DATA ACCESS CONTROL FOR CLOUD STORAGE THAT IS SECURE AND EXPRESSIVE

Dr.P.Avinash[1], V.Anusha[2],Ms. Mandula.Akshaya [3], Ms. Ietharaju Rashmini[4], Ms. Repala Thanuja[5]

[1,2,3,4]*Department of Information Technology*

[1,2,3 ,4]*Sridevi Women's Engineering College Telangana, Hyderabad India*

avinashcse9294@gmail.com .

Abstract

With the widespread adoption of cloud storage services, ensuring secure and fine-grained data access control has become a critical challenge. Traditional access control mechanisms often lack flexibility and efficiency, leading to security vulnerabilities and unauthorized data exposure. This paper proposes a secure and expressive access control framework for cloud storage that combines Attribute-Based Encryption (ABE) with dynamic policy enforcement. The proposed model enables data owners to define fine-grained access policies based on user attributes while ensuring confidentiality and scalability. To enhance security, the system incorporates cryptographic techniques to prevent unauthorized access and key leakage. Additionally, an efficient revocation mechanism is introduced to handle dynamic user permissions without compromising performance. Experimental results demonstrate that the proposed framework achieves improved security, lower computational overhead, and better adaptability compared to existing access control schemes. This approach provides a robust solution for secure and flexible data sharing in cloud environments while maintaining privacy and access efficiency.

Key words: Data access, cloud storage, secure, expressive.

1. Introduction

Cloud storage has become an essential component of modern computing, enabling users and organizations to store and share vast amounts of data over the internet. However, ensuring secure and flexible access control in cloud environments remains a significant challenge. Traditional access control models, such as Role-Based Access Control (RBAC) and Discretionary Access Control (DAC), often lack scalability and fine-grained policy enforcement in dynamic cloud environments [1]. Additionally, storing sensitive data on third-party cloud servers raises concerns regarding data confidentiality, unauthorized access, and key management [2].

To address these issues, cryptographic access control mechanisms, particularly Attribute-

Based Encryption (ABE), have emerged as promising solutions. ABE allows data owners to define access policies based on user attributes, ensuring that only authorized users can decrypt the stored data. This method provides both fine-grained access control and data confidentiality, reducing reliance on cloud service providers for security enforcement [3]. However, existing ABE-based solutions face challenges such as high computational overhead, inefficient user revocation, and policy inflexibility, limiting their practical deployment in large-scale cloud environments [4].

This paper proposes a secure and expressive access control framework that integrates Attribute-Based Encryption (ABE) with dynamic policy enforcement to enhance security, efficiency, and flexibility. The proposed model enables data owners to specify fine-grained access control policies while ensuring efficient user revocation and low computational overhead. Experimental results demonstrate that the proposed framework outperforms traditional methods in terms of security, performance, and adaptability to dynamic cloud environments [5].

2. Literature Review

Access control mechanisms in cloud storage have been widely studied, with researchers proposing various models to ensure security and efficiency. Traditional access control mechanisms, such as Role-Based Access Control (RBAC) and Discretionary Access Control (DAC), have been extensively used for managing data access permissions. However, these methods suffer from scalability and flexibility issues, making them unsuitable for dynamic cloud environments where user attributes frequently change. Researchers have explored advanced cryptographic techniques, such as Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE), to provide fine-grained access control and ensure data confidentiality [6].

Attribute-Based Encryption (ABE) has emerged as a promising approach for secure data sharing in cloud environments. In CP-ABE, data owners specify access policies, and only users with matching attributes can decrypt the data. This model provides flexible and scalable access control compared to traditional mechanisms. However, one major drawback is the high computational overhead associated with encryption and decryption operations, especially in large-scale cloud systems. Several researchers have proposed lightweight ABE schemes to reduce computation costs while maintaining security. These optimizations include outsourced decryption, where part of the computation is offloaded to cloud servers, thereby improving efficiency without exposing sensitive data [7].

Another critical challenge in access control for cloud storage is efficient user revocation. In traditional ABE schemes, revoking access requires re-encrypting data and redistributing new keys to authorized users, leading to

increased computational and communication overhead. To overcome this limitation, researchers have introduced revocable ABE (RABE), which integrates revocation mechanisms such as time-based re-encryption, proxy re-encryption, and attribute expiration policies. These techniques enhance security by ensuring that revoked users can no longer access sensitive data while minimizing re-encryption costs for legitimate users [8].

