International Journal of Modern Developments in Engineering and Science
Volume 1, Issue 6, June 2022
https://www.ijmdes.com | ISSN (Online): 2583-3138

Public Integrity Checking of Group Shared Data on Cloud Storage with Less Certified Using Ranking Search

J. Bharathi[1*], S. Pooja[2], E. Gopika[3], S. J. Vivekanandan[4], G. Abirami[5], R. Reni Hena Helan[6]

[1,2,3]*UG Scholar, Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India*

[4,5,6]*Assistant Professor, Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India*

***Abstract*: Now-a-days, the cloud server is deceitful. Remote Data Possession Checking Protocols have been put forward as a result. The RDPC protocol is built on a Public Key Infrastructure (PKI), which has reliability deficiency. To address this complication, RDPC's foundation is Identity Based Cryptography (IBC). Because of the precariousness, IBC has a key escrow disadvantage. To describe these issues, we introduce a novel RDPC protocol that checks the consistency of data communicated among a group using the certificate less signature mechanism. The user's private key under our suggestion is made up of two parts: a partial key generated by the group manager and a secret value picked out by the user. To ensure that the correct public keys are used during data consistency testing, each user's public key is associated with his or her unique identity, such as a name or phone number. As an out-turn, the certificate is no longer in need of, and the issue of key escrow is also resolved. What's More, our system clears the way for effective user withdrawal from the group. Most prevailed ranked keyword search schemes generally focus on improving search efficiency or service, but they are in need of efficient access control and formal security analysis at the same time, hence we handed out Multi-Keyword Ranked Search. To solve these issues, we offer a fast and private Multi-Keyword Ranked Search method with fine-grained access control in this study (MRSF). For security reasons, all files are stored in a group. Also, a Caution Indication System is included aiming at the security of the user. For example, whenever the end user logins, an indication message will be sent to the user's mail. So, if there is any questionable action taking place they can be identified and the required security measures can be taken.**

***Keywords*: Group sharing, cloud storage, ranking search.**

1. Introduction

Cloud storage service offers users an efficient way to share data and work as a team. Once someone on the team uploads a file to the server, other members are able to access and modify the file. The most pressing issue with such applications is whether the Cloud Service Provider (CSP) can guarantee data integrity. In fact, the CSP is not fully trustworthy and the failure of software or hardware is inevitable, so serious accidents of data corruption may occur at any time. In this project, we mainly focus on integrity checking for data shared within a group. Motivated by such a requirement, we propose a new RDPC scheme for data shared in a group. Different from previous work, our scheme is based on the certificate less signature technique to avoid the problems of certificate management and key escrow. Keyword Search with a ranking in comparison to the original SSE, the new system also includes the encrypted relevance scores in the searchable index. Also we included a caution indication system for the user i.e., when the user logins, a notification will be received via mail, so if there is any unauthorized action taking place they can be identified.

2. System Analysis

A. *Existing System*

This paper focuses on the integrity verification of data shared in groups. However, most existing RDPC schemes are based on PKI. Despite the fact that PKI is widely used and plays a vital role in public key cryptography, it nevertheless poses significant security risks. For example, the security of PKI is based on the trustworthiness of Certificate Authority (CA), but it is not an easy task to ensure the trustworthiness of CA. Besides, the management of certificates such as distribution, storage, revocation and verification is also a big burden. To avoid these problems, some ID-based RDPC schemes are proposed. Unfortunately, key escrow issues plague ID-based RDPC implementations. The Private Key Generator (PKG) creates all of the users' private keys. If PKG is untrusted, the scheme is not secure either. As a result, ID-based RDPC schemes may be limited to tiny, constrained environments. Compared with PKI and IBC, certificate less cryptography solves the problems of certificate management and key escrow at the same time. A certificate-less RDPC scheme is a good method for cloud data integrity checking.

Disadvantages:

- ID-based RDPC schemes are proposed. Unfortunately, key escrow issues plague ID-based RDPC implementations. To address the problem of key escrow and certificate management, two PDP schemes based on certificateless and certificate-based cryptography were proposed respectively.
- The problem of multi-user modification for blocks.
- Ranking scheme is not included for improvement and

*Corresponding author: bharathijyothiswaran@gmail.com accuracy of the user search scheme.

