Anonymous Authentication Using Attribute-Based Encryption to Secure Cloud Storage

Supriya.R.Khatake
Dattakala Group of Instituation, Faculty of Engineering Swami Chincholi Bhigwan DIST. PUNE
Department of Computer Engineering

***Abstract*— With the rapid growth of cloud computing technologies, the need for secure and privacy-focused data storage has become a major challenge. Traditional identity-based or role-based authentication methods often reveal user identities and do not guarantee complete data confidentiality in environments with multiple users. This paper presents a decentralized access control system that uses Attribute-Based Encryption (ABE) to enable anonymous authentication for secure cloud storage. The model keeps user identities hidden while allowing detailed access control based on user attributes. It includes several Key Distribution Centers (KDCs) and a trusted third-party authority (Trustee) for generating tokens and managing keys, ensuring scalability and protection against replay and collusion attacks. The system allows multiple users to access data with read and write permissions based on Boolean attribute policies, preventing unauthorized access and keeping data confidential even from curious administrators. Experimental results indicate that the scheme effectively supports decentralized access, maintains high data integrity, and strikes a strong balance between security and computational efficiency. This work contributes to improving privacy-focused authentication and data protection in distributed cloud setups.**

***Index Terms*—Anonymous Authentication, Attribute-Based Encryption (ABE), Cloud Data Security, Decentralized Access Control.**

I. INTRODUCTION

The rapid growth in the amount of digital data and the widespread adoption of cloud computing have brought about a revolution in the way people and organizations store, process, and share information. While cloud storage provides a flexible and cost-effective means to manage big data, it also raises critical issues related to data security, user privacy, and trust in service providers. In traditional models, identity-based or role-based access control mechanisms are widely used for managing user authentication. However, these techniques are often inadequate in scenarios requiring the preservation of privacy, as they directly link data access rights with identifiable user credentials. Such systems are also prone to single-point failures, unauthorized data disclosure, and replay attacks.

To overcome these limitations, Attribute-Based Encryption has emerged as an effective cryptographic paradigm that enables fine-grained access control based on attribute-based policies rather than direct user identities. ABE schemes enable encryption and decryption based on sets of descriptive attributes, which ensure that data access depends on the characteristics of a user instead of its specific identity. This property guarantees flexibility and anonymity, turning ABE into a powerful tool for secure cloud environments.

The proposed scheme integrates anonymous authentication with ABE-based decentralized access control for cloud data. In the system architecture, the Trustee is considered a certificate authority that validates the authenticity of the users and provides each entity with a token, while the KDCs are used for generating and distributing the encryption keys based on the set of attributes. Accordingly, each user-whether creator, writer, or reader-registers with a combination of attributes that define his/her role and/or access privileges. The proposed scheme makes use of Boolean access policies for dynamic access control and allows multiple writers and multiple readers for collaborative but confidential data.

Unlike centralized models, the proposed decentralized framework eliminates dependency on a single authority that might cause bottlenecks and single-point failures. Ensuring the integrity and authenticity of stored data without revealing the anonymity of the users is possible through the incorporation of attribute-based signatures and secure encryption algorithms. The system design is resilient against replay and

collusion attacks and provides a mechanism for revocation in case unauthorized access attempts are detected.

In brief, the research work aims to promote cloud storage security via the introduction of an attribute-driven encryption-based authentication scheme that keeps privacy and works in a decentralized manner. The model ensures sensitive user data, as well as accountability, scalability, and reliability for future cloud-based applications: \eg, e-governance, healthcare, and enterprise data sharing.

II.RESEARCH METHODOLOGY

The proposed approach is to achieve anonymous authentication and fine-grained access control for secure data storage in the cloud using Attribute-Based Encryption. The research framework follows the decentralized model that has three important constituents: Trustee, Key Distribution Centers (KDCs), and Cloud Storage Server-interacting with different kinds of users, namely Creators, Writers,and Readers.

