International Research Journal of Education and Technology

Peer Reviewed Journal, **ISSN: 2581-7795**

REVOCABLE IDENTITY-BASED BROADCAST PROXY RE-ENCRYPTION FOR SECURE CLOUD DATA SHARING

Mr. A. Abdul Faiz, M.Sc., M.Phil., Associate Professor,

Department of Computer Applications,

Sri Krishna Arts and Science College, Coimbatore – 641008

Gladwin David S, Department of Computer Applications,

Sri Krishna Arts and Science College, Coimbatore – 641008

ABSTRACT

Cloud computing has revolutionized data storage and sharing by providing scalable and on-demand services. However, secure data sharing in semi-trusted cloud environments remains a major challenge. Traditional encryption mechanisms require repetitive encryption for multiple users, increasing computational overhead and key management complexity. Identity-Based Broadcast Proxy Re-Encryption (IB-BPRE) improves efficiency but suffers from dependency on the data owner during user revocation and key renewal processes.

This paper proposes a **Revocable Identity-Based Broadcast Proxy Re-Encryption (RIB-BPRE)** scheme that enables secure broadcast data sharing with efficient and dynamic user revocation. The proposed system eliminates continuous dependency on the data owner during key updates while maintaining strong confidentiality guarantees. The cloud server acts as a semi-trusted proxy that transforms ciphertext without accessing plaintext. Performance evaluation demonstrates improved scalability, reduced computational overhead, and secure access control suitable for real-world cloud applications.

Keywords: Cloud Security, Identity-Based Encryption, Proxy Re-Encryption, Broadcast Encryption, User Revocation, Cryptography.

I. INTRODUCTION

Cloud computing has evolved into a foundational pillar of modern digital infrastructure, enabling organizations and individuals to store, process, and share vast volumes of data over distributed networks. Its elasticity, scalability, and cost-effectiveness have made it indispensable for enterprises, educational institutions, research organizations, and government agencies. However, as sensitive information is increasingly outsourced to third-party cloud servers, concerns regarding data confidentiality, integrity, and controlled access have intensified. Since cloud providers are often considered semi-trusted entities, robust cryptographic mechanisms are essential to prevent unauthorized data exposure.

In traditional public key encryption systems, when a data owner intends to share encrypted data with multiple users, the same file must be encrypted separately for each recipient. This approach results in significant computational overhead and increased communication cost, particularly in environments involving large user groups. Moreover, certificate management and key distribution complexities further burden system administration.

To address these challenges, Identity-Based Encryption (IBE) was introduced as an alternative cryptographic paradigm. In IBE, a user's unique identity—such as an email address—serves directly as the public key, eliminating the need for digital certificates. This significantly simplifies key management and enhances system usability. Building upon IBE, Proxy Re-Encryption (PRE) was developed to allow a semi-trusted proxy, such as a cloud server, to transform ciphertext encrypted for one user into ciphertext decryptable by another user, without revealing the underlying plaintext. PRE enables secure delegation of access rights while maintaining data confidentiality.

Further advancement led to the development of Identity-Based Broadcast Proxy Re-Encryption (IB-BPRE), which combines identity-based cryptography with broadcast encryption principles. IB-BPRE enables a data owner to share encrypted content with multiple recipients simultaneously using a single broadcast re-encryption key. While this approach improves efficiency and scalability, it presents a notable limitation: the data owner must participate in key renewal and user revocation processes. Specifically, updating access control typically requires the owner's private key, thereby creating operational dependency and reducing

flexibility in dynamic cloud environments where users frequently join or leave.

To overcome these limitations, this paper proposes a **Revocable Identity-Based Broadcast Proxy Re-Encryption (RIB-BPRE)** scheme. The proposed approach incorporates an efficient and secure revocation mechanism that allows the cloud proxy to update re-encryption keys and exclude revoked users without requiring repeated involvement from the data owner. By minimizing owner-side workload and maintaining strong confidentiality guarantees, the RIB-BPRE scheme enhances practicality, scalability, and security for modern cloud-based data sharing systems.