B. Proposed System

The user's private key in our system is made up of two parts: a partial key generated by the group manager and a secret value chosen by the users. The certificate is no longer required, and the issue of key escrow is thus resolved. Meanwhile, without downloading the entire data, a public verifier can still audit the data integrity. Furthermore, our system facilitates effective user withdrawal from the group. Our scheme's security is limited to its assumptions, suggesting a symmetric encryption-based scalable and efficient PDP method that included block adding, updating, and deletion. Wang et al suggested a system for verifying the integrity of shared data in a group in 2012. To create each, they used the group signature approach. In this paper, we propose an efficient and privacy-preserving Multi-Keyword Ranked Search scheme with Fine-grained access control (MRSF). In addition, linguistic terms are taken into account to weigh the most important non-functional preferences. Also, we included a caution indication system for the user that is, when the user logins, a notification will be received via mail, so if there is any unauthorized action taking place they can be identified and the required security measures can be taken.

Advantages:

- Proposed a protocol for checking the integrity of data shared in a group. They utilized the technique of group signature that is used to generate each authentication tag.
- Proposed another PDP scheme for group data which supported the group user's joining and leaving.
- The inclusion of the caution indication system for the user enhances the security.
- By delivering matched files in a ranked order based on specific relevance criteria, ranked search dramatically improves system usability.
- Extensive experimental findings show that the proposed solution is effective and efficient.

3. System Architecture

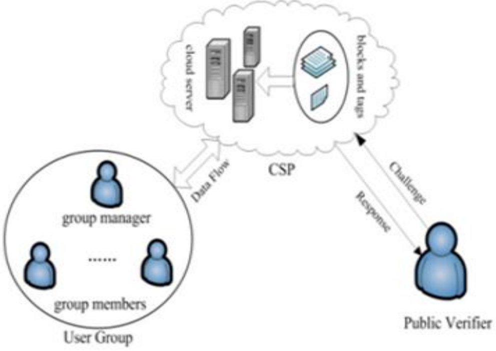


Fig. 1. System model

A. Group Manager

User group, Cloud Service Provider (CSP) and public verifier are the main modules included in this system. The user group consists of a number of users, who can upload, access and update the data shared within the group, as well as carry out the protocol uprightness. Without loss of generality, the original creator of the group plays the role of group manager, who sets up the system and produces partial keys for general group users. CSP owns powerful storage and computational abilities to supply cloud users with data storage service. In our project, the shared data is divided into multiple blocks, each of which has an authentication tag attached to it. Thus, the CSP stores all the blocks and the corresponding tags for cloud users.

B. Group User

When data is shared by several users, new difficulties arise that are not properly addressed by the RDPC schemes for personal data. For example, block tags may be generated by any group user, and different group users will output different tags even if the block is the same one. Furthermore, when a group user edits a block, the tag should be regenerated. All of the authentication tags created individually must be combined for checking the data integrity. Our scheme moves most computation operations to CSP, which greatly reduces the burden of group users and efficiently updates the tags generated by the revoked user. In our scheme, the group creator generates the partial key for each group user on behalf of the key generation centre. Each user selects a secret value privately. Each group user's private key is made up of two parts: a partial key and a secret value. All the data blocks are signed by the group user.

C. Public Verification

Public verification is an engaging attribute of the data integrity checking work. That is, the integrity of shared data can be verified by not only the data owner but also everyone who is interested in the cloud data. It is very important for the RDPC protocol to support public verification under the current open environment. The data verifier is a person who inspects the integrity of the data on CSP. Due to the feature of public verification, any file could be verified in our scheme.

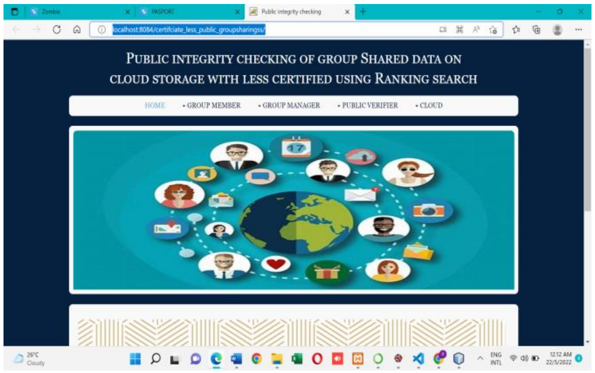
D. Caution Indication

The Caution Indication System enhances the security for the user and the system. This scheme detects the login activity of the user and sends a caution mail stating that 'the particular user id has logged in', to the login id each time the user logins to the system, so when and if there is any unauthorized action taking place, they can be identified and the required security measures can be taken.