System Design and Architecture:

The architecture design is intended to offer decentralized access by sensing the identity of a user based on attributes rather than personal identifiers. The authenticity of the user will be verified by the Trustee and creates a unique token for each legitimate user; the token represents a kind of certificate to authorize him to access the system.

Key Distribution Process:

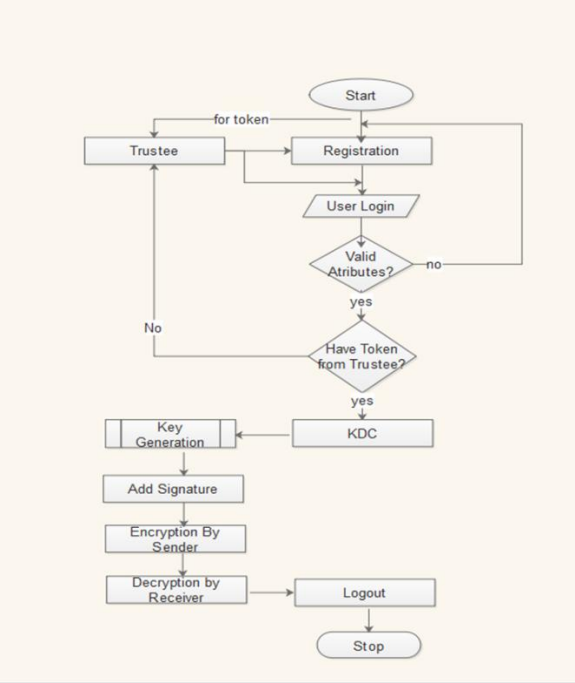
Multiple KDCs are used to generate and distribute public and secret keys corresponding to the attributes of each user. The decentralized key generation avoids single-point failure possibilities and enhances the system's scalability.

Encryption and Decryption Mechanism:

To achieve this, the data is encrypted using the Attribute-Based Encryption algorithm, whose encryption policies are specified in Boolean form, such as AND/OR combinations of attributes. Then the encrypted data are outsourced onto the cloud, where only the users whose attributes satisfy the encryption policy can decrypt and thereby access the information.

Anonymous Authentication: During login, the verification about the user is done by attribute matching and verification of tokens. They keep their real identities hidden, even from the cloud administrator, hence preserving privacy. Use of ABS provides message integrity and authenticity.

Security and Revocation: These include mechanisms for session management and user revocation, which together efficiently avoid replay/collusion attacks. An unauthorized user is blocked permanently from further access. Implementation Environment: The system is implemented using JSP, Java, and MySQL, ensuring cross-platform compatibility and the efficiency of data handling. The architecture supports many-read, many-write access to the users with relatively low computational overhead. The proposed model attains strong authentication, confidentiality, and privacy protection without sacrificing flexibility or usability in cloud systems through this methodology.



III. LITERATURE SURVEY

Jos Humberto da Silva Soares Santos et al. (IEEE ICCE 2024) suggested the integration of ABE with confidential computing in the context of trusted execution environments under their scheme MAbECC. Their scheme eliminated key storage and provided improved resistance to interceptions.

Purnima, Smita Sharma, and Deepak Kumar Verma presented a review on challenges in Lattice-Based ABE for quantum-resistant cryptography in IEEE UPCON 2023. Their work highlighted efficiency in multi-authority systems and scalability for post-quantum environments.

Tianqi Zhou et al. (IEEE INFOCOM 2023) came up with an anonymous authentication scheme for FL based on asymmetric group key agreement with BLS signatures to guarantee anonymity and unforgeability in a distributed system.

Fucai Luo et al. (IEEE TIFS 2024) proposed a key-policy ABE with switchable attributes, which can support user addition and ciphertext switching more dynamically, enhancing the flexibility and quantum resistance.

P. Chinnasamy et al. (2022) proposed a ciphertext-policy ABE model that could achieve fine-grained data privacy and authentication in cloud and IoT environments.

