Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 03, Issue 9, pp 588-590, September, 2026

Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking Protocol with Time-Bound Access in Public Cloud

[1]A.Dileep, [2]Ch.Pavan, [3]B Sowmika, [4]K Sowjanya

[1,2,3,4] Department of ECE
Narsimha Reddy Engineering College, Hyderabad

ABSTRACT:

As cloud storage adoption accelerates, large-scale data owners increasingly outsource their data to Public Cloud Servers (PCS) to minimize infrastructure and operating costs. However, maintaining control over remote data integrity and guaranteeing data confidentiality remains a significant technical hurdle. In many realistic scenarios, data owners face operational constraints—such as administrative isolation or connectivity restrictions—preventing direct interaction with cloud servers. To address these limitations, we propose a novel secure identity-based proxy-oriented data uploading and remote data integrity checking framework (ID-PUIC). Under this framework, restricted clients delegate data processing and uploading privileges to an authorized proxy server, which maintains a local backup to enable data restoration in case of cloud corruption. Furthermore, our scheme integrates a dedicated Time Server to enforce strictly bounded time-slot accessibility for uploaded files. Security analysis demonstrates that the proposed ID-PUIC protocol is provably secure against forgery attacks under the Computational Diffie-Hellman (CDH) assumption over bilinear groups, achieving flexible private, delegated, and public integrity auditing capabilities without heavy Public Key Infrastructure (PKI) certificate overheads.

Keywords: Cloud Storage Auditing, Identity-Based Cryptography, Proxy-Oriented Uploading, Remote Data Integrity Checking, Bilinear Pairings, Time-Bound Access Control.

1. INTRODUCTION

Cloud storage offers on-demand data outsourcing services, gaining wide popularity due to its elasticity and lower maintenance expenditure. However, transferring data control to third-party Public Cloud Servers (PCS) introduces security risks regarding data confidentiality, availability, and integrity. When an individual data owner is unable to access cloud networks directly (e.g., during administrative investigations or travel), legal business operations must continue seamlessly. The owner delegates data processing and uploading duties to a trusted proxy (e.g., a secretary or designated officer). However, delegation must not compromise privacy or grant permanent uncontrolled verification access to external entities.

To address certificate management overheads inherent in conventional Public Key Infrastructure (PKI), Identity-Based Cryptography (IBC) is integrated with proxy public key primitives. This eliminates costly public key certificates while providing robust integrity verification.

2. EXISTING SYSTEM ANALYSIS

In traditional cloud models, clients directly upload data and perform Remote Data Integrity Checking (RDIC) via Internet protocols. In delegation scenarios relying on traditional Public Key Infrastructures (PKI), several severe operational bottlenecks emerge:

2.1 Limitations & Disadvantages

Heavy Certificate Management: PKI-based authentication mandates continuous certificate generation, verification, delivery, and revocation checking, inducing massive computational overheads.

Resource Constraints: End-user devices (e.g., smartphones, low-power laptops) lack the computational power needed to verify multiple PKI certificates per audit.

Single Point of Failure: Lack of proxy backup mechanisms means corrupted cloud data cannot be reconstructed locally.

3. PROPOSED SYSTEM MODEL

The proposed ID-PUIC framework eliminates PKI certificate overheads by employing Identity-Based Cryptography where entity public keys are directly derived from known string identifiers (e.g., email IDs or IP addresses).

4. SYSTEM ARCHITECTURE DIAGRAM

The architecture introduces a dual-defense layer consisting of an authorized Proxy Server and a temporal Time Server. The proxy retains an encrypted cache of uploaded files to guarantee immediate local recovery if cloud storage integrity fails. The Time Server enforces rigorous time-stamped access windows after which cloud files automatically become un-decryptable and inaccessible.

