OUTSOURCING OF FILES BASED ON IDENTITY WITH AUDITING IN CLOUDS

[1]Amarunnisa Begum, [2]Dr. A. Amarendra Babu, [3]Ayesha Sania, [4]A. Nikhil Kumar
[1,3,4] B.Tech- Student, CSE, St. Martin's Engineering College, Secunderabad, India.
[2]Professor, CSE, St. Martin's Engineering College, Secunderabad, India.

***Abstract*:** Cloud storage system provides facilities like sharing services and data storage for distributed clients. To address integrity, controllable outsourcing and origin evaluating concerns on outsourced files, we propose an identity based data outsourcing (IBDO) plot outfitted with desirable features advantageous over existing proposals in securing outsourced information. First, our IBDO plot enables a user to authorize dedicated proxies to transfer information to the distributed storage server for her behalf, e.g., an organization may approve a few employees to transfer files to the organization's cloud account in a controlled way. The proxies are identified and approved with their conspicuous identities, which eliminates complicated certificate management in normal secure distributed computing systems. Second, our IBDO plot encourages comprehensive auditing, i.e., our scheme not just allows regular integrity auditing as in existing schemes for securing outsourced information, yet additionally permits to audit the information on data origin, type and consistence of outsourced files. Security investigation and experimental evaluation show that our IBDO scheme gives solid security with desirable efficiency.

Index Terms—Cloud storage model, Outsourcing of data, Proof of storage, Integrity, Auditing.

1. INTRODUCTION

Cloud system provides storage services to individuals and associations [1]. It brings awesome benefits of permitting on the move access to the outsourced files, at the same time relieves file-proprietors from complicated maintenance and local storage management [2]. However, some security concerns may hinder clients to utilize distributed storage. Among them, the integrity of outsourced files is considered as a main impediment [3], since the clients will lose physical control of their files after outsourced to a distributed storage server maintained by some cloud service provider (CSP). In this manner, the file-proprietors may stress over whether their files have been messed with, particularly for those of significance. Extensive endeavors have been made to address this issue. Among existing proposals, provable data possession (PDP) [4] is a promising methodology in proof of storage(PoS). With PDP, the file-proprietor just needs to retain a small amount of parameters of outsourced files and a secret key. To check whether the outsourced files are kept intact, the file proprietor or a auditor can challenge the cloud server with computation costs and low communication overheads. If some part of the data file has been changed or erased, for instance, due to random hardware failures, the distributed storage server would not have the ability to prove the integrity of data to convince the users. We observe two basic issues not well addressed in existing schemes. First, most proposals do not have a controlled method for delegatable outsourcing. One may note that numerous distributed cloud storage systems(e.g., Amazon, Dropbox, Google cloud storage) enable the account proprietor to create signed URLs using which some other designated entity can transfer, and change content on behalf of the client. However, in this situation, the delegator can't validate whether or not the authenticated one has uploaded the file as specified or verify whether or not the transferred data file has been kept intact. Hence, the delegator needs to completely trust delegates and the cloud server. In fact, the file-proprietor may not just need to authorize some others to create files and upload to a cloud, yet in addition need to verifiably ensure that the transferred files have been kept unaltered. For example, in Electronic Health Systems (EHS) [5], [6], while counseling a specialist, the patient needs to delegate her specialist to produce electronic health records (EHRs) and store them at a remote EHRs center maintained by a CSP [7]. In another situation of cloud-aided office applications, a group of engineers in different places may fulfill an assignment in cooperation. The group leader can generate a distributed storage account and authorize the individuals with secret warrants. The behavior of the group individuals and the cloud server ought to be verifiable.

Second, during the process of data possession proof, existing PoS-like schemes, including PDP and Proofs of Retrievability (PoR) [8], do not support information log related auditing. In practice, the logs are critical in addressing disputes. For instance, when the patient and specialist in EHS get involved in medical disputes, it would be useful if some specific data, for example, outsourcer, type and creating time of the outsourced EHRs are auditable. However, there exist no PoS-like proposals that can permit validation of these vital data in a multi-client setting.

2. LITERATURE SURVEY

A. Cloud Data Protection For The Masses

The challenging task is to offer strong data protection to cloud users while enabling rich applications. Researchers explore a new cloud platform architecture called Data Protection as a Service, which dramatically reduces the per-application development effort required to offer data protection, while still allowing rapid development and maintenance.

B. Security problems in Cloud Storage Services

A security analysis is done on the sharing methods of three main synchronization and cloud storage services: Dropbox, Google Drive, and Microsoft SkyDrive is provided by the authors. They had proved that all three services have poor security that may result in leakage of data without user's awareness.

