International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 31st Mar 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 03

10.48047/IJIEMR/V12/ISSUE 03/78

Title **IDENTITY-BASED DATA OUTSOURCING WITH COMPREHENSIVE AUDITING**

Volume 12, ISSUE 03, Pages: 551-556

Paper Authors

Mr.V.V.R.Manoj, M.Madhulika, J.Susmitha, B.Ruthika

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Identity-Based Data Outsourcing with Comprehensive Auditing

Mr.V.V.R.Manoj[1], Assistant Professor, Department of Computer Science Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
M.Madhulika[2], IV B. Tech Department of Computer Science Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
J.Susmitha[3], IV B. Tech Department of Computer Science Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
B.Ruthika[4], IV B. Tech Department of Computer Science Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada.

Abstract

The term "cloud" refers to the databases and software that operate on servers that may be accessed online. While using cloud storage, it is no longer essential to own and manage data centres in order to store, access, share, and maintain data. To address integrity, controllable outsourcing, and origin auditing concerns on outsourced files, we offer an identity-based data outsourcing (IBDO) solution with desirable features superior to existing data protection ideas. The initial feature of our IBDO solution allows users to authorise dedicated proxies to upload data to the cloud storage server on their behalf. The proxies are identified and approved using their distinguishable identities, unlike conventional secure distributed computing systems, which require complicated certificate administration. Second, Our IBDO scheme offers thorough auditing, i.e., our scheme not only allows for routine integrity auditing as in already-existing schemes, but also allowed for auditing the details of data origin, kind, and consistency of outsourced files. The results of experimental assessment and security analysis show that our IBDO scheme offers good security and favourable performance.

Index Terms: Public auditing, remote integrity verification, proof of storage, cloud storage, and data outsourcing.

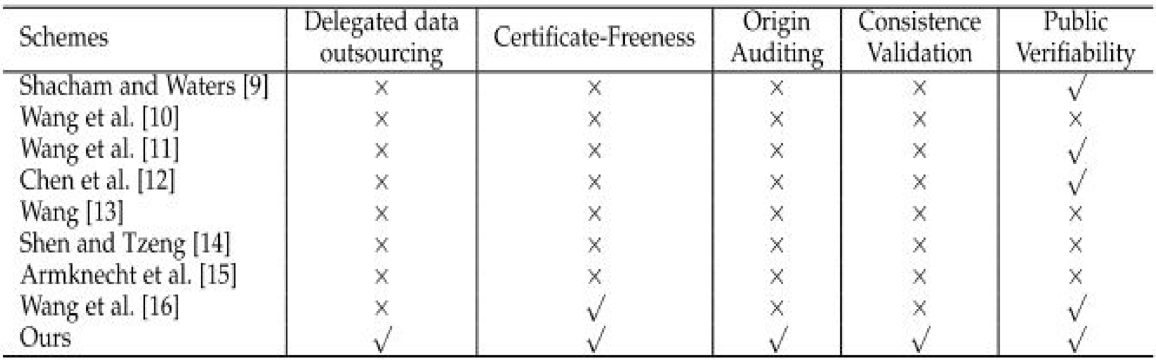
Introduction

The cloud platform is a fantastic resource that offers both consumers and businesses strong storage options. On-to-move access to the outsourced files is one of its major characteristics, and it also frees file owners from difficult local storage management and upkeep. Even though it is offering fantastic advantages as a result of the rapid advancement of technology, cloud storage is vulnerable to certain serious security vulnerabilities that may make it difficult for consumers to use it. As users will no longer have physical access to their data once they have been transferred to a cloud storage server, the "integrity" of the outsourced files is one of the biggest issues. So, the file owners can be concerned about how well the files were outsourced, especially if they are important.

To solve this issue, various ideas have been made. One existing proposal is the concept of "provable data possession," which might be used as a way to demonstrate storage (PoS). The file owner just needs to remember a secret key and a few outsourced file parameters when using PDP. The file owner or an auditor can test the cloud server with minimum communication or processing overhead to see if the files that were outsourced were retained intact. The cloud storage server would not be able to demonstrate the data

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

integrity, for instance, if a portion of the file had been changed or lost as a result of an arbitrary hardware failure. We now acknowledge that the current plans fall short in addressing the two significant problems. First of all, outsourcing is often not controlled in any way. It should be noted that many cloud storage services (including Amazon, Dropbox, and Google Cloud Storage) allow account holders to create signed URLs that can be used by any other authorised person to upload and edit content on the user's behalf. But, in this instance, the delegator is unable to certify that the authorised person sent the appropriate file. The delegator must therefore have complete confidence in the delegates and the cloud server. In fact, in addition to providing people permission to generate and upload data to a cloud, the file owner may be needed to confirm that the uploaded files have not changed. For instance, in Electronic Health Systems (EHS), a patient must first give her doctor permission to create and store electronic health records (EHRs) at a remote EHRs centre. Engineers located all over the world are another typical use case for cloud-based office tools.



