IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11747

# IDENTITY BASED PROXY ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

**HARSHITHGOWDA[1], Asst Prof RAJESHWARI N[2]**

Student, Department of MCA, Bangalore Institute of Technology, Karnataka, India[1]

Assistant Professor, Department of MCA, Bangalore Institute of Technology, Karnataka, India[2]

**Abstract:** The rapid proliferation of cloud-based services has transformed data storage, management, and sharing methods. Cloud computing offers significant advantages such as scalability, cost efficiency, and accessibility, making it a preferred choice for businesses and individuals. However, these benefits come with critical challenges, particularly in ensuring the security and accessibility of data stored in public cloud environments. As organizations increasingly rely on cloud services to manage their data, the need for robust data security mechanisms has become paramount.

The project introduces a novel approach to enhancing data security and accessibility in public cloud environments. It addresses the challenge of efficiently delegating decryption rights for subsets of encrypted data without requiring large decryption key sizes. The proposed system leverages a keyaggregate cryptosystem, termed DATA SHARING which integrates Triple DES (Data Encryption Standard) as the underlying encryption algorithm. The system aims to provide a comprehensive solution that combines robust encryption standards with efficient key management, ensuring data confidentiality and integrity while facilitating secure data sharing and access control.

## I. INTRODUCTION

In the "DATA SHARING" system, data security is achieved through the use of Triple DES (Data Encryption Standard), a symmetric-key encryption algorithm renowned for its robust security features. Triple DES applies the DES cipher algorithm three times to each data block, significantly enhancing the security compared to the original DES algorithm, which had become vulnerable to brute-force attacks due to its shorter key length. Utilizing three 56-bit keys, Triple DES offers an overall key length of 168 bits, ensuring stronger protection of data confidentiality and integrity. This choice is motivated by Triple DES's widespread acceptance and proven security in various applications.

In our system, each piece of encrypted data, or ciphertext, is associated with a unique identifier or class. This categorization facilitates granular control over decryption permissions, enabling data owners to efficiently delegate decryption rights. The system employs a master-secret key, held by the data owner, to generate compact aggregate keys. These aggregate keys possess the decryption capabilities required to access any subset of ciphertext classes associated with them.

A primary challenge in cloud data security is the efficient management of decryption rights for specific subsets of encrypted data. Traditional methods often necessitate unique decryption keys for each user or data subset, which can lead to increased complexity and larger key sizes. This complexity becomes particularly problematic in large-scale cloud environments where multiple users need access to various subsets of data.

To address this challenge, the "DATA SHARING" system introduces a key-aggregate cryptosystem. This system enables data owners to generate compact aggregate keys that can decrypt any subset of ciphertext classes associated with them. By reducing the number of keys that need to be managed, the keyaggregate cryptosystem simplifies key management and enhances both the security and scalability of the system.

Through the use of Triple DES and innovative keyaggregate techniques, the "DATA SHARING" system provides a high level of data protection while maintaining compatibility with existing security standards and protocols, ultimately facilitating more efficient and secure data sharing in cloud environments.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11747

## II. IMPLEMENTATION

The proposed framework leverages identity-based encryption (IBE) combined with proxy-oriented techniques to enhance security and integrity for data in public clouds. It includes several critical components: IBE for secure data uploads, proxy reencryption for secure data management, and remote data integrity verification mechanisms. Below, we outline each element of the methodology

### 1 Identity-Based Encryption for Secure Data Uploading

#### 1.1 Overview of IBE:

Identity-based encryption allows data to be encrypted using an identity (like an email address or user ID) as the key, which simplifies key management and the encryption/decryption process.

#### 1.2 Encryption Process:

- **Key Generation:** A trusted authority (TA) generates a master secret key and a master public key, issuing private keys to users based on their identities.
- **Data Encryption:** Users encrypt data with the master public key using their identity, ensuring that only those with the corresponding private key can decrypt it.

#### 1.3 Security Considerations:

- Only authorized users with the correct private key can decrypt the data.
- Utilizing elliptic curve cryptography enhances the security and efficiency of the IBE scheme.

### 2. Proxy-Oriented Data Management

#### 2.1 Overview of Proxy Re-Encryption:

Proxy re-encryption allows a proxy server to reencrypt data from one user to another without decrypting it, facilitating secure data sharing and management among multiple parties.

#### 2.2 Re-Encryption Process:

- **Re-Encryption Key Generation:** The data owner creates a re-encryption key enabling the proxy to transform ciphertext from the owner's scheme to the recipient's scheme.
- **Data Management:** The proxy uses the reencryption key to convert ciphertext, ensuring the data remains encrypted during the transformation process.

#### 2.3 Security Considerations:

- Proxy re-encryption maintains data confidentiality by preventing the proxy from accessing plaintext data.
- Secure key management and encryption schemes ensure the integrity and authenticity of re-encrypted data.

### 3. Remote Data Integrity Checking

#### 3.1 Overview of Remote Data Integrity Checking:

This mechanism allows users to verify the integrity of cloud-stored data without directly accessing it, using cryptographic proofs and challenge-response protocols.

#### 3.2 Integrity Checking Process:

- **Proof Generation:** The cloud service provider generates proofs of data integrity (e.g., hash values or Merkle trees) upon data upload or modification.
- **Verification Protocol:** Users or third parties request and verify these proofs to ensure data integrity by comparing provided proofs with expected values.

#### 3.3 Security Considerations:

- The mechanism detects any data tampering or corruption.
- Cryptographic hash functions and secure communication protocols enhance the reliability of the integrity checking process.