C. Data Storage and Auditing Service In Cloud Computing

Cloud computing is a promising model that permits convenient and on-demand network access to a shared pool of configurable computing resources. The first service offered by cloud is moving data into the cloud: data owners let cloud service providers host their data on cloud servers and data consumers can access the data from the cloud servers. The new security challenges are introduced by this new paradigm of data storage service , because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to ensure that the data is properly hosted in the Cloud. In this paper, we studied this kind of problem and done an extensive survey of storage auditing methods in the literature. First, we give a set of requirements of the auditing protocol for data storage in cloud computing. Then, some existing auditing schemes are introduced and analyze them in terms of performance and security. Finally, in the design of efficient auditing protocol for data storage in cloud computing some challenging issues are introduced.

D. Provable Data Possession at Untrusted Sites

When a client stores the data at an untrusted sever to verify that the server possesses the original data without extracting it , then provable data possession model is used. This model creates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically minimizes I/O costs. A constant amount of metadata is maintained by the client to verify the proof. A small, constant amount of data is transmitted by the challenge/response protocol, which reduces network communication. Thus, for remote data checking the PDP model supports large data sets in widely-distributed storage systems. Two PDP schemes are presented which are more efficient than previous results, even when compared with schemes that achieve poor guarantees. The overhead at the server is low, as opposed to linear in the size of the data. The performance of PDP is bounded by disk I/O and not by cryptographic computation is revealed by the experiments as well as practicality of PDF is also verified.

E. Cross-Domain Sharing of Data in Distributed Electronic Health Record Systems

In Electronic Health Record (EHR) system, a cross-organization or cross-domain cooperation takes place from time to time for necessary and high-quality patient treatment. Since the cooperation inevitably involves exchanging and sharing relevant patient data that are considered highly private and confidential, cautious design of delegation mechanism must be in place as a building block of cross-domain cooperation. The delegation mechanism grants permission to and restricts access rights of a cooperating partner. Patients are not ready to accept the EHR system unless their health data are guaranteed proper use and disclosure, which cannot be easily achieved without cross-domain authentication and fine-grained access control. In addition, revocation of the delegated rights should be possible at any time during the cooperation. In this paper, we propose a secure EHR system, based on cryptographic constructions, to enable secure sharing of sensitive patient data during cooperation and preserve patient data privacy. Our EHR system further incorporates advanced mechanisms for fine-grained access control, and on-demand revocation, as enhancements to the basic access control offered by the delegation mechanism, and the basic revocation mechanism, respectively. The proposed system of EHR is demonstrated to achieve objectives specific to the cross-domain delegation scenario of interest.

3. OVERVIEW OF THE SYSTEM

3.1 SYSTEM ARCHITECTURE

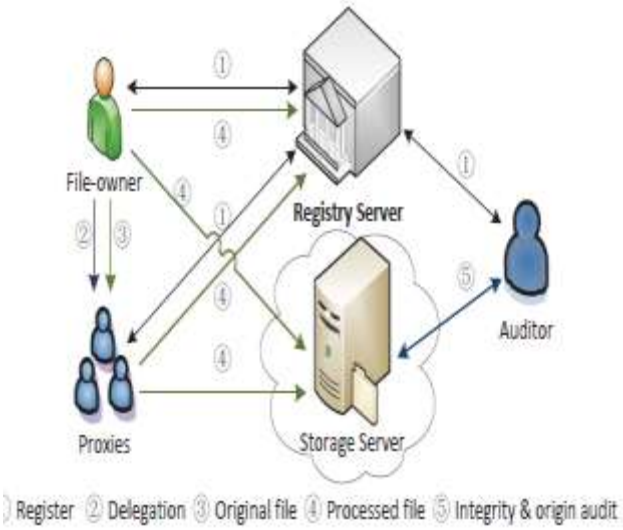

Fig. 1. System Architecture

3.2 MODULES

An IBDO system consists of five types of entities i.e., file-owners, proxies, auditors, registry server, and storage server. Generally, the file-owners, proxies and auditors are cloud clients

3.2.1 File Owner

File owner will register with application and registration details are sent to registration server for authentication after authentication is successful owner can login with username and password and upload files to cloud server directly or through proxy server. If owner is uploading directly to cloud server his attribute details like file name, size, user name are sent to registry server and files are encrypted and then sent to cloud server. In the same way if data is uploaded to cloud server through proxy server attributes are sent to proxy server and then encrypted files are uploaded to cloud server. Owner can view all uploaded files by proxy and owner and owner can also a type of user who can request for file download of other owners.

3.2.2 Proxies

On behalf of the owner, the authorized proxy processes the file, sends the processed results to the storage server, and uploads the corresponding public parameters of the file to the registry server. Neither the file-owner nor the proxy is required to store the original file or the processed file locally.

Proxy can be curious person who can modify data of user and upload to cloud server. When proxy uploads data file parameters are sent to registry server.

