Anonymous Authentication Using Attribute-Based Encryption to Secure Cloud Storage

Supriya Raghunath Khatake[1], Dr.Ganesh G. Taware[2]
[1]*PG Scholor, Dattakala Group of Instituation, Swami Chincholi Bhigwan, Dist. Pune*
[2]*Assistant Professor, Dattakala Group of Instituation, Swami Chincholi Bhigwan, Dist. Pune*

***Abstract*— In today's information technology environment personal data is exposed to risks every day. Attribute-Based Encryption (ABE) has shown to be a useful cryptographic primitive that allows one to build privacy-enhancing technologies. We propose an anonymous authentication protocol based on ABE. It allows users to prove their identity without revealing their identity to anyone, not even verifier.**

The proposed scheme enables granting access to users only based on their attributes. Attributes can be anything from user roles to group membership or credentials. This provides an additional privacy guarantee since the identity of a user is not strictly tied to their attributes. We implement our protocol on top of OpenID Connect (OIDC), which is an industry-standard protocol. This allows us to demonstrate the applicability of our protocol to real-world production systems such as cloud environments and federated identity providers.

Our protocol ensures that users remain anonymous during all stages of the system. Further it is collusion-resistant, meaning that multiple users cannot gather attributes together in order to gain access. The protocol is also secured against replay attacks by using timestamped tokens and nonces. Access and keys are distributed in a decentralised manner. We evaluate our protocol and show that it incurs little overhead.

***Index Terms*— Access Control, Attribute Based Encryption, Anonymous Authentication, Key Distribution Center, CP-ABE, KP-ABE**

I. INTRODUCTION

- Access control is a key concern in cloud computing because it ensures that only authorized users can access information.
- A lot of data is stored in the cloud, and much of it is sensitive. For important documents, it is important to keep them private and confidential. There are several types of access control systems. These include User Based Access Control (UBAC), Role Based Access Control (RBAC), and Attribute Based Access Control (ABAC).
- Cloud computing provides storage for different types of digital information, such as databases, software, platforms, communication services, and business data.
- The security of the data stored in the cloud is a major concern. To protect data from unauthorized access and from threats like loss or attacks, various encryption techniques are used. These include public key infrastructure, identity-based encryption, and attribute-based encryption. Attribute-based encryption uses properties to encrypt data. This paper discusses some of these techniques to secure cloud storage using attribute-based methods. Many types of sensitive data can be protected using this method. This idea was first introduced by Sahai and Waters.

A. Introduction: Attribute

The term "attribute" refers to any property used to describe a group or category.

For example, a student is a group that can be described by properties like class, division, and roll number. Similar properties like color, height, and weight can be used to describe any object. These attributes help determine the category of a user, such as student, teacher, or principal.

B. Attribute Based Encryption

Attribute-based encryption is a way of encrypting data based on the attributes of a user.

This is a stronger method than traditional encryption. In this method, both a public key and a secret key are used, but the secret key depends on the attributes assigned to the user. The system is designed to resist collusion, meaning that no group of users can combine

their keys to access data they shouldn't. Attribute-based encryption is a good choice for encrypting sensitive data stored in the cloud.

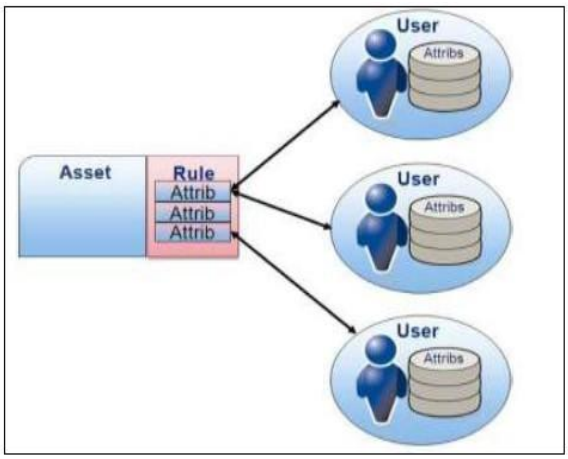


Fig. 1 Attribute Based Authentication

This is a general cloud storage model with higher security.

