International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1262-1266 www.ijaem.net ISSN: 2395-5252

Certificateless Public Integrity Checking Of Group Shared Data on Cloud Storage

Vanika E[1], Diana G.P[2]

1.IIMCA, Sri Muthukumaran Institute of Technology, Mangadu
2.Assistant Professor,MCA, Sri Muthukumaran Institute of Technology, Mangadu

Submitted: 10-08-2022 Revised: 22-08-2022 Accepted: 24-08-2022

ABSTRACT

Cloud storage service supplies people with an efficient method to share data within a group. The cloud server is not trustworthy, so lots of remote data possession checking (RDPC) protocols are proposed and thought to be an effective way to ensure the data integrity. However, most of RDPC protocols are based on the mechanism of traditional public key infrastructure (PKI), which has obvious security flaw and bears big burden of certificate management. To avoid this shortcoming, identity-based cryptography (IBC) is often chosen to be the basis of RDPC. Unfortunately, IBC has an inherent drawback of key escrow. To solve these problems, we utilize the technique of certificateless signature to present a new RDPC protocol for checking the integrity of data shared among a group. In our scheme, user's private key includes two parts: a partial key generated by the group manager and a secret value chosen by herself/himself. To ensure the right public keys are chosen during the data integrity checking, the public key of each user is associated with her unique identity, for example the name or telephone number. Thus, the certificate is not needed and the problem of key escrow is eliminated too. In addition, our scheme also supports efficient user revocation from the group. The security of our scheme is reduced to the Experiment results exhibit that the new protocol is very efficient and feasible. We proposed Multi-keyword Ranked Search, most of the existing ranked keyword search schemes mainly focus on enriching search efficiency or functionality, but lack of providing efficient access control and formal security analysis simultaneously. To address these limitations, in this paper we propose an efficient and privacy-preserving Multi-**keyword**: Ranked Search scheme with Fine-grained access control (MRSF).All Files storage into group for security purpose.

I. INTRODUCTION

Cloud storage service offers user an efficient way to share data and work as a team. Once someone of the team uploads a file to the server, other members are able to access and modify the file by Internet. The most important problem of such applications is whether the cloud server provider (CSP) can ensure the data to be kept intact [3]. In fact, the CSP is not fully trustworthy and the failure of software or hardware is inevitable in some way, so serious accidents of the data corruption may occur at any time. In this paper, we mainly focus on the integrity checking for data shared within a group Motivated by such requirement, we propose a new RDPC scheme for data shared in a group. Different from previous work, our scheme is based on the certifcateless signature technique to avoid the problems of certificate management and key escrow. Ranked Keyword Search Compared to the original SSE, the new scheme embeds the encrypted relevance scores in the searchable index in addition to file.

II. RELATED WORKS

"Scalable and Efficient Provable Data Possession"

Storage outsourcing is a rising trend which prompts a number of interesting security issues, many of which have been extensively investigated in the past. However, Provable Data Possession (PDP) is a topic that has only recently appeared in the research literature. The main issue is how to frequently, efficiently and securely verify that a storage server is faithfully storing its client's (potentially very large) outsourced data. The storage server is assumed to be untrusted in terms of both security and reliability. (In other words, it might maliciously or accidentally erase hosted data; it might also relegate it to slow or off-line storage.) The problem is exacerbated by the client being a small computing device with limited resources. Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form. In this paper, we construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption. Also, in contrast with its predecessors, our PDP technique allows outsourcing of dynamic data, i.e, it efficiently supports operations, such as block modification, deletion and append.

Secure Ranked Keyword Search over Encrypted Cloud Data

Query processing that preserves both the data privacy of the owner and the query privacy of the client is a new research problem. It shows increasing importance as cloud computing drives more businesses to outsource their data and querying services. However, most existing studies, including those on data outsourcing, address the data privacy and query privacy separately and cannot be applied to this problem. In this paper, we propose a holistic and efficient solution that comprises a secure traversal framework and an encryption scheme based on privacy homomorphism. The framework is scalable to large datasets by leveraging an index-based approach. Based on this framework, we devise secure protocols for processing typical queries such as k-nearest-neighbor queries (kNN) on R-tree index. Moreover, several optimization techniques are presented to improve the efficiency of the query processing protocols. Our solution is verified by both theoretical analysis and performance study.

III. EXISTING SYSTEM

The integrity verification of data shared in group. However, most of existing RDPC schemes are based on PKI. Although PKI is widely used and occupies an important position in public key cryptography, there are still some security threats in it. For example, the security of PKI is based on the trustworthy of certificate authority (CA), but it is not an easy work to ensure the trustworthiness of CA. Besides, the management of certificate such as distribution, storage, revocation and verification is also a big burden. To avoid these problems, some ID-based RDPC schemes are proposed. Unfortunately, ID-based RDPC schemes suffer from key escrow problem. Namely, the private key generator (PKG) generates all the private keys for the users. If PKG is untrusted, the scheme is not secure either. Thus, ID-based RDPC schemes may be restricted to small, closed settings. Compared with PKI and IBC, certificateless cryptography solves the problems of certificate management and key escrow at the same time. To construct certificateless RDPC scheme is a good method for cloud data integrity checking. Ranking is include in the included improve our more efficiency on ranking system.