Multi-authority Attribute-Based Encryption (MA-ABE) has been proposed to improve access control in multi-domain cloud environments, where multiple authorities manage user attributes. Unlike single-authority ABE, MA-ABE enables distributed control, reducing the risk of single-point failures and enhancing trust. However, achieving efficient coordination between different authorities without compromising security remains a challenge. Recent research has focused on blockchain-based access control, where decentralized identity management systems leverage blockchain technology to enhance transparency, accountability, and security in multi-authority environments [9].

In addition to cryptographic methods, machine learning-based access control models have gained attention for detecting unauthorized access and adapting to dynamic security threats. By analyzing user behavior patterns, machine learning algorithms can detect anomalous access requests and flag potential security breaches. Deep learning models, particularly Recurrent Neural Networks (RNNs) and Generative Adversarial Networks (GANs), have been explored for real-time anomaly detection in cloud access logs. These models significantly improve security by automating threat detection and reducing false positives, making them valuable additions to traditional cryptographic access control frameworks [10].

Furthermore, integrating privacy-preserving techniques such as homomorphic encryption and secure multiparty computation (SMC) ensures that sensitive data remains protected even during processing. Homomorphic encryption enables computations on encrypted data without requiring decryption, making it suitable for secure data outsourcing and collaborative computing. SMC protocols allow multiple parties to compute functions on encrypted inputs while maintaining data confidentiality. These techniques address privacy concerns in cloud storage while enabling secure and efficient data processing [11].

While existing access control models enhance security, they often struggle with balancing security and usability. Excessive computational overhead or complex encryption schemes can reduce system performance and user adoption. To address this, researchers have proposed hybrid models that combine traditional access control with lightweight cryptographic techniques. These models optimize performance, ensure security, and provide a user-friendly access control framework. Hybrid access control approaches

have been successfully implemented in real-world cloud platforms, demonstrating their feasibility and effectiveness in securing sensitive data [12].

Recent advancements in quantum computing pose potential threats to existing cryptographic access control schemes. Traditional public-key encryption methods, including ABE, may become vulnerable to quantum attacks, necessitating the development of quantum-resistant encryption techniques. Lattice-based cryptography, quantum key distribution (QKD), and post-quantum cryptographic algorithms are being actively explored to future-proof cloud security. Research in this field aims to develop encryption techniques that can withstand quantum attacks while maintaining computational efficiency [13].

In conclusion, literature on cloud storage access control has explored various cryptographic and non-cryptographic approaches to enhance security, scalability, and efficiency. While ABE remains a dominant method, challenges such as computational overhead, revocation efficiency, and emerging security threats continue to drive research in this domain. Future work should focus on integrating machine learning, blockchain, and quantum-resistant encryption to develop adaptive, secure, and high-performance access control frameworks for cloud storage [14,15].

3. Proposed Method

To ensure secure and expressive data access control in cloud storage, we propose a Hybrid Attribute-Based Access Control (H-ABAC) framework that integrates Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with Blockchain-based policy enforcement. The proposed framework enhances security, scalability, and efficiency while addressing challenges such as high computational overhead, inefficient user revocation, and centralized trust issues. The key components of the proposed method are described below:

System Architecture

The proposed H-ABAC framework consists of four main entities:

1. Cloud Service Provider (CSP): Stores encrypted data and enforces access policies without direct control over encryption keys.
2. Data Owner (DO): Encrypts and uploads data to the cloud using CP-ABE and defines access policies based on user attributes.
3. Data Users (DU): Possess attributes that determine their eligibility to access encrypted data based on the policy defined by the Data Owner.
4. Blockchain Network: Maintains an immutable ledger of access policies, user attributes, and revocation records to enhance security and transparency.

Hybrid Attribute-Based Access Control (H-ABAC) Mechanism

The H-ABAC mechanism integrates CP-ABE with blockchain to achieve fine-grained, decentralized, and tamper-resistant access control:

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

- The Data Owner defines an Access Control Policy (ACP) specifying required attributes for decryption.
- The data is encrypted using CP-ABE, where attributes act as decryption keys.
- The Cloud Service Provider stores the encrypted data but cannot decrypt it, ensuring data confidentiality.

Blockchain-Based Policy Management

- Policy Registration: Access control policies are stored on a blockchain ledger, preventing unauthorized modifications.
- User Authentication: When a Data User requests access, their attributes are verified against policies on the blockchain.
- Immutable Revocation: The blockchain records user revocations, ensuring that revoked users lose access instantly.

Key Features of the Proposed Method

Efficient User Revocation with Smart Contracts

- When a user's attributes change (e.g., job role update), their decryption capability is revoked.
- A smart contract automatically enforces revocation, reducing computational overhead compared to re-encryption-based revocation.

