**ATTRIBUTE-BASED PROXY RE-ENCRYPTION WITH DIRECT REVOCATION MECHANISM FOR SECURE DATA SHARING IN CLOUD**

**ABSTRACT**

In the evolving landscape of cloud computing and data security, the protection of sensitive information is a critical concern. Traditional encryption systems often face challenges related to scalability, access control, and secure key management in decentralized environments. This paper introduces an innovative approach for **key encryption** by leveraging **public and secret key pairs**, alongside **hash algorithms** for data integrity and security. The proposed system utilizes **blockchain technology** for decentralized key management, providing tamper-proof storage and verification of encryption keys and associated hashes.

In the proposed solution, a **public key** is used to encrypt sensitive data, ensuring that only authorized parties with the corresponding **secret key** can decrypt the information. Additionally, a **hash value** is generated from the encrypted data using a secure hashing algorithm (e.g., SHA-256). This hash serves as a digital fingerprint of the encrypted data, ensuring its integrity and authenticity. Any unauthorized modifications to the data will result in a mismatch between the hash values, signaling potential tampering.

The integration of **blockchain** technology enhances the system by offering a transparent, decentralized, and immutable ledger for storing the **public keys** and **hash values**. Blockchain’s tamper-resistant nature ensures that key management and data verification are secure and auditable. The system also allows for efficient revocation and management of keys without requiring re-encryption, addressing scalability concerns in dynamic environments.

This approach provides a robust solution for secure **data sharing**, **key management**, and **data integrity** verification in cloud environments, making it ideal for applications in sectors such as healthcare, finance, and government. By combining **encryption**, **hashing**, and **blockchain**, the system ensures confidentiality, integrity, and transparency in the management of cryptographic keys and sensitive data.

**Keywords: Public Key, Secret Key, Encryption, Hash Algorithm, Blockchain, Data Integrity, Key Management, Cloud Security, Cryptography, Secure Data Sharing**

**INTRODUCTION**

The rapid adoption of cloud computing has revolutionized the way organizations store and manage sensitive data. As more businesses and individuals turn to the cloud for convenience and scalability, the importance of securing data and ensuring privacy has never been more critical. Cloud storage systems, while offering numerous benefits, introduce unique challenges in terms of **data security**, **access control**, and **key management**. Traditional encryption methods often struggle to address these challenges, especially in decentralized and dynamic environments.

**Encryption** serves as the backbone of data security, ensuring that unauthorized users cannot access sensitive information. However, conventional systems often rely on centralized management of encryption keys, which poses risks such as key leakage, unauthorized access, and single points of failure. To mitigate these issues, the use of **public-key cryptography** has become a common practice, where a **public key** is used for encryption, and only the holder of the **secret key** can decrypt the data. However, as organizations grow and share encrypted data across multiple parties, managing these keys becomes increasingly complex and prone to errors.

Additionally, the issue of **data integrity** arises. Once data is encrypted, ensuring that it remains unaltered during transmission or storage is essential. **Hashing algorithms**, such as SHA-256, have been used to generate unique, fixed-length representations of data, which can be used to verify its integrity. Any tampering with the data will result in a mismatch between the hash values, alerting users to potential security breaches.

To address these challenges, we propose an integrated solution that combines **public-key encryption**, **hashing algorithms**, and **blockchain technology**. The use of **blockchain** enhances key management and ensures that both the **public keys** and **hash values** of encrypted data are securely stored and auditable. Blockchain's decentralized and immutable nature provides an additional layer of trust and transparency in data sharing processes.

This framework introduces an advanced **Attribute-Based Proxy Re-Encryption (ABPRE)** system with a **Direct Revocation Mechanism**, allowing for more flexible and dynamic access control in cloud environments. The solution ensures that access rights to encrypted data can be easily granted, revoked, and audited, without requiring re-encryption, making it highly efficient and scalable.

This paper explores the advantages and potential applications of this integrated solution in enhancing **data privacy**, **security**, and **scalability** for cloud-based systems. By leveraging encryption, hashing, and blockchain, we aim to provide a robust, secure, and transparent mechanism for managing cryptographic keys and ensuring the integrity of sensitive data in cloud environments.