DISADVANTAGES

- To avoid these problems, some ID-based RDPC schemes are proposed. Unfortunately, ID-based RDPC schemes suffer from key escrow problem.
- the problem of user revocation from the team should be considered
- To address the problem of key escrow and certificate management, two PDP scheme based on certificateless [20] and certificate-based cryptography were proposed respectively.
- The problem of multi-user modification for blocks.
- Ranking scheme is not included improve more accuracy in user search ranking scheme.

IV. PROPOSED SYSTEM

In our scheme, user's private key includes two parts: a partial key generated by the group manager and a secret value chosen by herself/himself. The certificate is not needed and the problem of key escrow is eliminated too. Meanwhile, the data integrity can still be audited by public verifier without downloading the whole data. In addition, our scheme also supports efficient user revocation from the group. The security of our scheme is reduced to the assumptions. Proposed another scalable and efficient PDP scheme by symmetric encryption, which supported block appending, updating and deleting. The integrity verification for personal data. In 2012, Wang et al. Proposed a protocol for checking the integrity of data shared in a group. They utilized the technique of group signature to generate each authentication tag so as to preserve the tag generator's privacy. The proposed ranking system is based on measuring the shortest distance to the minimum and maximum of the selected consumer’s non-functional preferences. In addition, linguistic terms are taken into account to weight the most important non-functional preferences. The proposed system is evaluated against traditional SaaS ranking systems using data collected.

ADVANTAGES

- Proposed a protocol for checking the integrity of data shared in a group. They utilized the technique of group signature to generate each authentication tag

- Proposed another PDP scheme for group data which supported the group user's joining and leaving
- Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria
- Extensive experimental results demonstrate the effectiveness and efficiency of the proposed solution
- The proposed scheme by analysing its fulfilment of the security.

V. ARCHITECTURE DIAGRAM

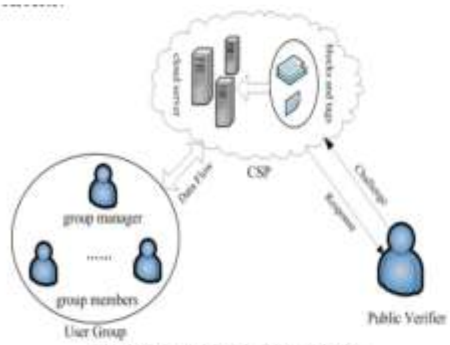


Fig. 1. System Model of Our Scheme

Fig – 1 Architecture Diagram

VI. MODULE DESCRIPTION

Group manager

User group, cloud service provider (CSP) and public verifier. The user group includes numbers of users, who can upload, access and update the data shared within the group, and honestly execute the protocol. Without loss of generality, the original creator of the group plays the role of group manager, who sets up the system and generates partial keys for general group users. CSP owns powerful storage and computational abilities to supply cloud users with data storage service. In our scheme, the shared data is divided into many blocks and each block is attached with an authentication tag. Thus, the CSP stores all the blocks and the corresponding tags for cloud user. The data verifier is a person who checks the integrity of the data on CSP. Due to the feature of public verification, anyone could be the verifier in our scheme

Group user

Data is shared among multiple users, some new challenges appear which are not well solved in the RDPC schemes for personal data. For example, block tags may be generated by any group user, and different group user will output different tags even if the block is the same one. Moreover, when a group user updates a block, it should regenerate the tag again. When auditing the data integrity, all the authentication tags generated individually need to be aggregated and the information of all the generators. Our scheme moves most computation operation to CSP, which greatly reduces the burden of group user and efficiently updates the tags generated by the revoked user. Our scheme, the group creator generates the partial key for each group user on behalf of key generation centre. Each user selects a secret value privately. The private key of each group user contains two parts: a partial key and a secret value. All the data blocks are signed by group user.

