,PRAYS can carry out more extravagant roles (e.g., completely powerful tasks) while keeping up with sensible calculation and correspondence cost..

3.1 IMPLEMENTATION

1. Group Manager Module :

Group manager takes charge of followings:

- System parameters generation
- User registration
- User revocation
- Revealing the real identity of a dispute data owner.

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

2. Group Member Module :

Group members are a set of registered users that will

- Store their private data into the cloud server and
- Share them with others in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it.

File Security Module :

- Encrypting the data file.
- File stored in the cloud can be deleted by either the group manager or the data owner.

(i.e., the member who uploaded the file into the server).

Group Signature Module :

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature’s originator when a dispute occurs, which is denoted as traceability.

User Revocation Module :

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

3. Member Registration Module

In this module, registration can be done by the members who wants to join in the particular group by giving their details like,

- User name
- Password
- Respective Group
- Email
- Mobile number
- Place

These details are mandatory and enter the details with required specifications. .

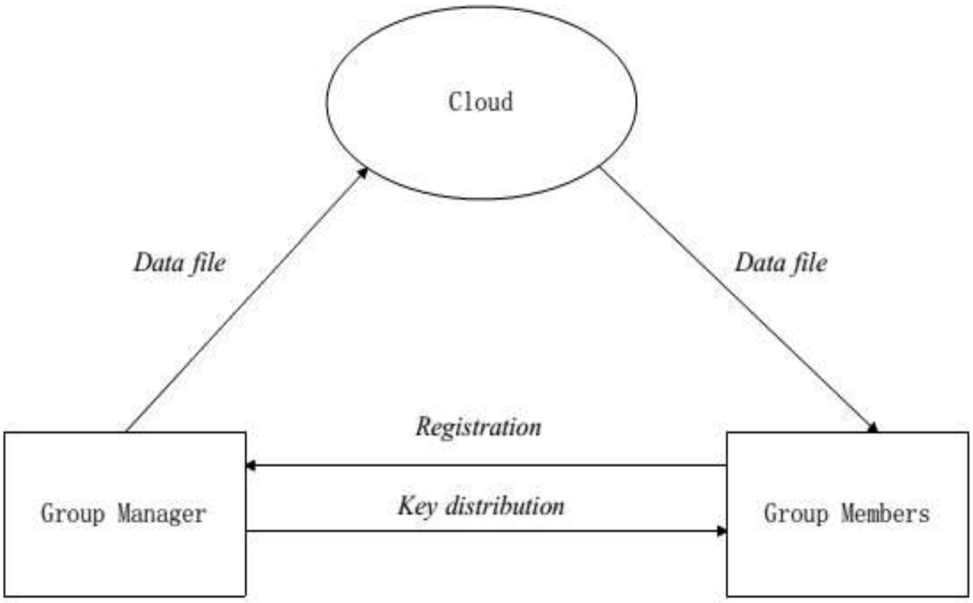
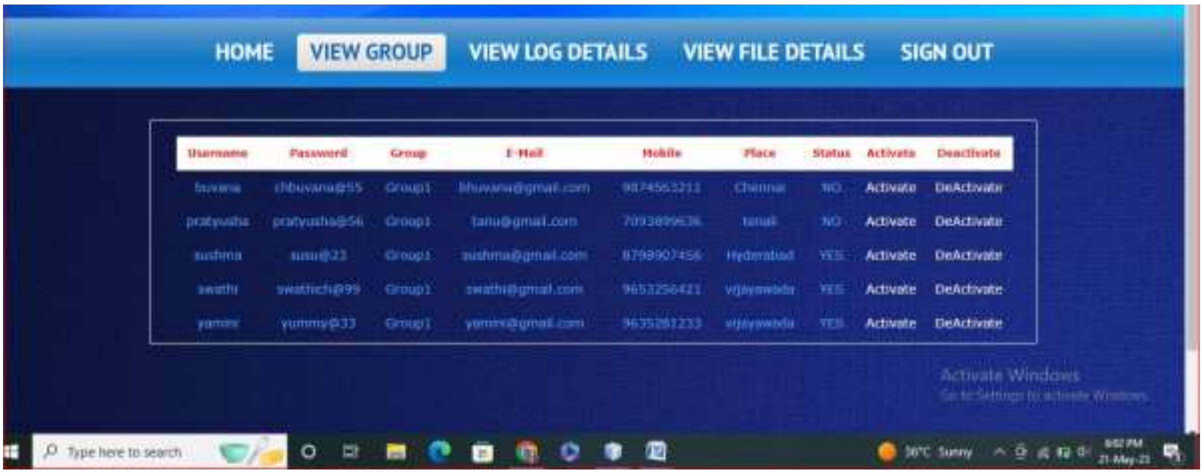


