IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 10, October 2024

Impact Factor: 5.731

Enabling Identity-based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage.

Prof. Rakesh Tannu
Department of Information Technology
JCEI's Jaihind Polytechnic Kuran, India

Abstract: *With cloud storage services, users can remotely store their data to the cloud and realize the data sharing with others. Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud. In some common cloud storage systems such as the electronic health records system, the cloud file might contain some sensitive information. The sensitive information should not be exposed to others when the cloud file is shared. Encrypting the whole shared file can realize the sensitive information hiding, but will make this shared file unable to be used by others. How to realize data sharing with sensitive information hiding in remote data integrity auditing still has not been explored up to now. In order to address this problem, we propose a remote data integrity auditing scheme that realizes data sharing with sensitive information hiding in this paper. In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file and transforms these data blocks' signatures into valid ones for the sanitized file. These signatures are used to verify the integrity of the sanitized file in the phase of integrity auditing. As a result, our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed. Meanwhile, the proposed scheme is based on identity-based cryptography, which simplifies.*

Keywords: Cloud Storage, data sharing, sensitive information hiding

I. INTRODUCTION

A distributed computation model over a vast pool of shared-virtualized computing resources, such as storage, processing power, applications, and services, cloud computing has drawn a lot of interest from research communities in academia and industry. In a cloud computing environment, users can provide and release resources as they see fit. This new type of computing model is a fresh approach to offering computing services as essential public services like electricity and water. Many advantages come with cloud computing for users. However, a wide range of obstacles must be overcome before cloud computing may be widely used. Security concerns account for 87% of cloud users' worries, according to a recent Oracle survey that used data from the IDC Enterprise Panel1. One of the principal since customers no longer physically retain their data and lose control over it, their outsourced files' integrity is a security problem for cloud users. Furthermore, the cloud server cannot be completely trusted, and it is not required to notify instances of data loss. In fact, the cloud security alliance (CSA) presented an examination of cloud vulnerability occurrences to determine the dependability of cloud computing.

II. RELATED WORK

In order to verify the integrity of the data stored in the cloud, many remote data integrity auditing schemes have been proposed. To reduce the computation burden on the user side, a Third Party Auditor (TPA) is introduced to periodically verify the integrity of the cloud data on behalf of user. firstly proposed a notion of Provable Data Possession (PDP) to ensure the data possession on the untrusted cloud. In their proposed scheme, homomor- phic authenticators and random sampling strategies are used to achieve blockless verification and reduce I/O costs. defined a model named as Proof of

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 10, October 2024
Impact Factor: 5.731

Retrievability (PoR) and proposed a practical scheme. In this scheme, the data stored in the cloud can be retrieved and the integrity of these data can be ensured. Based on pseudorandom function and proposed a private remote data integrity auditing scheme and a public remote data integrity auditing scheme.

The distributed file system at the far site ensures availability by copying each file to numerous desktop computers. It's critical to reclaim used space when you can because this replication uses a lot of storage capacity. Over 500 desktop file systems were measured, and the results reveal that duplicate files take up about half of the total space used. We outline a method for recovering space from this unintentional duplication so that it can be used for carefully regulated file replication. Our mechanism uses SALAD, a self-arranging, lossy, associative database, to aggregate file content and location data in a decentralised, scalable, fault-tolerant manner, as well as convergent encryption, which allows duplicate files to merge into the space of a single file even if they are encrypted with different users' keys. Experiments with large-scale simulations reveal that theThe duplicate-file coalescing system is highly efficient, fault-tolerant, and scalable.