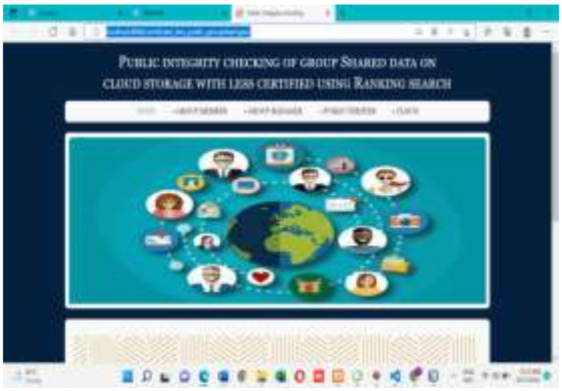
Public verification

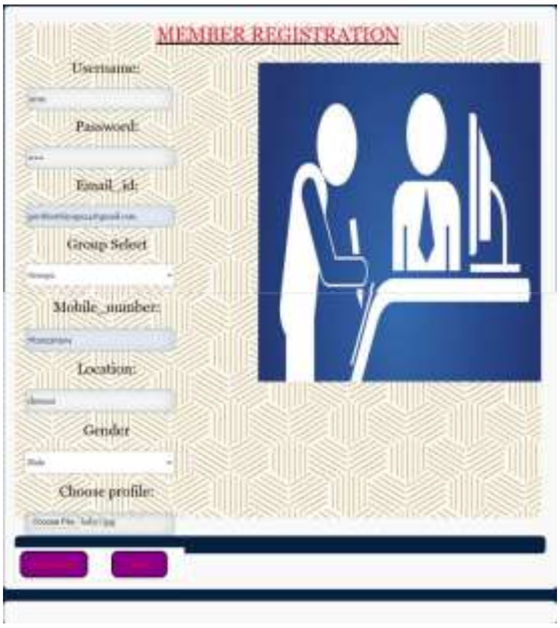
Public verification is an attractive feature of the data integrity checking work. That is, the integrity of shared data can be verified by not only the data owner but also everyone who is interested in the cloud data. It is very important for RDPC protocol to support public verification under current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

Ranked search

Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. our ranked searchable symmetric encryption scheme indeed enjoys “as-strong as-possible” security guarantee compared to previous SSE schemes. We consider the secure ranked keyword search problem as follows: the search result should be returned according to certain ranked relevance criteria (e.g., keyword frequency based scores, as will be introduced shortly), to improve file retrieval accuracy for users without prior knowledge on the file collection

VII. RESULTS


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


MEMBER REGISTRATION

Username:

Password:

Email_id:

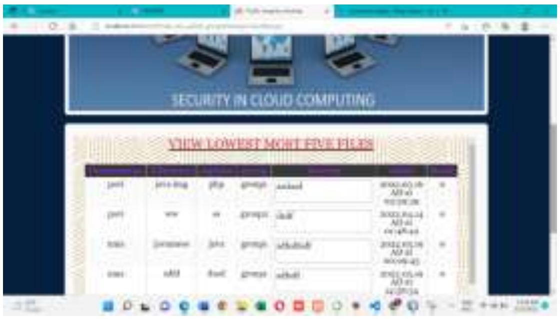
Group Select

Mobile_number:

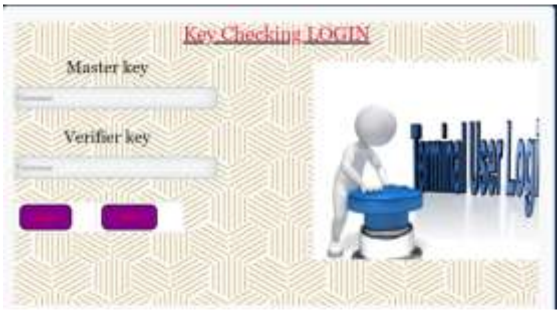
Location:

Gender

Choose profile:


SECURITY IN CLOUD COMPUTING

VIEW LOWEST MOST FIVE FILES


Key Checking LOGIN

Master key

Verifier key

VIII. CONCLUSION

Our scheme devotes to solve the integrity checking for the group data which is shared among many clients of a team. We focused on shared data auditing in cloud and proposed a privacy preserving public auditing system for dynamic shared data storage in cloud computing by utilizing certificate less signatures. In information retrieval, a ranking function is used to calculate relevance scores of matching files to a given search request. The most widely used statistical measurement for evaluating relevance score in the information retrieval community uses. This solves the problem of semantic ignorance or unclear semantics in traditional searchable encryption schemes. The realization of the tree-based index further improves the search time. The results show that the scheme is an efficient and privacy-protected semantic-based multi-keyword ranked search scheme over encrypted cloud data.

REFERENCES

[1]. Dropbox for Business. [Online]. Available: https://www.dropbox.com/ business, accessed Sep. 16, 2016.

[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 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 (IICIS'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. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastruc 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. [11] L. Chen, S. Zhou, X. Huang and L. X possession checking in cloud storage, ’’ Comput. Electr. Eng., vol. 39, no. 7, pp. 2413-2424, 2013.

[11]. Y. Yu, Y. Zhang, J. Ni, M.H. Au, L. Chen, and possession checking with enhanced security for cloud,’’ Future Gener. Comp. Syst., no. 52, pp. 77-85, 2015.

[12]. K. Yang and X. Jia, ‘‘An efficient and secure dynamic a for data storage in cloud computing,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717-1726, 2013.

[13]. H. Yan, J. Li, J. Han and Y. Zhang, ‘‘A Novel Efficient Re Possession Checking Protocol in Cloud Storage, ’’ IEEE Trans. Inf. Foren. and Sec., vol. 12, no. 1, pp. 78-88, 2017.

[14]. Y. Feng, Y. Mu, Checking Scheme with User Privacy,’’ in Proc 20th Australasian Conf. on Inf. Security and Privacy (ACISP’15), pp. 377-394