E. Ranked Search

Ranked search improves system usability by returning matching files in a ranked order based on particular relevance criteria (for example, keyword frequency), bringing us one step closer to practicality. Cloud Computing deployment of privacy-preserving data hosting services. The following is how we look at the problem of secure ranked keyword search: The search result should be returned based on a set of ranking relevance criteria (for example, keyword frequency-based scores, as will be the case in the future be introduced shortly) and to improve file retrieval accuracy for people who have no prior experience with the file collection.

4. Results

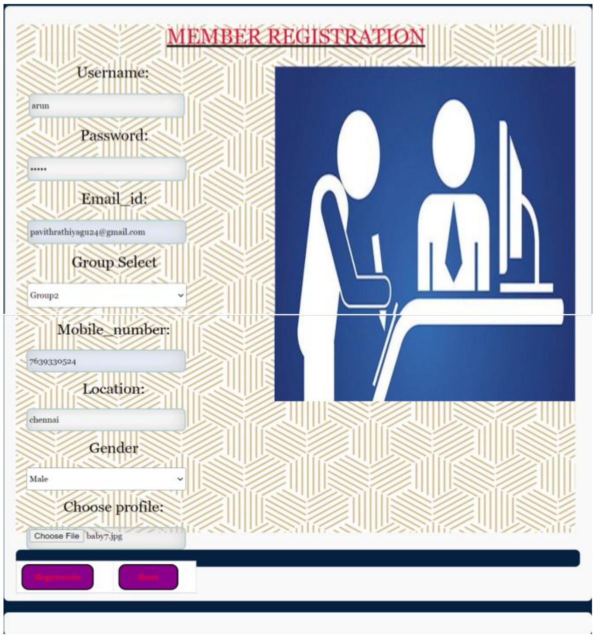

Zombiz
PASPORT
Public integrity checking
localhost:8084/certifciate_less_public_groupsharingss/

PUBLIC INTEGRITY CHECKING OF GROUP SHARED DATA ON CLOUD STORAGE WITH LESS CERTIFIED USING RANKING SEARCH

HOME
• GROUP MEMBER
• GROUP MANAGER
• PUBLIC VERIFIER
• CLOUD

Fig. 2. Home page

Fig. 2. Home page - utilized for group member registration and login. Also, for group manager login, public verifier login and cloud login.