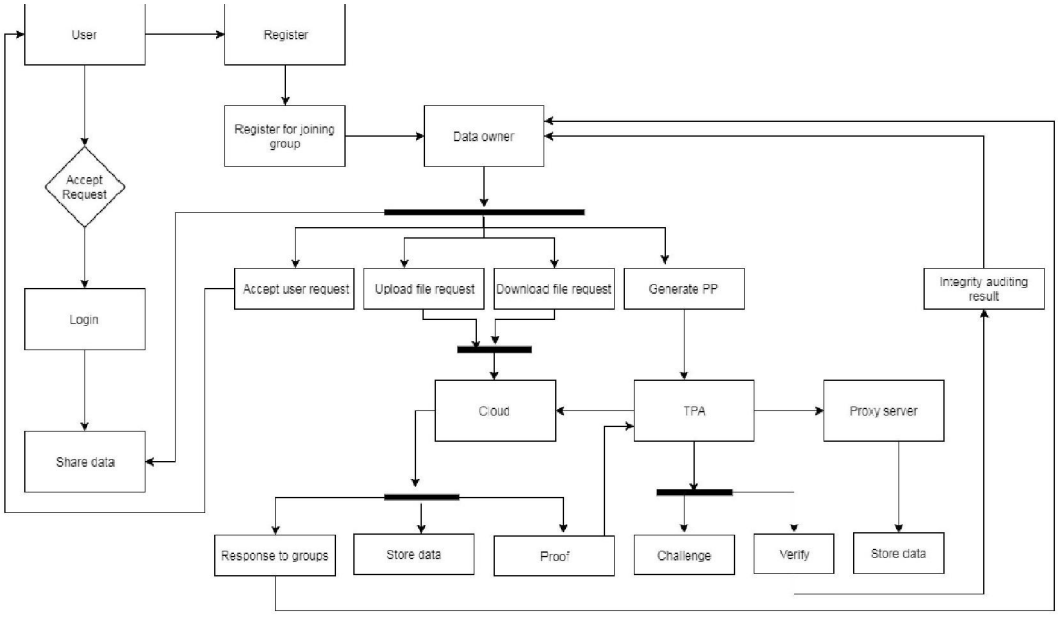
III. SYSTEM ARCHITECTURE

Overall system design consists of following modules:

1. User
2. Cloud Sever
3. Third Party Auditor

In identity-based remote data integrity checking protocols, we take into account three security aspects, namely completeness, security against a malicious server (soundness), and privacy against the TPA (absolute data privacy). According to Shacham and Waters' security theories [7], an identity-based RDIC scheme is said to be secure against a server if neither a polynomial-time algorithm nor a polynomial-time extractor exists that can successfully circumvent the challenges-response protocols and recover the file. Completeness states that the ProofCheck algorithm will accept the proof when communicating with a legitimate cloud server. According to soundness, a cheating prover who is able to persuade the TPA that it is saving the data file is truly doing so. Now that the security is formalized

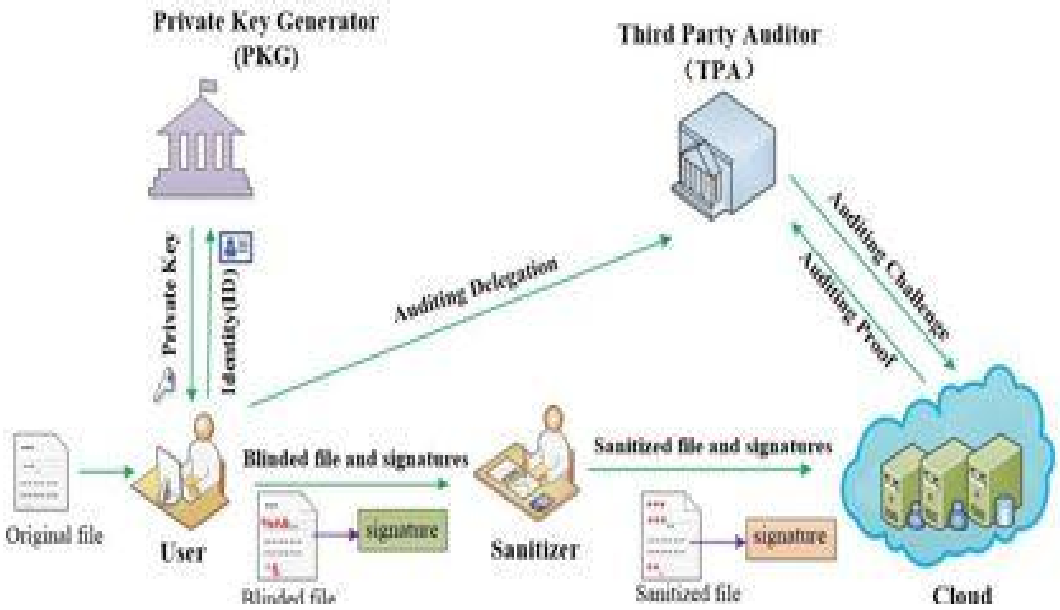
Model of soundness for identity-based remote data integrity checking is shown below, where a challenger who represents a data owner and an adversary who assumes the role of an untrusted server are both involved.



System Design

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 10, October 2024
Impact Factor: 5.731

In order to verify the integrity of the data stored in the cloud, many remote data integrity auditing schemes have been proposed. To reduce the computation burden on the user side, a Third Party Auditor (TPA) is introduced to periodically verify the integrity of the cloud data on behalf of user. firstly proposed a notion of Provable Data Possession (PDP) to ensure the data possession on the untrusted cloud. In their proposed scheme, homomor- phic authenticators and random sampling strategies are used to achieve blockless verification and reduce I/O costs. Juels and Kaliski [3] defined a model named as Proof of Retrievability (PoR) and proposed a practical scheme. In this scheme, the data stored in the cloud can be retrieved and the integrity of these data can be ensured. Based on pseudorandom function and proposed a private remote data integrity auditing scheme and a public remote data integrity auditing scheme.