### 4. Integration and Implementation

#### 4.1 System Integration:

- The framework integrates IBE, proxy re-encryption, and remote integrity checking into a unified system.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11747

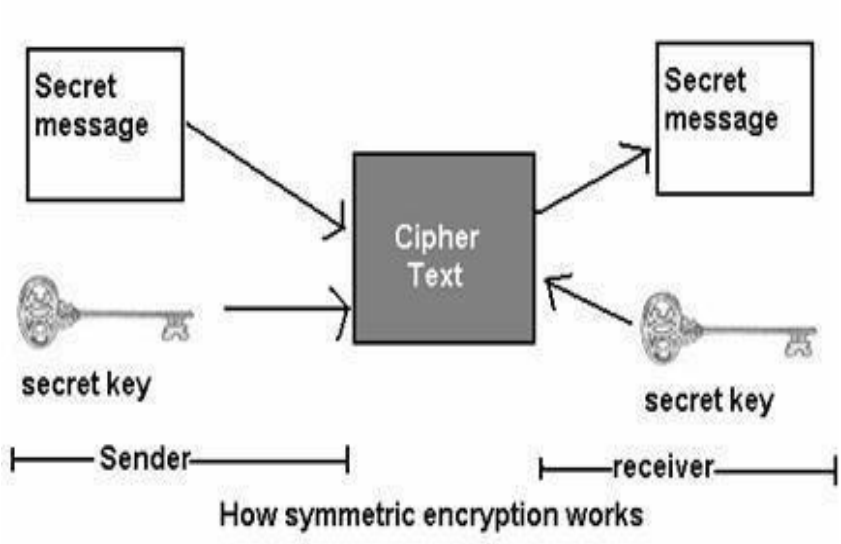
- It is designed to seamlessly work with existing cloud storage solutions, enhancing security and integrity features.

**4.2 Implementation Details:**

- The methodology is implemented using a combination of cryptographic libraries and cloud storage APIs.
- Performance benchmarks and security evaluations assess the framework's efficiency and robustness.

**4.3 Evaluation Metrics:**

- **Security:** Assessing the encryption and integrity checking mechanisms' robustness against various attack vectors.
- **Performance:** Measuring encryption/decryption times, re-encryption efficiency, and integrity checking response times.



How symmetric encryption works

## III. CONCLUSION

The project presented a groundbreaking approach to enhance data security and manageability within public cloud environments by integrating Triple DES encryption with a novel keyaggregate cryptosystem known as "DATA SHARING." This comprehensive solution addresses several critical challenges associated with data protection, encryption, and access control, and represents a significant advancement over traditional methods. The use of Triple DES (Data Encryption Standard) as the foundational encryption algorithm ensures a robust level of security for sensitive data. Triple DES, an extension of the original DES algorithm, employs three rounds of encryption with a key size of 168 bits, making it substantially more secure than its predecessor.

This strong encryption standard effectively safeguards data against unauthorized access and potential breaches, which is crucial for protecting sensitive information in cloud environments.

One of the primary innovations of the project is the development of the "DATA SHARING" cryptosystem, which provides a novel method for managing decryption rights. Traditional encryption systems often require individual keys for each subset of data, leading to a proliferation of keys and increased complexity in key management. In contrast, the "DATA SHARING" system employs a mastersecret key to generate compact aggregate keys. These aggregate keys enable users to access specific subsets of encrypted data without the need for multiple individual decryption keys. This streamlined approach significantly reduces the complexity of key management and enhances operational efficiency.

The successful integration of Triple DES encryption with the "DATA SHARING" cryptosystem represents a significant step forward in the field of data security

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11747

## REFERENCES

[1]. Buckley, P. J., Clegg, J., Wang, C., & Cross, A. R. (2002). FDI, regional differences and economic growth: Panel data evidence from China. Transnational Corporations, 11(1), 1–28.
[2]. Emmanuel, N. (2013). Analysis of Indian FDI Inflows Using an Augmented Gravity Model. International Economics and Economic Policy, 10(3), 485-503.
[3]. Contractor, F. J. (2021). The world economy through the lens of international business. Journal of International Business Studies, 52, 1461–1476.
[4]. Casi, L., & Resmini, L. (2010). Evidence on the determinants of Foreign Direct Investment: The case of EU regions. Eastern Journal of European Studies, 1(2), 93-118.
[5]. Kumar, N., & Pradhan, J. P. (2002). FDI, Externalities and Economic Growth in Developing Countries: Some Empirical Explorations and Implications for WTO Negotiations on Investment. RIS Discussion Papers.
[6]. Buller, P. F., & McEvoy, G. M. (1999). Creating and sustaining ethical capability in the multinational corporation. Journal of World Business, 34(4), 326–343.
[7]. Caceres, L. R., & Caceres, S. A. (2015). Financing investment in sub-Saharan Africa: Savings, human development, or institutions, The Journal of Developing Areas, 49(4), 1–23.
[8]. Campbell, J. L., & Lindberg, L. N. (1990). Property rights and the organization of economic activity by the state. American Sociological Review, 55(5), 634–647.
[9]. Chintrakarn, P., Herzer, D., & Nunnenkamp, P. (2012). FDI and income inequality: Evidence from a panel of US states. Economic Inquiry, 50(3), 788–801.
[10]. Ethier, W. J. (1986). The Multinational Firm. Quarterly Journal of Economics, 101(4), 805–833.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License