There are three types of users: creator, writer, and reader. Users log in or register by providing a set of attributes that define their category. They also need to specify their role, which determines what they can do. When users choose a role, they must verify their identity. To do this, they may contact a trustee before registration and get a unique token. Using this token, they can get a key from the Key Distribution Center. This key is used to encrypt data when creating or writing to the cloud, and to decrypt data when reading from the cloud.

II. PRELIMINARIES

Background Overview of Anonymous Authentication using Attribute Based Encryption.

- Attribute

An attribute is a property or characteristic of an object. We can describe an object using its attributes. For example, a student is a group that can be described by properties like class, division, and roll number. Similar properties like color, height, and weight can be used to describe any object. Each user has many attributes, which help to determine their category, such as student, teacher, or principal.

In the proposed system, attributes are an important part because users can register or log in using attributes that define their category.

These attributes are used to encrypt data when a user is the creator, and they are also used to decrypt data for a reader.

- ABE

Attribute-based encryption is a method where data is encrypted based on the attributes of the user.

- This is a stronger approach than conventional encryption. In this method, a public key and a secret key are used, and the secret key is based on the attributes of the user. The system is designed to resist collusion, meaning no group of users can combine their keys to access data they shouldn't. Attribute-based encryption is a useful method for encrypting sensitive data stored in the cloud. Typically, attributes are used to describe a user's category. During encryption, these attributes are combined with a unique token received from a trusted authority. There are two common types of ABES: Cipher-Text Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute-Based Encryption (KP-ABE). In CP-ABE, a user’s private key is connected to certain attributes, and a ciphertext includes an access policy based on these attributes. A user can decrypt the ciphertext only if their attributes satisfy the policy set in the ciphertext.

- Anonymous Authentication

The word 'anonymous' means unknown or not recognized by the system. In this system, users remain anonymous to everyone. They are real but their identity is kept secret. This is done by using attributes for authentication instead of using things like usernames, passwords, or roles.

- Key Distribution Center

The Key Distribution Center (KDC) is a system that makes and gives out keys to users based on their attributes and requests.

There are two types of keys. The public key is shared with everyone in the system. The secret key is given only to specific users based on their request. When sending a message, the sender uses their public key and secret key. The receiver uses their own secret key and the public key to decrypt the message. Even though these keys are different, they are somewhat similar to each other.

- Cipher-Text-Policy Attribute-Based Encryption (CP-ABE)

In CP-ABE, a user's private key is connected to certain features, and the encrypted message has a policy that says who can access it.

A user can decrypt the message only if their features match the policy. The policy can be a mix of conditions like "and" or "or". It uses Boolean logic to check if the user's attributes fit. For example, if the universe of attributes is P, Q, R, S, and a user have P and Q, they can't decrypt a message that requires P and S or R.

- Key-Policy Attribute-Based Encryption (KP-ABE)

KP-ABE is the opposite of CP-ABE.

In this case, the message is encrypted using a user's secret key. Encryption and decryption depend on the secret keys given by the KDC. The KDC acts as a central authority that makes both types of keys and gives them out based on the user's needs. The keys are usually linked to the access policies used in the system.

III. SYSTEM IMPLEMENTATION

In our proposed system the access control is to be fine grained. The proposed system has decentralized access control so as to keep flexible access with respect to location and machine. The encryption process is based on attribute-based encryption technique. The Read/Write access control is Many Write Many Reads. There is authentication for privacy preserving. The User will authenticate himself/herself by using set of attributes. The proposed system is collusion resisting as well as it will protect from replay attack

A. System Architecture

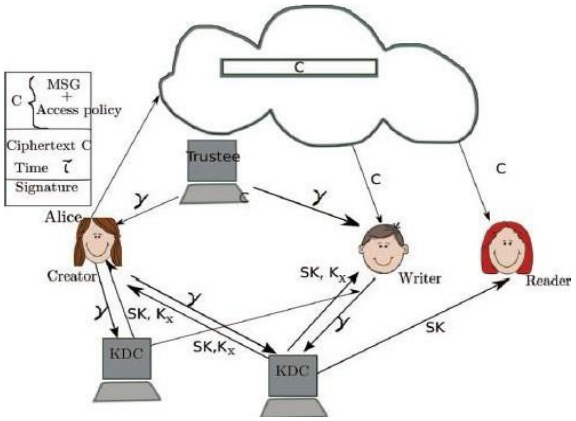


Fig 2. System Architecture

In general, the scenario of our proposed system is as follows.