Schemes	Delegated data outsourcing	Certificate-Freeness	Origin Auditing	Consistence Validation	Public Verifiability
Shacham and Waters [9]	×	×	×	×	√
Wang et al. [10]	×	×	×	×	×
Wang et al. [11]	×	×	×	×	√
Chen et al. [12]	×	×	×	×	√
Wang [13]	×	×	×	×	×
Shen and Tzeng [14]	×	×	×	×	×
Armknecht et al. [15]	×	×	×	×	×
Wang et al. [16]	×	√	×	×	√
Ours	√	√	√	√	√

Fig: Comparison with Existing Related Works

The group leader can create a cloud storage account and authorize the members with secret identity. The behaviour of the group members and the cloud server should be verifiable. Second, existing PoS-like schemes, including PDP and Proofs of Retrievability (PoR) do not support data log related auditing in the process of data possession proof. The logs are critical in addressing disputes in practice. For example, when the patient and doctor in EHS get involved medical disputes, it would be helpful if some specific information such as outsourcer, type and generating time of the outsourced EHRs are auditable. However, there exist no PoS-like schemes that can allow validation of these important information in a multi-user setting.

I. Our Contributions

This study suggests an identity-based data outsourcing (IBDO) approach to address the aforementioned problems with providing secured outsourced data in the cloud. In contrast to other ideas, our plan has the following qualities.

- **Outsourcing based on identity.** Users and their authorised proxies can safely outsource files to a remote cloud server that may not be completely reliable, but any unauthorised parties are prohibited from doing so on the owner's or user's behalf. By avoiding the danger of certificate administration, the cloud clients, including the file-owners, proxies, and auditors, are recognised with their own identities. This technique enables many users in a setting as well.

- **Strong security guarantee.** Strong security is achieved by our plan. This means that it can identify any unauthorised changes made to files that were outsourced as well as any abuse of authorizations. These security features have been demonstrated to be effective against active collaborating attackers, or covert attackers. According to our understanding, this is the first plan that successfully accomplishes both objectives.
- **Comprehensive auditing.** Our IBDO programme features a robust auditing system. Because an auditor is a computer and uses a computer-generated report to perform some aspect of assurance, the integrity (i.e., no corruption in the data that can be assured with consistency and accuracy over time) of outsourced files can be effectively verified by an auditor, even if the files are outsourced by different clients. Also, additional information regarding the source, nature, and consistency of the outsourced data can be watched by the public. The advantage of the comprehensive auditability, which is also similar to the existing auditable schemes, is that it enables a public common auditor to examine the files that have been outsourced by various users, and in the event of a dispute, the auditor can use the auditing protocol to produce convincing evidence.

II. Related Work

The PDP, developed by Ateniese et al., enables an auditor to verify the integrity without downloading the entire file from the cloud server. In addition, the server need not access the entire file to respond to integrity queries. A fantastic job was done on the file that was outsourced in terms of modification and deletion, but not insertion activities. A plan for supporting dynamic update for the outsourced file was developed by Yang and Jia. In order to create verifiable metadata in a blind manner, Wang et al. included a third-party mediator into the PDP system. In a multi-user context, Wang et al. suggested a secure cloud storage technique with user revocation using proxy re-signatures; if a user is revoked, then the cloud storage server will re-sign their outsourced data.

A methodical approach is provided to build a secure cloud storage scheme from any secure networking coding protocol, according to Chen et al researcher's on the connection between secure cloud storage and secure networking coding. Publicly verifiable data outsourcing by Zhang and Dong is demonstrated with stringent security reduction in an ID-based environment. A certificateless public verification approach created by Zhang et al. offers stronger protection against a dishonest auditor. Three PoR schemes with private and public verifiability were also given by Shacham and Water. These are the first PoR schemes with strict security proofs.

For privately auditable PoR methods, Armknecht et al. researched delegatable auditing, which simultaneously guards against collusion assaults by nefarious clients, auditors, and cloud servers. Wang et al. suggested a safe data outsourcing method in the identity-based setting based on a variant of the Schnorr signature, but their scheme similarly does not enable delegated data outsourcing mechanisms.