System Architecture

In order to protect the data privacy, proposed a privacy-preserving remote data integrity auditing scheme with the employment of a random masking technique. utilized a different random masking technique to further construct a remote data integrity auditing scheme supporting data privacy protection. This scheme achieves better efficiency compared with the scheme To reduce the computation burden of signature generation on the user sid designed a remote data integrity auditing scheme based on the indistinguishability obfuscation introduced a Third Party Medium (TPM). to design a light-weight remote data integrity auditing scheme. In this scheme, the TPM helps user generate signatures on the condition that data privacy can be protected. In order to support data dynamics, firstly proposed a partially dynamic PDP scheme.used a skip list to construct a fully data dynamic auditing scheme. proposed another remote data integrity auditing scheme supporting full data dynamics by utilizing Merkle Hash Tree. To reduce the damage of users' key exposure, '

The data sharing is an important application in cloud storage scenarios. To protect the identity privacy of user, designed a privacy-preserving shared data integrity auditing scheme by modifying the ring signature for secure cloud storage. \ constructed an efficient shared data integrity auditing scheme, which not only supports the identity privacy but only achieves the identity traceability of users. designed a privacy-aware shared data integrity auditing scheme by exploiting a homomorphic verifiable group signature. In order to support efficient user revocation, proposed a shared data integrity auditing scheme with user revocation by using the proxy re-signature. With the employment of the constructed a shared data integrity auditing scheme supporting user revocation.

The aforementioned schemes all rely on Public Key Infrastructure (PKI), which incurs the considerable overheads from the complicated certificate management. To simplify certificate management, proposed an identity-based remote data

integrity auditing scheme in multicloud storage. This scheme used the user's identity information such as user's name or e-mail address to replace the public key.] designed a novel identity-based proxy- oriented remote data integrity auditing scheme by intro- ducing a proxy to process data for users. constructed a remote data integrity auditing scheme with perfect data privacy preserving in identity-based cryptosys- tems proposed an identity-based data integrity auditing scheme satisfying unconditional anonymity and incentive. proposed an identity-based remote data integrity auditing scheme for shared data support- ing real efficient user revocation.

Other aspects, such as privacy-preserving authentica- and data remote data integrity auditing have also been explored. However, all of existing remote data integrity auditing schemes cannot support data sharing with sensitive information hiding. In this paper, we explore how to achieve data sharing with sensitive infor- mation hiding in identity-based integrity auditing for secure cloud storage.

IV. THE PROPOSED SCHEME

In order to achieve data sharing with sensitive information hiding, we consider making use of the idea in the sanitizable to sanitize the sensitive information of the file by introducing an authorized sanitizer. Nonetheless, it is infeasible if this sanitizable signature is directly used in remote data integrity auditing. Firstly, this signature in [30] is constructed based on chameleon . However, a lot of chameleon hashes exhibit the key exposure problem. To avoid this security problem, the signature used in requires strongly unforgeable chameleon hashes, which will inevitable incur huge computation overhead . Secondly, the signature used in does not support blockless verifiability. It means that the verifier has to download the entire data from the cloud to verify the integrity of data, which will incur huge communication overhead and excessive verification time in big data storage scenario. Thirdly, the signature used in is based on the PKI, which suffers from the complicated certificate management.

In order to address above problems, we design a new effi- cient signature algorithm in the phase of signature generation. The designed signature scheme supports blockless verifiability, which allows the verifier to check the integrity of data without downloading the entire data from the cloud. In addition, it is based on identity-based cryptography, which simplifies the complicated certificate management. In our proposed scheme, the PKG generates the private key for user according to his identity ID. The user can check the correctness of the received private key. When there is a desire for the user to upload data to the cloud, in order to preserve the personal sensitive information of the original file from the sanitizer, this user needs to use a blinding factor to blind the data blocks corresponding to the personal sensitive information of the original file. When necessary, the user can recover the original file from the blinded one by using this blinding factor. And then this user employs the designed signature algorithm to generate signatures for the blinded file.