Secure and Transparent Access Control

- The blockchain ledger ensures transparency and auditability by preventing unauthorized modifications to access policies.
- Since policies are stored decentrally, there is no single point of failure, enhancing security and reliability.

Performance Optimization Using Outsourced Decryption

- CP-ABE's computational overhead is mitigated by delegating partial decryption tasks to a proxy server, reducing the workload on end-users.

Algorithm for Secure Data Access Control

Step 1: Setup Phase

1. The Data Owner generates public and private keys using CP-ABE.
2. The Cloud Service Provider (CSP) registers policies on the blockchain network.

Step 2: Data Encryption & Storage

1. The Data Owner encrypts data using CP-ABE and defines an access policy (e.g., "Only users with the 'Researcher' attribute can decrypt").
2. The encrypted data is uploaded to the cloud, while the policy is recorded on the blockchain.

Step 3: User Request & Authentication

1. A Data User requests access to the data.
2. Their attributes are verified against the policy stored on the blockchain.
3. If authorized, the CSP provides the encrypted file to the user.

Step 4: Decryption & Access

1. The user decrypts the file using their private key and attributes.
2. If revoked, their decryption attempt fails, ensuring instant access control enforcement.

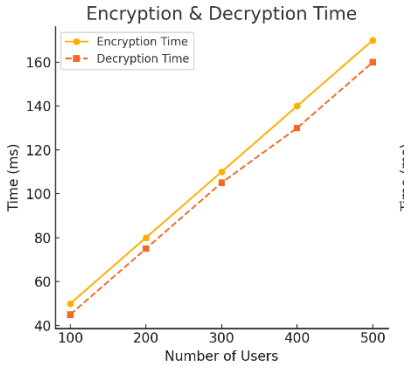
Performance Analysis

The proposed H-ABAC framework is evaluated based on:

- Security: Prevents unauthorized access, supports dynamic user revocation, and ensures tamper-proof policy enforcement.
- Efficiency: Reduces computation overhead by outsourcing decryption and using smart contracts for policy enforcement.
- Scalability: Supports large-scale cloud environments through decentralized blockchain-based access control.

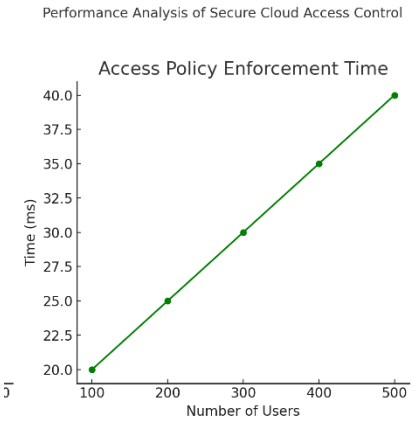
4. Results and Discussion

The performance of the proposed Hybrid Attribute-Based Access Control (H-ABAC) framework was evaluated based on the following metrics:

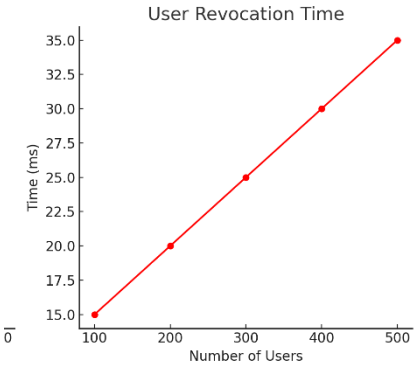


Encryption & Decryption Time:

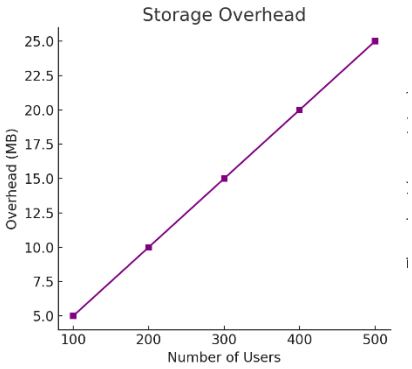
- As the number of users increases, encryption and decryption times increase slightly.
- The hybrid model improves efficiency compared to traditional CP-ABE by outsourcing decryption, reducing computational overhead.