3.2.3 Registry Server

The registry server is a trusted party responsible for setting up the system and responding to the client's registration, and also allows the registered clients to store the public parameters of outsourced files.

Registry server can verify user and proxy registration and give authentication and he also stores public parameters of each file uploaded by user as well as proxy server. He will send public parameter details to auditor.

3.2.4 Storage Server

The cloud storage server provides storage services to the registered clients for storing outsourced files. Storage server can view details of file uploaded by user and proxy server. Storage server can send details of uploaded files to auditor for verification.

3.2.5 Auditor

The duty of the auditor is to check the integrity of outsourced files and their origin like general log information by interacting with the cloud storage server without retrieving the entire file.

Auditor will get information of each user and proxy uploaded files details through registry server also. He will verify integrity based on files information received from cloud server and registry server. If there are any changes in file size auditor will consider it as modified file.

4. METHODOLOGY

In IBDO, it is challenging to accomplish both proxy information outsourcing and comprehensive auditing functionalities. At a first, it appears that if the owner of the data has delegated his/her outsourcing rights to some proxy, at that point the authenticated proxy can essentially utilize the existing PDP/PoR proposals for processing and outsourcing data files. But, there exists a gap that the information of the owner of the file isn't bounded with the data, which leaves a Vulnerability that the proxy may abuse the delegation without being caught, even though this delegation has been signed by the owner of the data. In our IBDO development we will fill this gap. In our IBDO framework, the owner of the file signs a dedicated warrant for the proxy in order to delegate outsourcing rights to a proxy. The warrant may determine who can outsource which sort of files amid what time on behalf of owner of the file, and so on. At the point file is divided into blocks when it is processed in order to create metadata for each block individually. The warrant ought to be embedded into each metadata, to portray that the metadata are produced by the authenticated proxy. The auditor also asks for the aggregate metadata and the signed warrant except the aggregate file blocks during the execution of origin and integrity auditing. To conclude that data is intact and is indeed outsourced by the one as specified in the warrant then both the aggregate metadata and signed warrant ought to be audited. From a specialized perspective, we utilize Paterson and Schuldt's identity based signature proposals [10] as building block. In this way the delegation which is produced as a identity based signature on a warrant by their proposal, can be publicly verified in Audit protocol of IBDO framework. Additionally, we follow the system due to Shacham and Waters [9] to part the file blocks while creating metadata, which gives a trade-off between communication overheads and storage costs in auditing.

5. CONCLUSION

In this paper, we examined proofs of storage in cloud in a multi-client setting. We presented the idea of identity based information outsourcing and proposed a secure IBDO plot. It permits the data-owner to delegate his/her outsourcing capability to proxies. Only the authenticated proxies can process and outsource the data on behalf of the data-owner. A public auditor can verify both the data integrity and origin. The comprehensive auditing and the identity based features make our plan advantageous over existing PDP/PoR proposals. Security examinations and outcomes of experiments show that the proposed system is secure and has comparable performance as the SW scheme.

REFERENCES

[1] D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud data protection for the masses,” Computer, IEEE, vol. 45, no. 1, pp. 39–45, Jan 2012.

[2] C.-K.. Chu, W.-T. Zhu, J. Han, J. Liu, J. Xu, and J. Zhou, “Security concerns in popular cloud storage services,” Pervasive Computing, IEEE, vol. 12, no. 4, pp. 50–57, Oct 2013.

[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, 2012.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” in Proceedings of the 14th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM, 2007, pp. 598–609.

[5] J. Sun and Y. Fang, “Cross-Domain Data Sharing in Distributed Electronic Health Record Systems,” Parallel and Distributed Systems, IEEE Transactions on, vol. 21, no. 6, pp. 754–764, 2010.

[6] J. Sun, X. Zhu, C. Zhang, and Y. Fang, “HCPP: Cryptography based Secure EHR System for Patient Privacy and Emergency Healthcare,” in Distributed Computing Systems (ICDCS), 2011 IEEE 31st International Conference on. IEEE, 2011, pp. 373–382.

[7] L. Guo, C. Zhang, J. Sun, and Y. Fang, “PAAS: A Privacy Preserving Attribute-Based Authentication System for e Health Networks,” in Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on. IEEE, 2012, pp. 224–233.

[8] A. Juels and B. S. Kaliski, Jr., "PoRs: Proofs of Retrievability for Large Files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, New York, NY, USA, 2007, pp. 584– 597.

[9] H. Shacham and B. Waters, "Compact proofs of retrievability," Journal of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[10] K. G. Paterson and J. C. N. Schuldt, "Efficient Identity-Based Signatures Secure in the Standard Model," in Information Security and Privacy, ser. LNCS, L. Batten and R. Safavi-Naini, Eds., vol. 4058. Springer, Heidelberg, 2006,pp.207-22