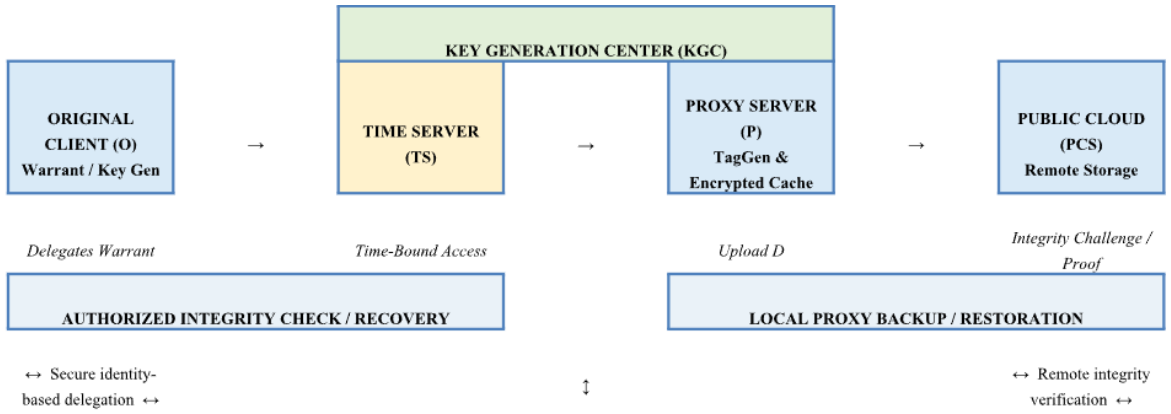

Figure 1: High-Level System Architecture and Interactions of ID-PUIC Protocol.

4.1 Key Advantages

Provable Security: Formal security reduction under the Computational Diffie-Hellman (CDH) problem over bilinear pairings.
Zero Certificate Overhead: Eliminates certificate revocation lists (CRLs) and verification chains.
Multi-Mode Auditing: Supports private checking (client only), delegated checking (third-party auditor), and public checking depending on authorization degrees.
Fault Recovery: Automatic file recovery from local proxy caches upon cloud data integrity failure detection.

5. CORE FUNCTIONAL MODULES

The ID-PUIC protocol consists of four key entities:
Original Client: Holds large data assets, grants authorization via formal warrants, and verifies data integrity.
Public Cloud Server (PCS): Offers flexible storage and computational resources to host client data.
Proxy Server: Authorized by the client's warrant to generate authentication tags and upload encrypted blocks.
Key Generation Center (KGC): Generates system parameters and identity-derived private keys for system participants.

6. TECHNICAL & SYSTEM REQUIREMENTS

Configuration Parameter	Hardware Requirements	Software Specifications
Processor / CPU	Intel Core i3 / Pentium IV 1.1 GHz or higher	Windows 10 / Linux Ubuntu 20.04 LTS
System Memory (RAM)	256 MB Minimum (4 GB Recommended)	Java Development Kit (JDK 1.8+)
Storage Capacity	20 GB HDD Minimum space	Apache Tomcat 8.5 / Cloud Simulator
Cryptographic Primitives	Bilinear Pairing Support (PBC Library)	SHA-256 / 160-bit Elliptic Curve Groups

7. CONCLUSION

This paper established the novel ID-PUIC paradigm for identity-based proxy data uploading and remote integrity checking in public cloud storage. By leveraging bilinear pairings in identity-based cryptography, the protocol achieves high operational efficiency while eliminating public key certificate management overheads. The framework supports private, delegated, and public integrity audits alongside local proxy recovery and time-bounded access controls. Security analyses confirm robust resistance against unauthorized modification and forgery under standard cryptographic assumptions.

REFERENCES

1. B. Chen and H. Yeh, "Secure proxy signature schemes from the Weil pairing," Journal of Supercomputing, vol. 65, no. 2, pp. 496–506, 2013.
2. H. Guo, Z. Zhang, and J. Zhang, "Proxy re-encryption with unforgeable re-encryption keys," Cryptology and Network Security, LNCS 8813, pp. 20–33, 2014.