II. RELATED WORK

Secure data sharing in cloud environments has been extensively studied over the past two decades, particularly with the rapid adoption of distributed storage systems. Traditional Public Key Infrastructure (PKI)-based encryption mechanisms were initially used to secure outsourced data. In these systems, a data owner encrypts data using the recipient's public key, and only the corresponding private key holder can decrypt it. While secure, this approach becomes inefficient when sharing the same data with multiple users, as it requires multiple encryption operations and complex certificate management.

To simplify key management, Shamir introduced the concept of **Identity-Based Encryption (IBE)**, where a user's identity (such as an email address) functions as the public key. Later, Boneh and Franklin provided a practical pairing-based IBE construction, demonstrating feasibility in real-world applications. IBE eliminates certificate distribution overhead and simplifies authentication. However, it does not inherently support flexible delegation or efficient multi-user sharing.

To address delegation challenges, Blaze, Bleumer, and Strauss introduced **Proxy Re-Encryption (PRE)**. PRE allows a semi-trusted proxy to transform ciphertext encrypted for one user into ciphertext decryptable by another user without revealing the plaintext. Ateniese et al. later improved PRE schemes with stronger security definitions and unidirectional re-encryption. Although PRE enables flexible access delegation, early constructions were limited to one-to-one sharing and lacked broadcast capabilities.

Broadcast Encryption (BE) schemes were developed to efficiently share encrypted data with multiple recipients simultaneously. In BE, a sender encrypts a message once, and only a

selected group of users can decrypt it. However, traditional BE systems often rely on complex key distribution mechanisms and may not integrate naturally with identity-based frameworks.

To combine the advantages of IBE, PRE, and broadcast encryption, researchers proposed **Identity-Based Broadcast Proxy Re-Encryption (IB-BPRE)** schemes. IB-BPRE allows a data owner to encrypt data once and generate a broadcast re-encryption key that enables the cloud proxy to convert ciphertext for multiple users. This significantly reduces computational overhead compared to encrypting separately for each recipient. Despite these improvements, IB-BPRE schemes typically require the data owner's private key during key renewal and revocation processes. This dependency creates operational inefficiencies and reduces practicality in dynamic cloud environments.

Recent research has focused on revocable identity-based encryption mechanisms to support dynamic user management. Revocable IBE schemes introduce time-based keys or revocation lists to exclude users without regenerating the entire system. However, integrating efficient revocation directly into broadcast proxy re-encryption frameworks remains a complex challenge.

The proposed **Revocable Identity-Based Broadcast Proxy Re-Encryption (RIB-BPRE)** scheme addresses this research gap by enabling dynamic and efficient user revocation without requiring repeated private key involvement from the data owner. By shifting key update responsibilities to the cloud proxy while preserving strong security guarantees, the proposed model enhances scalability, flexibility, and real-world applicability compared to existing IB-BPRE systems.

III. SYSTEM ARCHITECTURE

The proposed Revocable Identity-Based Broadcast Proxy Re-Encryption (RIB-BPRE) system is designed to provide secure, scalable, and efficient data sharing in a cloud computing environment. The architecture follows a modular and distributed design model to ensure confidentiality, controlled access, and dynamic user management. The system consists of three primary entities: the **Trusted Authority (TA)**, the **Cloud Server (Proxy)**, and the **End Users**, which include the Data Owner and Delegates.

A. TRUSTED AUTHORITY (TA)

The Trusted Authority is responsible for initializing the cryptographic environment. During the setup phase, the TA generates global system

parameters and a master secret key required for identity-based encryption. Using this master secret key, the TA derives private keys for registered users based on their unique identities, such as email addresses. The TA securely distributes these private keys to users through protected communication channels.

The TA does not participate in routine data sharing operations after initialization, which reduces central dependency and enhances scalability.

B. CLOUD SERVER (PROXY)

The Cloud Server acts as a semi-trusted proxy. It stores encrypted files uploaded by data owners and performs re-encryption operations when sharing is requested. Importantly, the cloud server never gains access to plaintext data or private keys.