These signatures will be used to verify the integrity of this blinded file. In addition, the user generates a file tag, which is used to ensure the correctness of the file identifier name and some verification values. The user also computes a transformation value that is used to transform signatures for sanitizer. Finally, the user sends the blinded file, its corresponding signatures, and the file tag along with the transformation value to the sanitizer. When the above messages from user are valid, the sanitizer firstly sanitizes the blinded data blocks into a uniform format and also sanitizes the data blocks corresponding to the organization's sensitive information to protect the privacy of organization, and then transforms their corresponding signatures into valid ones for sanitized file using transformation value. Finally, the sanitizer uploads the sanitized file and the corresponding signatures to the cloud. When the data integrity auditing task is performed, the cloud generates an auditing proof according to the challenge from the TPA. The TPA can verify the integrity of the sanitized file stored the cloud by checking whether this auditing proof is correct or not. The details will be described in the following subsection.

V. METHODOLOGY

Using key-homomorphic cryptographic primitives, we suggest a new architecture of the identity-based (ID-based) RDIC protocol in Fig. 1 to simplify the system and lower the cost of setting up and maintaining the public key authentication framework in PKI-based RDIC schemes.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 10, October 2024
Impact Factor: 5.731

We formalise ID-based RDIC, along with its security model, which includes protection from rogue cloud servers and zero knowledge privacy from a third-party verification.

During the RDIC procedure, the proposed ID-based RDIC protocol does not reveal any information about the stored data to the verifier.

VI. LITERATURE SURVEY

Compare the relative merits of prevailing security theories for public key encryption systems. We take into account the objectives of privacy and non-malleability, separately, for two different types of chosen ciphertext attacks and a chosen plaintext assault. We demonstrate either an implication or a contradiction for each of the resulting pairs of definitions. We describe a fresh method for swiftly revoking user credentials and fine-grained control over their security rights that is based on the idea of an online semi-trusted mediator (SEM). There are a number of practical benefits to using a SEM in conjunction with the mediated RSA cryptosystem as opposed to existing revocation methods. The advantages include faster revocation of signature and decryption capabilities as well as streamlined certificate revocation for legacy systems. "public key" systems allowing data encryption queries Tokens can be created using a secret key to test any supported query predicate. Without learning anything else about the plaintext, the token enables anyone to test the predicate on a given cypher text.

VII. FUTURE SCOPE

We provide evidence that the suggested plan successfully satisfies the criteria for completeness, soundness, and perfect data privacy preservation. While soundness demonstrates that the protocol is secure against an untrusted server, completeness ensures that the protocol is proper. The definition of perfect data privacy is the protocol not disclosing any information about the stored files to the verifier.

VIII. CONCLUSION

In this, we looked into a brand-new basic for safe cloud storage called identity-based remote data integrity checking. We defined the security model of this primitive's two key characteristics, soundness and absolute data privacy. We gave this primitive a fresh design and demonstrated how it achieves soundness and full data privacy. The proposed protocol's effectiveness and applicability were demonstrated by both the numerical analysis and the execution. Group Management with Forward Secrecy and Backward Secrecy by Time Duration & File Recovery when Data Integrity Checking Fault Occurs are extensions of this work.

Data sharing with sensitive information hiding. In our scheme, the file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Besides, the remote data integrity auditing is still able to be efficiently executed. The security proof and the experimental analysis demonstrate that the proposed scheme achieves desirable security and efficiency.

REFERENCES

[1]. P. Mell, T. Grance, Draft NIST working definition of cloud computing, Reference on June. 3rd, 2009. http://csrc.nist.gov/groups/SNC/cloudcomputing/index.html.

[2]. Cloud Security Alliance. Top threats to cloud computing. http://www.cloudsecurityalliance.org, 2010.

[3]. M. Blum, W. Evans, P.Gemmell, S. Kannan, M. Naor, Checking the correctness of memories. Proc. of the 32nd Anual Symposium on Foundations foVomputers, SFCS 1991, pp. 90–99, 1991.

[4]. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N.J. Peterson, D. X. Song, Provable data possession at untrusted stores. ACM Conference on Computer and communications Security, 598-609,2007.

[5]. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson, and D. Song, Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur., 14, 1–34, 2011.

[6]. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson, and D. Song, Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur., 14, 1–34, 2011.

[7]. A.Juels, and B. S. K. Jr. Pors, proofs of retrievability for large files.Proc.of CCS 2007, 584-597, 2007.

[8]. H. Shechem, and B. Waters, Compact proofs of retrievability. Proc. of Cryptology-ASIACRYPT 2008, LNCS 5350, pp. 90-107, 2008.

[9]. G. Ateniese, S. Kamara, J. Katz, Proofs of storage from homomorphicidentification protocols. Proc. of ASIACRYPT 2009, 319-333, 2009.

[10]. A. F. Barsoum, M. A. Hasan, Provable multicopy dynamic data possession in cloud computing systems, IEEE Trans. on Information Forensics and Security, 10(3): 485–497, 2015