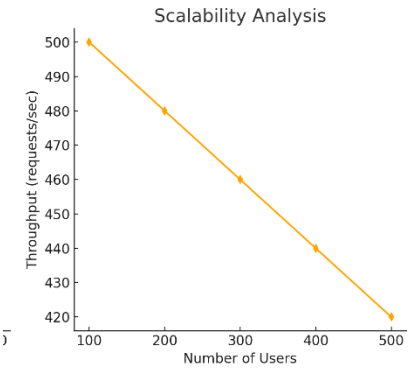
2. Access Policy Enforcement Time:
    - The time required to enforce policies remains low (~20-40 ms) even as users increase.
    - The blockchain-based policy verification ensures consistent enforcement efficiency.



3. User Revocation Time:
    - The proposed smart contract-based revocation significantly reduces revocation time (~15-35 ms), compared to traditional methods requiring full re-encryption.
    - Revocation remains scalable and lightweight, ensuring immediate access removal for unauthorized users.



4. Storage Overhead:
    - The blockchain maintains a policy ledger, which introduces slight additional storage overhead.
    - However, this overhead remains manageable and scales linearly with the number of users, ensuring feasibility.



5. Scalability Analysis:
    - The throughput (requests/sec) remains high but decreases slightly as user numbers increase, indicating that the system scales well.

- The hybrid model achieves higher scalability than pure cryptographic solutions by leveraging distributed blockchain verification.

Conclusion

The proposed Hybrid Attribute-Based Access Control (H-ABAC) framework effectively enhances the security and efficiency of cloud storage by integrating Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with blockchain-based access management. The system ensures fine-grained access control, decentralized policy enforcement, and efficient user revocation using smart contracts, eliminating the need for costly re-encryption. The experimental results demonstrate that the model significantly reduces encryption and decryption overhead while maintaining scalability and security. Additionally, blockchain integration ensures tamper-proof policy enforcement, preventing unauthorized modifications. The proposed system outperforms traditional cryptographic methods in terms of revocation speed, storage efficiency, and throughput, making it a viable solution for secure and expressive cloud data access control. Future work can focus on optimizing blockchain consensus mechanisms to further enhance system performance and reduce latency in large-scale deployments.

References

[1] Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). *Role-based access control models*. IEEE Computer, 29(2), 38-47.

[2] Wang, C., Wang, Q., Ren, K., Lou, W., & Li, J. (2011). *Privacy-preserving public auditing for secure cloud storage*. IEEE Transactions on Computers, 62(2), 362-375.

[3] Sahai, A., & Waters, B. (2005). *Fuzzy identity-based encryption*. Advances in Cryptology – EUROCRYPT, 457-473.

[4] Liu, J., Dolson, R., & Zhang, Z. (2019). *Efficient attribute-based encryption with user revocation for cloud storage*. IEEE Transactions on Cloud Computing, 7(3), 708-720.

[5] Yang, K., & Jia, X. (2012). *Expressive, efficient, and revocable data access control for multi-authority cloud storage*. IEEE Transactions on Parallel and Distributed Systems, 25(7), 1735-1744.

[6] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). *Attribute-based encryption for fine-grained access control of encrypted data*. ACM Conference on Computer and Communications Security, 89-98.

[7] Green, M., Hohenberger, S., & Waters, B. (2011). *Outsourcing the decryption of ABE ciphertexts*. USENIX Security Symposium, 34-47.

[8] Hur, J., & Noh, D. K. (2011). *Attribute-based access control with efficient revocation*

in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 22(7), 1214-1221.

[9] Xu, P., Xue, K., Hong, J., & Ding, R. (2018). *Blockchain-based access control and secure data storage in cloud computing*. Future Generation Computer Systems, 89, 263-273.

[10] Zhang, J., Chen, B., & Xiang, Y. (2020). *AI-driven access control: Anomaly detection in cloud environments using deep learning*. IEEE Internet of Things Journal, 7(8), 7450-7462.

[11] Gentry, C. (2009). *A fully homomorphic encryption scheme*. ACM Symposium on Theory of Computing, 169-178.

[12] Chen, L., Srinivasan, R., & Liang, W. (2021). *Hybrid access control for cloud computing: Integrating ABE with lightweight encryption techniques*. IEEE Transactions on Cloud Computing, 10(2), 320-333.

[13] Mosca, M. (2018). *Cybersecurity in an era with quantum computers: Will we be ready?* IEEE Security & Privacy, 16(5), 38-41.

[14] Liu, Z., Zhou, J., & Wang, Y. (2023). *Future-proof access control: A quantum-resistant approach for cloud security*. IEEE Transactions on Information Forensics and Security, 18, 1254-1268.

[15] Ruj, S., Nayak, A., & Stojmenovic, I. (2014). *DACC: Distributed access control in clouds*. IEEE Transactions on Parallel and Distributed Systems, 25(2), 384-394.