When a broadcast re-encryption key is generated by the data owner, the cloud server uses it to transform the stored ciphertext into a new ciphertext that authorized delegates can decrypt. In the proposed RIB-BPRE system, the cloud server also plays a key role in enforcing user revocation by updating re-encryption keys according to the revocation list.

C. END USERS

The end users are categorized into:

1. **Data Owner** – Encrypts and uploads data to the cloud and defines the list of authorized users.
2. **Delegates (Authorized Users)** – Decrypt shared data using their identity-based private keys.

The data owner performs encryption locally before uploading data to the cloud, ensuring end-to-end confidentiality. Delegates only gain access after the proxy completes re-encryption.

ARCHITECTURAL PHASES

The architecture operates through the following structured phases:

1. **System Setup Phase**
   The Trusted Authority generates system parameters and master secret keys.
2. **User Registration and Key Generation Phase**
   Users register with their identities, and private keys are generated accordingly.
3. **Data Encryption Phase**
   The data owner encrypts the file using identity-based encryption and uploads the ciphertext to the cloud.
4. **Broadcast Re-Encryption Phase**
   The data owner generates a broadcast re-encryption key for a

selected group. The proxy transforms the ciphertext without accessing plaintext.

5. **Revocation Phase**
   When a user is revoked, the system updates the re-encryption key to exclude that user without requiring repeated private key usage from the owner.

6. **Decryption Phase**
   Authorized users decrypt the transformed ciphertext using their private keys.

ARCHITECTURAL ADVANTAGES

The proposed architecture provides several benefits:

- Reduced computational overhead for the data owner
- Elimination of certificate management complexity
- Secure multi-user sharing with single encryption
- Efficient dynamic user revocation
- Confidentiality preservation in semi-trusted cloud environments
- Scalability for large user groups

Overall, the RIB-BPRE system architecture ensures that security, flexibility, and performance are maintained even in dynamic and large-scale cloud environments.

IV. SYSTEM WORKFLOW

The system workflow of the proposed Revocable Identity-Based Broadcast Proxy Re-Encryption (RIB-BPRE) scheme defines the sequence of operations involved in secure cloud data sharing. The workflow ensures confidentiality, controlled delegation, and efficient revocation while minimizing the computational burden on the data owner. Each phase is executed systematically to maintain strong security guarantees.

Step 1: System Initialization

The workflow begins with the Trusted Authority (TA) executing the setup algorithm. The TA generates global public parameters and a master secret key. The public parameters are made available to all users in the system, while the master secret key is securely retained by the TA. This initialization establishes the cryptographic foundation of the system.

Step 2: User Registration and Private Key Generation

Users register with the system using a unique identity, such as an email address. Based on this identity, the TA generates a corresponding private key using the master secret key. The private key is securely transmitted to the user. This identity-based approach eliminates the need for digital certificates and simplifies key management.

Step 3: Data Encryption and Upload

When a data owner intends to store data in the cloud, the file is first encrypted locally using identity-based encryption. The encryption ensures that the cloud server cannot access the plaintext content. The encrypted file (ciphertext) is then uploaded to the cloud storage system.

Step 4: Broadcast Sharing

If the data owner wishes to share the encrypted file with multiple users, a broadcast re-encryption key is generated for the selected group of authorized users. This single re-encryption key enables efficient multi-user sharing without re-encrypting the file separately for each recipient.

The re-encryption key is sent to the cloud server, which transforms the stored ciphertext into a new ciphertext that can be decrypted by the selected delegates. The proxy performs this transformation without accessing the plaintext or private keys.

Step 5: Data Decryption by Delegates

Authorized users download the transformed ciphertext from the cloud server. Using their identity-based private keys, they decrypt the file and access the original content. If a user is not included in the broadcast group, decryption will fail.

Step 6: User Revocation

In dynamic environments, users may need to be removed from the authorized group. When revocation is required, the data owner specifies the user(s) to be revoked. The system updates the revocation list and generates an updated re-encryption key that excludes revoked users.

The cloud server applies the updated re-encryption key to ensure that revoked users cannot decrypt future or updated ciphertext. Importantly, this process does not require the data owner's private key for every update, thereby reducing operational dependency and improving system efficiency.