MEMBER REGISTRATION

Username: arun

Password: •••••

Email_id: pavithrathiyagu24@gmail.com

Group Select: Group2

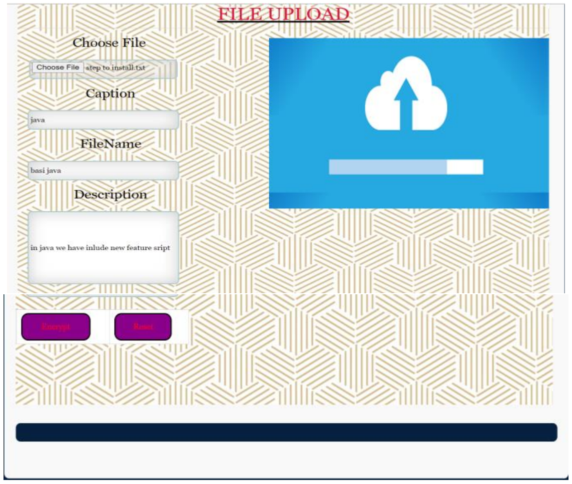
Mobile_number: 7639330524

Location: chennai

Gender: Male

Choose profile: Choose File baby7.jpg

Fig. 3. Member registration


FILE UPLOAD

Choose File: Choose File step to install.txt

Caption: java

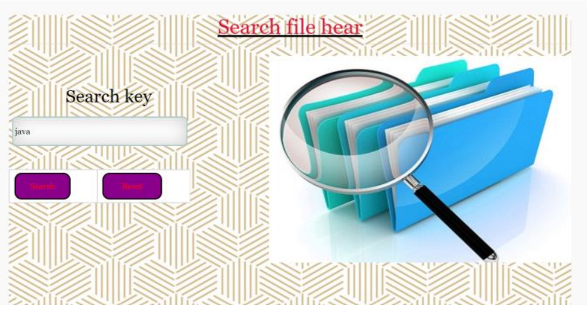
FileName: basi java

Description: in java we have inlude new feature sript

Fig. 4. File upload

Fig. 3. Member Registration - Group member or user registration details that are required to register into the group. The above registration details are used in the system for checking the identity of users and for security purposes.

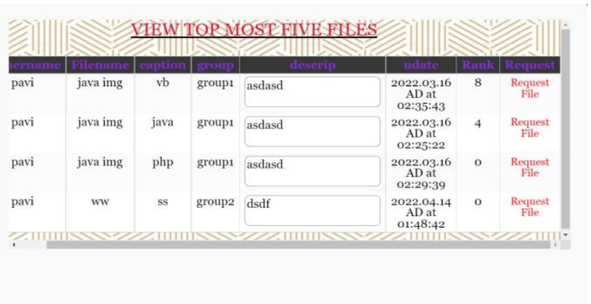
Fig. 4. File Upload - The required file along with its name, appropriate caption and description is uploaded in the system in an encrypted format by using Blowfish algorithm.


Search file hear

Search key: java

Fig. 5. Ranking search

Fig. 5. Ranking Search - The search key engine is used to search for the desired file using a keyword. The results are shown in a ranked order based on the keyword relevance frequency.


VIEW TOP MOST FIVE FILES

ername	Filename	caption	group	descrip	udate	Rank	Request
pavi	java img	vb	group1	asdasd	2022.03.16 AD at 02:35:43	8	Request File
pavi	java img	java	group1	asdasd	2022.03.16 AD at 02:25:22	4	Request File
pavi	java img	php	group1	asdasd	2022.03.16 AD at 02:29:39	0	Request File
pavi	ww	ss	group2	dsdf	2022.04.14 AD at 01:48:42	0	Request File

Fig. 6. Top most ranking files

Fig. 6. Top Most Ranking Files - The top five most viewed files in the system are shown in a ranked order along with the file name, owner name, caption, the group they belong to, description and the updated time. If the user's desired file is present in the ranked file, he or she can directly request the file to view it.

5. Conclusion

Our scheme focuses on solving integrity checking for the group data which is shared among many members of a team. We focused on shared data auditing in the cloud and proposed a privacy preserving public auditing system for dynamic shared data storage in cloud computing by utilizing certificate-less signatures. The relevance scores of matching files to a particular search request are calculated using a ranking algorithm in information retrieval. The most widely used statistical measurement for evaluating relevance score in the information retrieval community is used. In traditional searchable encryption methods, this eliminates the problem of semantic ignorance or confusing semantics. We also included a caution indication system which enhanced the security of our scheme. This caution indication system sends notification through mail to the user every time the user logins. The results reveal that the scheme over encrypted cloud data is an efficient and privacy-protected semantic-based multi-keyword ranked search method.

References

[1] Dropbox for Business. [Online].
Available: https://www.dropbox.com/business

[2] TortoiseSVN. [Online Sep. 1, 16, 2016.

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering,” Future Generation Computer Systems, vol. 25, no. 6, pp. 599 – 616, 2009.

[4] Y. Deswarte, J. J. Quisquater, and A. Saïdane, “Remote integrity checking,” in Proc. 6th Working Conf. Integr. Internal Control (ICIS 03), pp. 1-11.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” in Proc. 14th ACM Conf. on Comput. and Comm 598-609.

[6] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” in Pro and Privacy in Commun. Netw. (SecureComm’08), pp. 1-10.

[7] F. Sebé, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte and J. -J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," in IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[8] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, “Dynamic Provable Data Possession,’’ in Proc. 16th ACM C Commun. Security (CCS’09), pp. 213-222.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Computing,” IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847-859, May, 2011.

[10] C. Wang, S. S. M. Chow, Q. Wang, preserving public auditing for secure cloud storage,” IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.