Identity-Based Data Outsourcing withComprehensive Auditing in Clouds

ABSTRACT:

Cloud storage system provides facilitative file storage and sharing services for distributed clients. To address integrity,controllable outsourcing and origin auditing concerns on outsourced files, we propose an identity-based data outsourcing (IBDO)scheme equipped with desirable features advantageous over existing proposals in securing outsourced data. First, our IBDO schemeallows a user to authorize dedicated proxies to upload data to the cloud storage server on her behalf, e.g., a company may authorizesome employees to upload files to the company's cloud account in a controlled way. The proxies are identified and authorized with theirrecognizable identities, which eliminates complicated certificate management in usual secure distributed computing systems. Second,our IBDO scheme facilitates comprehensive auditing, i.e., our scheme not only permits regular integrity auditing as in existing schemesfor securing outsourced data, but also allows to audit the information on data origin, type and consistence of outsourced files. Securityanalysis and experimental evaluation indicate that our IBDO scheme provides strong security with desirable efficiency.

EXISTING SYSTEM:

- Among existing proposals, provable data possession (PDP) is a promising approach in proof of storage (PoS). With PDP, the file-owner only needs to retain a small amount of parameters of outsourced files and a secret key. To

check whether or not the outsourced files are kept intact, the fileowner or an auditor can challenge the cloud server with low communication overheads and computation costs. If some part of the file has been altered or deleted, for example, due to random hardware failures, the cloud storage server would not be able to prove the data integrity to convince the clients.

- Tzeng proposed a delegatable PDP scheme, where a user can delegate integrity auditing capability to a delegate so that the delegatee can perform auditing protocol on any outsoured files of this user.
- Armknecht et al. studied delegatable auditing for privately auditable PoR schemes, which simultaneously protects against collusion attacks by malicious clients, auditors and cloud servers.
- Based on a variant of the Schnorr signature, Wang et al. proposed a secure data outsourcing scheme in the identity-based setting, however, their scheme also does not support delegated data outsourcing mechanism.

DISADVANTAGES OF EXISTING SYSTEM:

- The users will lose physical control of their files after outsourced to a cloud storage server maintained by some cloud service provider (CSP). Thus, the file-owners may worry about whether their files have been tampered with, especially for those of importance.
- We observe two critical issues not well addressed inexisting proposals. First, most schemes lack a controlled wayof delegatable outsourcing.

- The delegator cannot validate whether or not the authorized one has uploaded the file as specified or verify whether or not the uploaded file has been kept intact. Hence, the delegator has to fully trust the delegatees and the cloud server. In fact, the file-owner may not only need to authorize some others to generate files and upload to a cloud, but also need to verifiably guarantee that the uploaded files have been kept unchanged.
- 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.

PROPOSED SYSTEM:

- To address the existing issues for securing outsourced data in clouds, this paper proposes an identity-based data outsourcing (IBDO) system in a multi-user setting.
- Our scheme has the following distinguishing features.
- **Identity-based outsourcing.** A user and her authorizedproxies can securely outsource files to a remotecloud server which is not fully trustable, while anyunauthorized ones cannot outsource files on behalf ofthe user. The cloud clients, including the file-owners,proxies and auditors, are recognized with their identities,which avoids the usage of complicatedcryptographic

certificates. This delegate mechanismallows our scheme to be efficiently deployed in amulti-user setting.

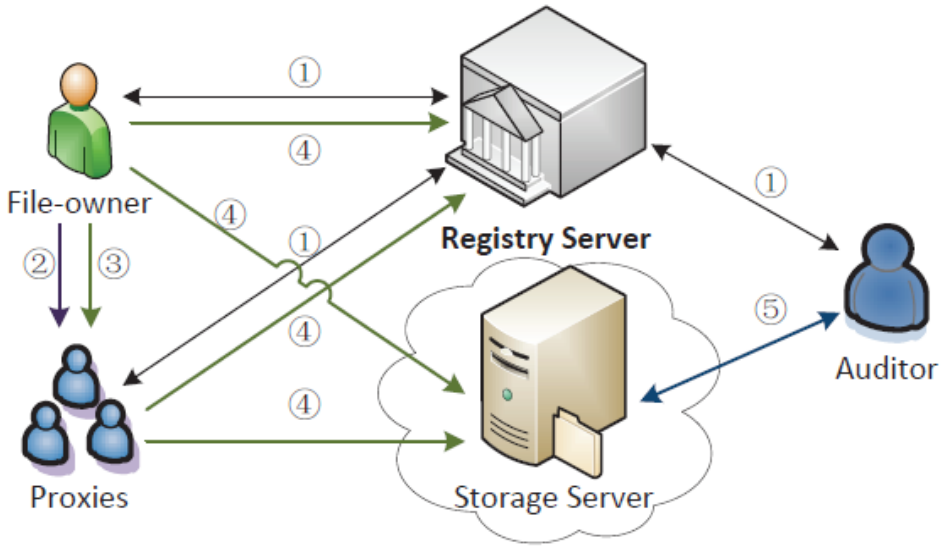
- **Comprehensive auditing.** Our IBDO schemeachieves a strong auditing mechanism. The integrityof outsourced files can be efficiently verified byan auditor, even if the files might be outsourcedby different clients. Also, the information about theorigin, type and consistence of outsourced files canbe publicly audited. Similar to existing publicly auditableschemes, the comprehensive auditability hasadvantages to allow a public common auditor toaudit files owned by different users, and in case ofdisputes, the auditor can run the auditing protocolto provide convincing judicial witnesses without requiringdisputing parties to be corporative.
- **Strong security guarantee.** Our IBDO schemeachieves strong security in the sense that: (1) it candetect any unauthorized modification on the outsourcedfiles and (2) it can detect any misuse/abuseof the delegations/authorizations. These securityproperties are formally proved against active colludingattackers. To the best of our knowledge, this is thefirst scheme that simultaneously achieves both goals.

ADVANTAGES OF PROPOSED SYSTEM:

- Both theoretical analyses and experimental results confirm that the IBDO proposal provides resilient security properties without incurring any significant performance penalties.
- It allows the file-owner to delegate her outsourcing capability to proxies.
- Only the authorized proxy can process and outsource the file on behalf of the file-owner.

❖ Both the file origin and file integrity can be verified by a publicauditor.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB.

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

Yujue Wang, Qianhong Wu, Member, IEEE, Bo Qin, Wenchang ShiRobert H. Deng, Fellow, IEEE, Jiankun Hu, "Identity-Based Data Outsourcing withComprehensive Auditing in Clouds",**IEEE Transactions on Information Forensics and Security, 2017.**