- Data storage for the authorized users (authorization is based on set of attributes). Here User can access as per his role. The user might be a creator, Writer or a reader.
- For storing and accessing of data, user must need to authenticate themselves.
- This authentication is based on the category of the user; not by the identity base. The authentication is based on set of the attributes that are responsible for describing the category of the user.
- User is not known by his identity. This is the main aim of the proposed system to hide the identity of the user from all. That means the user will be anonymous.
- Trustee: This is the third-party certificate issuing authority for the assurance of the genuine users. Before authentication, User must need to approach the trustee to receive the token (The token denotes that the user is verified by the trustee and the unique token is given for him) This token is to be submitted to the KDC to get the secret key for the particular user.
- Key distribution Center: This is the KDC work to distribute the keys required for encryption and decryption of the contents stored to the cloud. These contents are visible to the admin only in encrypted formats only.
- Denial of access for rejected users.

B.User Registration Process:

The user registration process uses certain properties called attributes.

These attributes are specific to the type of user. For example, if the user is a student, the attributes could be rolling number, class, division, and batch. Users use these attributes to register themselves. The access rules for users follow a Boolean pattern, as shown in the example.

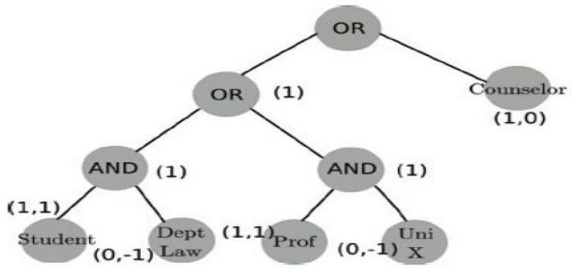


Fig 3. Example of Claim Policy

Two types of users can register using the right combination of attributes.
The claim policy works like this: A = a1 and a2 or b1 and b2 or C. Here, A, B, and C are user categories. a1 and a2 are the attributes for user A; b1 and b2 are the attributes for user B; and C represents the user. During login, the system checks the combination of attributes from the same category.

C. Trustee Module:
This is a third-party certifying authority (CA) that verifies valid users.
Users need to log in using the trustee module when they use the system. The trustee checks the user details and determines the user's type, then generates a token based on the user's occupation from their records.
An example of a trustee could be an insurance department where a user has a policy.
Users log in to the automated trustee module by providing the last six digits of their policy number, their date of birth, and their mother's maiden name. The administrator at the trustee module does not see the full details of the policy holder. Instead, the automated system only shows the last six digits of the policy, the user's date of birth, the mother's maiden name, and the occupation.
User input for the trustee module: T(Ui) = {I, B, M}
The verification process is done at the module:
V = {(if T(Ui) == true) then RID, Tkn}
Here, RID is the request ID, and Tkn is the token generated, which shows the user's occupation starting with the first letter.

D. KDC - Key Distribution Center
Every user needs to go to the KDC to get the public and secret keys required for encryption and decryption.
Users log in to the KDC using the token they receive from the Trustee.
User input at the KDC: IK(Ui) = {A, Tkn}
The secret key generated is SK(Ui)
The public key generated = PK(U)

E. Algorithm for Encryption Process
The algorithm has two main parts: sender-side encryption and receiver-side decryption.
Sender Side Encryption
Encryption happens at the sender's end for each message using attributes and keys.
If the original message is MSG, the encryption ENC can be ENC = {ABE.SK, PK, MSG}
Here, ABE stands for attribute-based encryption.
The message is decrypted at the receiver's end.
The decrypted message returns to its original form: MSG = {ENC / (SK.PK.ABE)}

F. Algorithm for Signature
The signature is created based on the user's attributes.
Both the secret and public keys are used during transactions.
This signature is generated during the transaction and is verified every time the message is used.
The signature is created like this:
$ = {(SK1, SK2, ..., SKn where ï□¢ï□□SKUI), (PK1, PK2, ..., PKnï□¢ï□□PKUI), (a1, a1 where ï□¢ï□□A)
}
Verification of the signature is done as: ABS.V($, MSG, ï□¡) where ï□¡ is a monotone program generated.