Methodology

I. System Architecture

Five different categories of entities make up the architecture of our IBDO system: file owners, proxies, auditors, registry servers, and storage servers. File owners, proxies, and auditors are typically cloud clients. The system configuration and client registration are handled by the registry server, a dependable third party that also enables registered clients to save the public parameters of outsourced files. For the purpose of storing outsourced files, the cloud storage server offers storage services to approved clients.

The cloud server can be used to offshore files by the file owner and authorised proxies. More specifically, the authorised proxy processes the file on behalf of the owner, uploads the corresponding public parameters of the file to the registry server, and transmits the processed results to the storage server. The original file or the processed file need not be kept locally by either the file-owner or the proxy. The auditor must communicate with the cloud storage server to verify the authenticity of outsourced files and their origin, such as general log data, without downloading the complete file.

In practical applications, a company purchases storage services from a CSP, and the IT division of the company can act as a registry server. The storage services are therefore available to the registered clients (workers).

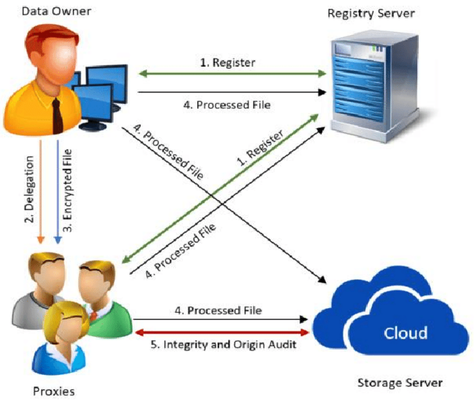


Fig 1: The architecture of IBDO system

II. Module Analysis

The modules in this scheme are of five types. They are:

- File Owner
- Proxies
- Auditor
- Registry Server
- Storage Server

MODULES DESCRIPTION

File owner:

One of the clients of the cloud is the file owner. Register your information with the registry server, file owner. Owners of the files upload them to a storage server. trustworthy proxies are permitted to upload files to storage servers by the file owner. The file owner will send a secret key to activate the proxies. Following activation, the file owner will distribute the file to the proxies required for cloud storage.

Proxies:

Delegated individuals are proxies. On behalf of the file owner, they will upload the data to the cloud storage server. Proxies are also registered with registry servers; for instance, a business may give specific employees permission to upload data in a regulated manner to the company's cloud account. In contrast to typical secure distributed computing systems, which need complex certificate administration, the proxies are identified and approved using their distinguishable identities. These registered proxies will function as an approved proxy once they are activated.

Auditor:

The auditor's responsibility is to connect with the cloud storage server without downloading the complete file in order to verify the authenticity of outsourced data and their source, such as general log information. Our IBDO plan successfully creates a reliable auditing system. Even though the files may have been outsourced by many clients, an auditor can effectively verify the integrity of the files. Moreover, information regarding the source, nature, and consistency of outsourced files can be audited openly.

Registry Server:

All cloud clients (file owners, auditors, and proxies) have their identities registered in the registry server. Files that have been handled by both file owners and proxies may be seen by registry servers. In practical applications, a company purchases storage services from a CSP, and the IT division of the company can act as a registry server.

Storage Server:

This storage server may be owned by a company and is maintained by a Cloud Service Provider (CSP). Employees who have registered as clients can therefore benefit from this storage server. The cloud will receive files in an encrypted manner from the file owner and designated proxies. The integrity of processed files that are uploaded into the cloud will be examined by the auditor.

III. Security Goals

Two different active attack types are faced by an IBDO system. A rogue storage server could alter or even delete the outsourced files thanks to the cloud client, especially if they are rarely visited files.

To solve all the attacks IBDO system has following requirements:

- Dedicated delegation: A delegation granted by the file owner can only be used by one authorised proxy at a time to access the files, and numerous proxies are unable to determine whether a delegation is legitimate in order to outsource a potential file.

- Comprehensive auditing: It not only guarantees integrity but also upholds the correct information on the kind, consistency, and origin of an outsourced file. An IBDO system can offer reliable proofs since it retains both integrity and log information.

IV. Experimental Analysis

The IBDO approach offers durable security features without suffering any large performance costs, according to both theoretical analysis and experimental findings. It enables the file owner to provide proxies access to her outsourcing power. The file can only be processed and outsourced on behalf of the file owner by the authorised proxy. A public auditor can confirm the file's origin and integrity.

Figure 2 illustrates the performance of creating and validating a delegation in Dlgtn and a private key for a specific user in Regst. Each of these stages takes about 10ms, which is very little time when deploying in practical applications.

