Message-Locked Encryption for Secure Cloud Deduplication

Cross-user deduplication in cloud storage creates security challenges. Message-locked encryption (MLE) derives encryption keys from the message content, allowing the cloud to detect duplicates without accessing plaintext.

Convergent encryption is the simplest MLE scheme but is vulnerable to offline brute-force attacks on predictable files. Server-aided MLE schemes address this by involving a key server in the key derivation process.

Proof-of-ownership protocols ensure that only clients who possess the full file can claim ownership of deduplicated data. This prevents a malicious client from gaining access to files by only knowing their hash values.