SECURITY PROPERTIES ENSURED BY THE WORKFLOW

The workflow guarantees the following properties:

- **Confidentiality:** Cloud server cannot access plaintext data.
- **Forward Security:** Revoked users cannot access future shared data.
- **Backward Security:** Revoked users cannot use previously issued credentials to access updated ciphertext.
- **Scalability:** Efficient broadcast sharing reduces computational cost.
- **Reduced Owner Dependency:** Revocation does not require continuous owner participation.

The structured workflow ensures secure, flexible, and efficient cloud-based data sharing suitable for collaborative and dynamic environments.

V. METHODOLOGY

The methodology consists of six phases:

1. SETUP PHASE

Global system parameters and master secret key are generated.

2. KEY GENERATION PHASE

Private keys are generated based on user identities.

3. ENCRYPTION PHASE

Data owner encrypts file before cloud upload.

4. BROADCAST RE-ENCRYPTION PHASE

A single broadcast re-encryption key is generated for a group.

5. REVOCATION PHASE

Revoked users are excluded without requiring full re-encryption.

6. DECRYPTION PHASE

Authorized users decrypt transformed ciphertext.

The methodology ensures confidentiality, scalability, and dynamic access control.

VI. IMPLEMENTATION DETAILS

The system is implemented using:

- Programming Language: Java / Python
- Cryptographic Libraries: Pairing-Based Cryptography (PBC/JPBC)
- Database: MySQL / PostgreSQL
- Secure Communication: HTTPS (SSL/TLS)

Modules implemented:

- System Setup Module
- User Registration Module
- Data Encryption Module
- Broadcast Re-Encryption Module
- Revocation Module
- Decryption Module

The web interface provides features including encryption, delegate management, revocation control, and analytics visualization

VII. PERFORMANCE EVALUATION

Performance metrics evaluated:

- Encryption Time
- Re-Encryption Time
- Decryption Time
- Revocation Update Time
- CPU and Memory Usage

Results show:

- Efficient broadcast sharing
- Reduced computational burden on data owner
- Stable performance under concurrent access
- Scalable handling of increasing users

The revocation mechanism introduces minimal overhead compared to full re-encryption approaches.

VIII. COMPARATIVE ANALYSIS

Feature	**Traditional Encryption**	**IB-BPRE**	**Proposed RIB-BPRE**
Multi-user Sharing	Inefficient	Efficient	Efficient
Owner Dependency	High	High	Low
User Revocation	Complex	Limited	Efficient
Scalability	Moderate	High	Very High
Cloud Confidentiality	Yes	Yes	Yes

RIB-BPRE provides superior flexibility and reduced owner dependency.

IX. DISCUSSION

The proposed system significantly improves cloud-based data sharing by reducing owner-side workload and introducing dynamic revocation. The semi-trusted proxy model ensures confidentiality while improving efficiency.

However, pairing-based cryptography introduces computational cost. Optimization techniques and hardware acceleration can further improve performance.

X. FUTURE WORK

Future enhancements include:

- Integration of Post-Quantum Cryptography
- Blockchain-based revocation transparency
- AI-based intrusion detection
- Parallelized re-encryption mechanisms
- Edge-computing assisted encryption
- Mobile application interface

These improvements can further strengthen security and scalability.

XI. CONCLUSION

This paper presented a **Revocable Identity-Based Broadcast Proxy Re-Encryption (RIB-BPRE)** scheme for secure cloud data sharing. The system enables efficient broadcast sharing with dynamic revocation while minimizing dependency on the data owner.

The proposed architecture ensures confidentiality, scalability, and usability in real-world cloud environments. Performance evaluation demonstrates reduced computational overhead and secure access enforcement.

XII. REFERENCES

[1] W. Stallings, *Cryptography and Network Security*, 7th ed., Pearson, 2017.

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed., CRC Press, 2014.

[3] A. Kahate, *Cryptography and Network Security*, McGraw-Hill, 2013.

[4] B. A. Forouzan, *Cryptography and Network Security*, McGraw-Hill, 2007.

[5] IEEE Xplore Digital Library, Research on Proxy Re-Encryption and Cloud Security.