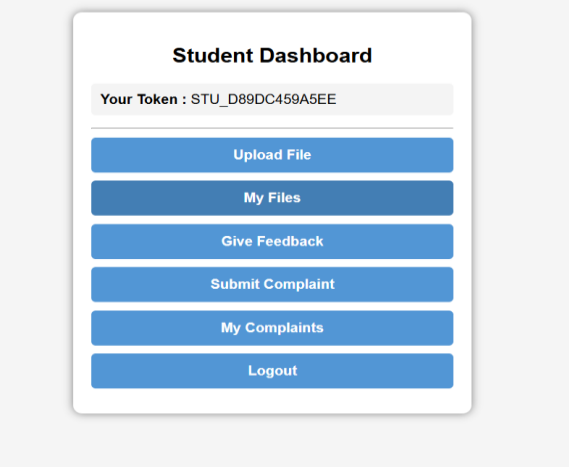
G. Storage of Contents to Cloud
As discussed earlier, every message is in an encrypted format before being stored in the cloud.
The message is in the following format:
CP = ABE.ENC (MSG, ï□£)

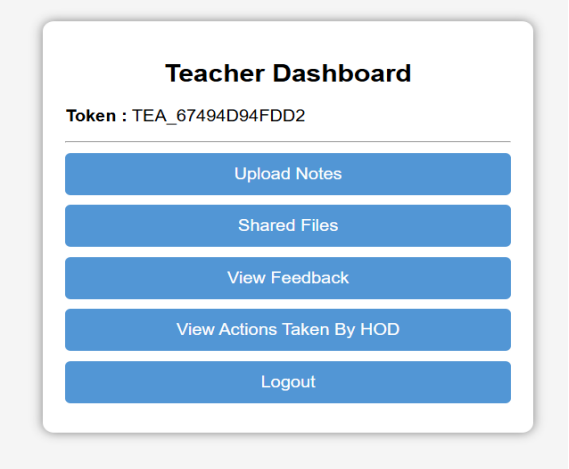
H. User Revocation
User revocation is possible in this system.

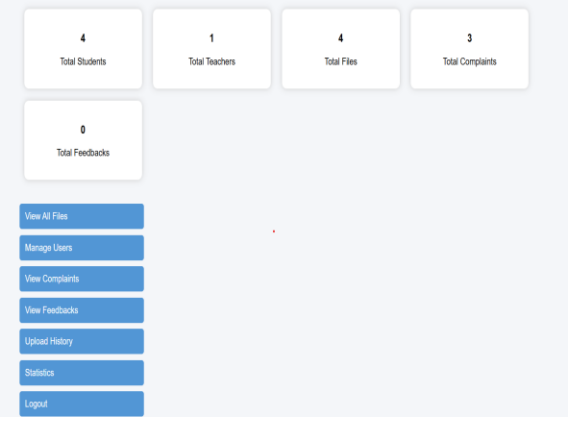
IV. RESULTS

After running all the modules properly, here are the results and observations from the system:
i. The system can work in a decentralized way, meaning it can be used from different places as long as there is a network connection.
ii. Access to the system is controlled using authentication based on the user's category and attributes.
iii. The CA (Trustee) is responsible for creating tokens and verifying if a user is genuine.
iv. The KDC is available throughout the network and creates public and secret keys depending on the attributes used and the token received from the user during transactions.
v. Encryption is done using the set of attributes and the key generated by the KDC, which is based on the same set of attributes.

vi. The system allows multiple users to read and write data.
vii. Any attempt to access without proper permission is rejected.
viii. Replay attacks are not possible.
ix. The contents are encrypted, but they are not hidden from the user and the intended destination user.







V. LIMITATIONS

Because the administrator of the storage has access to the policy, they can partially decrypt the data.