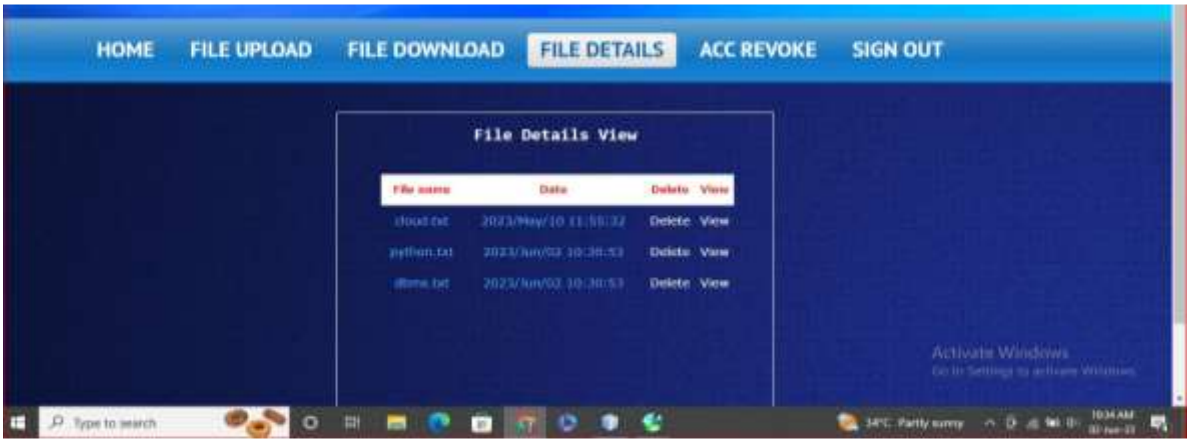
Fig 1:Architecture

4.RESULTS AND DISCUSSION



Username	Password	Group	E-Mail	Mobile	Place	Status	Activate	Deactivate
buvana	chbuvana@55	Group1	bhuvana@gmail.com	9874563211	Chennai	NO	Activate	DeActivate
pratyusha	pratyusha@56	Group1	tanu@gmail.com	7093899636	tenali	NO	Activate	DeActivate
sushma	susu@23	Group1	sushma@gmail.com	8798907456	Hyderabad	YES	Activate	DeActivate
swathi	swathich@99	Group1	swathi@gmail.com	9653256421	vijayawada	YES	Activate	DeActivate
yamini	yummy@33	Group1	yamini@gmail.com	9635281233	vijayawada	YES	Activate	DeActivate

Fig 2:After view a respective group, the group contains the group member username, passwords which group they are belonging to and their e-mail addresses mobile number, place and as well active statuses.



File Details View

File name	Date	Delete	View
cloud.txt	2023/May/10 11:50:32	Delete	View
python.txt	2023/Jun/02 10:30:53	Delete	View
dbms.txt	2023/Jun/02 10:30:53	Delete	View

Fig 3: After file download and then we can see the file details file uploaded date and file delete and view files option. When we want to delete or to view the files it asks the signature key of the file as shown below.

5.CONCLUSION

PRAYS, a privacy-preserving auditing method for dynamically shared data, was proposed in this paper. To our knowledge, it is the first group-oriented provable data possession scheme that supports both continuous metadata auditing and fully dynamic operations. A brand-new two-step paradigm developed for group-oriented integrity checking contributes to the success of the proposed plan. To understand this worldview, we introduced a blockless Merkle tree for the initial step, and introduced a consent based signature for the subsequent step. PRAYS provides the multi-writer storage services' essential features, including fully dynamic operations, constant auditing of metadata, secure user revocation, anonymity, and traceability, with these two tools. In our future work, we will expand Asks from the accompanying viewpoints. 1) As stated in Section 5.1, bringing the user-side storage cost down to O1. 2) Improving the calculation cost in the renouncement stage. In contrast to the conventional paradigm, which has a lower bound on the cost of computation in the revocation phase..

REFERENCES

1. M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz,A.Konwinski, G. Lee, D.Patterson, A.Rabkin, I.Stoica, andM.Zaharia. “A View of Cloud Computing,”Comm. ACM, vol. 53,no.4, pp.50-58, Apr.2010.

2. S.Kamara and K.Lauter,“Cryptographic Cloud Storage,” Proc.Int’l Conf. Financial Cryptography and Data Security (FC), pp.136-149, Jan. 2010.

3. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K.Fu,“Plutus:

Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

4. E.Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003.

5. G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.

6. Shucheng Yu, Cong Wang, KuiRen, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

7. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

8. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.