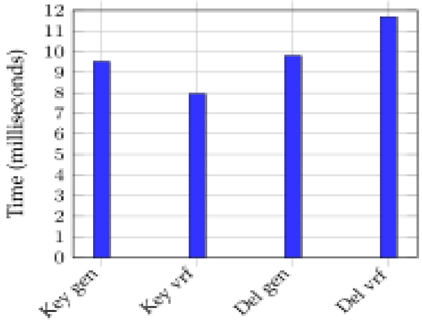
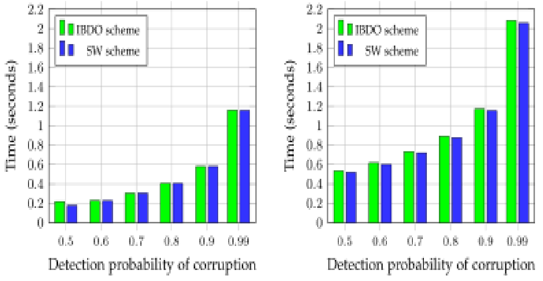


Fig. 2. Performance of Regst and Dlgtn

The simulation results shown in Figure 3 show that our IBDO scheme executes the auditing protocol as effectively on the side of the auditor and cloud storage server as the SW scheme does. For instance, the auditor can complete both schemes in less than 1.2 seconds for a 0.9 detection probability. Also, according to the theoretical study, in both schemes the time cost on the auditor side is higher than on the cloud side. Keep in mind that in a multi-auditor situation, the former can be shared by numerous auditors. A lower detection probability necessitates fewer computations, making each auditor involved more productive.



(a) (b)

Fig 4: Performance in a round of (comprehensive) auditing protocol with different detection probability on a 1% corrupted file. (a) Cloud side. (b) Auditor side.

V. Conclusion

We looked into cloud storage proofs in a multi-user environment. We defined identity-based data outsourcing and suggested a safe IBDO system. It enables the file owner to assign proxies with her outsourcing authority. The file can only be processed and outsourced on behalf of the file owner by the authorised proxy. A public auditor can confirm the file's origin and integrity. Our scheme has an edge over current PDP and PoR schemes thanks to the identity-based feature and the thorough auditing feature. Experimental findings and security studies demonstrate that the suggested scheme is safe and performs as well as the SW scheme.

VI.FUTURE ENHANCEMENTS

The first effective Identity-Based Encryption system that is secure in the whole model without random oracles was presented by our team. By restricting our scheme to the decisional Bilinear Diffie-Hellman issue, we were able to demonstrate its security. Furthermore, we demonstrated how our Identity-Based encryption technique can be transformed into a reliable signature system that simply relies on the computational Diffie-Hellman assumption.

Two intriguing open problems are motivated by this work. Finding an Identity-Based Encryption system with short public parameters and efficiency (without random oracles) is the initial step. The second is to locate an IBE system with a strict security decrease. Such a method would also likely offer an efficient reduction for an analogous HIBE scheme.

References

[1] Cloud data protection for the masses: D. Song, E. Shi, I. Fischer, and U. Shankar, Computing, IEEE, vol. 45, no. 1, pp.

[2] Security considerations in popular cloud storage services, Pervasive Computing, IEEE, vol. 12, no. 4, pp. 50–57, C.-K. Chu, W.-T. Zhu, J. Han, J. Liu, J. Xu, and J. Zhou.

[3] K. Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities," World Wide Web, vol. 15, no. 4, pp. 409–428.

[4]https://www.researchgate.net/figure/System-Model_fig1_327337186.

[5] "Provable data possession in untrusted storage," Proc. 14th ACM Conf. Comput. Commun. Secur., New York, NY, USA, G. Ateniese et al., pp. 598–609.

[6] Partha Pratim Ray (2018). Dew Computing: Definition, Concept, and Consequences - IEEE Journals & Magazine. S2CID 3324933. IEEE Access. 6: 723–737. doi:10.1109/ACCESS.2017.2775042. On 2021-02-10, the original version was archived. 2021-02-12 retrieved.

[7] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 6, pp. 754–764.

[8] "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," by J. Sun, X. Zhu, C. Zhang, and Y. Fang, in Proc. IEEE 31st Int. Conf. Distrib. Comput. Syst. (ICDCS), pp. 373–382.

[9] IDC predicts that by 2025, global "whole cloud" spending will total $1.3 trillion. Idc.com. 2021-09-14. On 2022-07-29, the original version was archived. Retrieved July 30, 2022.

[10] The History of Auditing by Derek Matthews. The evolving auditing procedure since the 19th century. ISBN 9781134177912. Routledge-Taylor & Francis Group, page 6.