VI. CONCLUSIONS

The system is designed to be decentralized and easy to access. It uses certain characteristics as login information and also forms the foundation for encryption. The system is protected against replay attacks. It allows users to log in without revealing their identity. The process of sharing keys through the KDC happens in a decentralized way.

ACKNOWLEDGEMENTS

We want to sincerely thank Dattakala Dattakala Group of Institutions, Faculty of Engineering, Swami Chincholi Bhigwan, District Pune, for giving us a strong platform to develop our skills and abilities. We would also like to thank HOD Dr. Bere S.S, Guide Dr. Taware G.G, and all the teachers for their valuable guidance. We also wish to express our gratitude to everyone who directly or indirectly supported us in completing this paper.

REFERENCES

[1] J. Tong, Q. Liu, and Y. Long, "A File Encryption System Based on Attribute-Based Encryption," in *Proc. 17th Int. Conf. Computational Intelligence and Security (CIS)*, Wuhan, China, 2021, pp. 454–460, doi: 10.1109/CIS54983.2021.00100.

[2] T. Zhou, J. Shen, P. Vijayakumar, M. Z. A. Bhuiyan, and A. Sivaraman, "Anonymous Authentication Scheme for Federated Learning," in *Proc. IEEE INFOCOM Workshops: Int. Workshop on AI-Driven Trustworthy, Secure, and Privacy-Preserving Computing (AidTSP)*, 2023, pp. 1–7, doi: 10.1109/INFOCOMWKSHPS57453.2023.10225800.

[3] F. Luo, H. Wang, X. Yan, and J. Wu, "Key-Policy Attribute-Based Encryption With Switchable Attributes for Fine-Grained Access Control of Encrypted Data," *IEEE Transactions on Information Forensics and*

Security, vol. 19, pp. 7245–7261, Aug. 2024, doi: 10.1109/TIFS.2024.3432279.

[4] Purnima, S. Sharma, and D. K. Verma, "LABE: Challenges and Perspectives of Attribute-Based Encryption in Lattice-Based Cryptography," in *Proc. 10th IEEE Uttar Pradesh Section Int. Conf. Electrical, Electronics and Computer Engineering (UPCON)*, Greater Noida, India, 2023, pp. 1145–1150, doi: 10.1109/UPCON59197.2023.10434485.

[5] J. H. da S. S. Santos, D. C. G. Valadares, K. C. Gorgônio, and A. Perkusich, "Mobile Data Security With Attribute-Based Encryption and Confidential Computing," in *Proc. IEEE Int. Conf. Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2024, pp. 1–6, doi: 10.1109/ICCE59016.2024.10444176.

[6] P. Chinnasamy, P. Deepalakshmi, A. K. Dutta, J. You, and G. P. Joshi, "Ciphertext-Policy Attribute-Based Encryption for Cloud Storage: Toward Data Privacy and Authentication in AI-Enabled IoT System," *Mathematics*, vol. 10, no. 1, Art. no. 68, 2022.

[7] J. Zhang, J. Zhang, Y. Yuan, and Z. Li, "An Expressive Fully Policy-Hidden Ciphertext-Policy Attribute-Based Encryption Scheme with Credible Verification Based on Blockchain," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8681–8694, 2022, 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. no. 281, May 2023.

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

About the Authors

1]Supriya Raghunath Khatake is a second-year M.E. student in Computer Engineering at Dattakala Group of Institution, Faculty of Engineering Swami Chincholi Bhigwan DIST. PUNE. Her research interests include Cloud Storage Security,Privacy-Preserving Techniques, and Attribute-Based Encryption (ABE). Currently, she focusing on designing anonymous authentication schemes to enhance user privacy in decentralized cloud storage environments.

2]Dr.Ganesh G. Taware is currently working as a professor in the department of Comupter Science and Engineering at Dattakala Group of Instituation, Faculty of Engineering Swami Chincholi Bhigwan DIST. PUNE.As a guide, he has supervised this project on developing an Anonymous Authentication using Attribute-Based Encryption to Secure Cloud Storage, providing technical guidance on implementing access policies to maintain user anonymity.