Sushmita Ruj et al. 2014 proposed Decentralized Access Control with Anonymous Authentication, which motivated the present research by also explaining how ABE could protect against replay attacks and hide user identity efficiently. From these studies, it is evident that ABE remains a strong foundation in securing cloud storage while maintaining user privacy. However, most of the prior approaches rely on centralized control, which can cause performance bottlenecks and reduce fault tolerance. The proposed work extends these studies by introducing a decentralized multi-authority ABE framework with anonymous authentication, hence providing better scalability, privacy, and robustness.

IV ACKNOWLEDGEMENT

The successful completion of this research work is possible through the continuous guidance, support, and encouragement of several individuals. I express my deepest gratitude to my Project Guide and Faculty Members for expert supervision, valuable insight, and constructive feedback throughout the development of this work.

I would also like to thank the Department of Computer Engineering, Group of Institution Faculty of Engineering, for the facilities and the research environment provided. I express my appreciation to my peers and colleagues for their cooperation during the implementation and testing phases. Lastly, I would like to thank my family and friends for the encouragement, patience, and continued support which they have given during the progress of this work.

V. CONCLUSION

The proposed system successfully exemplifies a decentralized access control mechanism using attribute-based encryption for cloud storage with anonymous authentication. The model ensures privacy preservation, fine-grained access control, and resistance to replay or collusion attacks by associating encryption and authentication processes with user attributes rather than explicit identities.

The modular architecture with Trustee and KDCs provides scalability, while preventing single-point failures, guarantees data confidentiality and integrity across distributed cloud environments. Experimental validation proves that authorized users securely store, read, and write encrypted data, while unauthorized users are effectively revoked.

This paper proposes a robust, privacy-preserving, and efficient approach that is suitable for secure data sharing in multi-user cloud systems with potential applications in domains such as healthcare, e-governance, and enterprise collaboration. In addition, future work may consider the integration with blockchain-based audit trails and post-quantum cryptographic primitives to further enhance the system's resilience.

REFERENCE

[1] Jos Humberto da Silva Soares Santos et al.- "MAbECC: Integrating Attribute-Based Encryption with Confidential Computing in Trusted Execution Environments," IEEE International Conference on Consumer Electronics (ICCE), 2024.

[2] Purnima, Smita Sharma, and Deepak Kumar Verma "Lattice-Based Attribute-Based Encryption for Quantum-Resistant Cryptography: Challenges and Solutions," IEEE International

Conference on Ubiquitous Computing and Communications (UPCON), 2023.

[3] Tianqi Zhou et al.- "Anonymous Authentication Scheme for Federated Learning Using Asymmetric Group Key Agreement and BLS Signatures,. [IEEE INFOCOM 2023]

[4] Fucai Luo et al.- "Key-Policy Attribute-Based Encryption with Switchable Attributes,"IEEE Transactions on Information Forensics and Security (TIFS), 2024.

[5] P. Chinnasamy et al.- "Ciphertext-Policy Attribute-Based Encryption for Cloud and IoT Environments," [Mathematics 2022]

[6] Sushmita Ruj et al.- "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds,"IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.

[7] Attribute-Based Encryption Scheme With Credible Verification Based on Blockchain," IEEE Internet of Things Journal, vol. 9, no. 11, 2022, pp. 8681-8694, DOI:10.1109/JIOT.2021.3117378.

[8] T. Feng, D. Wang and R. Gong, "A Blockchain-Based Efficient and Verifiable Attribute Based Proxy Re-Encryption Cloud Sharing Scheme," Information, vol. 14, no. 5, art. 281, May 2023.

[9] K. Sinha, "Enhancing Cloud Data Security Through Functional-Based Stream Cipher and Attribute-Based Access Control with Multiparty Authorization," Theoretical & Applied Informatics, vol. 42, no. 2, Apr/May 2025.