PRIVACY-PRESERVING PUBLIC AUDITING FOR REGENERATING-CODE-BASED CLOUD

ABSTRACT

To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. Recently, regenerating codes have gained popularity due to their lower repair bandwidth while providing fault tolerance. Existing remote checking methods for regenerating-coded data only provide private auditing, requiring data owners to always stay online and handle auditing, as well as repairing, which is sometimes impractical. We propose a public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, we introduce a proxy, which is privileged to regenerate the authenticators, into the traditional public auditing system model.

Moreover, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating-code-based cloud storage.
ARCHITECTURE

EXISTING SYSTEM

The overhead of using cloud storage should be minimized as much as possible such that a user does not need to perform too many operations to their outsourced data. In particular, users may not want to go through the complexity in verifying and reparation.

DRAWBACK OF EXISTING SYSTEM

- To fully ensure the data integrity and save the users’ computation resources as well as online burden.
- Both of them are designed for private audit, only the data owner is allowed to verify the integrity and repair the faulty servers. Considering the large size of the outsourced data and the user’s constrained resource capability, the
tasks of auditing and reparation in the cloud can be formidable and expensive for the users.

PROPOSED SYSTEM

Many mechanisms dealing with the integrity of outsourced data without a local copy have been proposed under different system and security models up to now.

The most significant work among these studies are the PDP (provable data possession) model and POR (proof of retrievability) model, which were originally proposed for the single-server scenario.

Considering that files are usually striped and redundantly stored across multi-servers or multi-clouds, explore integrity verification schemes suitable for such multi-servers or multi-clouds setting with different redundancy schemes, such as replication, erasure codes, and, more recently, regenerating codes.

ADVANTAGE OF PROPOSED SYSTEM

- Universal data access with location independence
- Relief of the burden for storage management
- Avoidance of capital expenditure on hardware, software, and personal maintenances, etc.,
SYSTEM SPECIFICATION

Hardware Requirements

System : Pentium IV 2.4 GHz
Hard Disk : 40 GB
Floppy Drive : 1.44 Mb
Monitor : 15 VGA Colour
Mouse : Logitech
Ram : 512 Mb

Software Requirements

Operating system : Windows XP
Technology Used : Microsoft .NET
Backend Used : SQL Server
Do Your Projects With Domain Experts...