https://doi.org/ 10.33472/AFJBS.6.10.2024.1081-1087

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

# ATTRIBUTE-BASED ENCRYPTION APPROACH FOR STORAGE, SHARING AND RETRIVAL OF ENCRYPTED DATA IN THE CLOUD

***[1]P. Anusha, [2]Mohammed Zubair Ahmed, [3]Gangasani Tharun, [4]Sajjan Rohith,***

***[5] Jarupula Mahender***

Assistant Professor in Department of CSE Sreyas Institute Of Engineering And Technology

***[1]anusha.palreddy@sreyas.ac.in***

[2.3.4,5]UG Scholar in Department of CSE Sreyas Institute Of Engineering And Technology

***[2]mohammedzubairahmed2020@gmail.com , [3]tharungangasani2001@gmail.com , [4] Rohithsajjan11@gmail.com,***

***[5] mahenderjarupula2000@gmail.com***

Article History
Volume 6,Issue 10, 2024
Received:17 Apr 2024
Accepted : 05 May 2024
doi: 10.33472/AFJBS.6.10.2024.1081-1087

**Abstract**

One of the most cost-effective services in cloud computing is storage, used by businesses and individuals to outsource their massive data to untrusted servers. Efforts have studied problems around this application scenario in different fronts: efficiency, flexibility, reliability, and security. In this paper we address the security concerns of cloud storage under the scenario where users encrypt-then-outsource data, share their outsourced data with other users, and the service provider can be queried for searching and retrieval of encrypted data. As main distinctive, we propose a security approach for storage, sharing and retrieval of encrypted data in the cloud fully constructed on the basis of attribute-based encryption (ABE) thus enabling access control mechanisms over both the encrypted data and also for the information retrieval task through search access control. Compared to related works, our approach considers efficient encryption at three different levels: i) bulk encryption of data outsourced to the cloud, ii) keys management for access control over encrypted data by means of digital envelopes from attribute based encryption, and for ABSE are provided over the asymmetric setting (Type-III pairings) to support security levels of 128-bits or greater. Experimental results on benchmark data sets demonstrate the viability of our approach for practical realizations using Barreto-Naehrig curves.

**KEYWORDS:** *cloud computing, Attribute Based encryption*

## I INTRODUCTION

One of the most cost-effective services in cloud computing is storage, used by businesses and individuals to outsource their massive data to untrusted servers. Efforts have studied problems around this application scenario in different fronts: efficiency, flexibility, reliability, and security. In this paper we address the security concerns of cloud storage under the scenario where users encrypt-then-outsource data, share their outsourced data with other users, and the service provider can be queried for searching and retrieval of encrypted data. As main distinctive, we propose a security approach for storage, sharing and retrieval of encrypted data in the cloud fully constructed on the basis of attribute-based encryption (ABE) thus enabling access control mechanisms over both the encrypted data and also for the information retrieval task through search access control. Compared to related works, our approach considers efficient encryption at three different levels: i) bulk encryption of data outsourced to the cloud, ii) keys management for access control over encrypted data by means of digital envelopes from attribute based encryption, and iii) novel construction for attribute based searchable encryption (ABSE). Our underlying ABE algorithms are carefully selected from the body of knowledge and novel constructions for ABSE are provided over the asymmetric setting (Type-III pairings) to support security levels of 128-bits or greater. Experimental results on benchmark data sets demonstrate the viability of our approach for practical realizations using Barreto-Naehrig curves.

## II LITERATURESURVEY

### *Introduction to Attribute-Based Encryption (ABE):*

Attribute-Based Encryption (ABE) is a type of public-key encryption that enable fine-grained access control over encrypted data. The concept was introduced by Sahai and Waters in 2005, aiming to enhance security by using attributes for encryption and decryption rather than traditional identity-based methods.

### *Early Developments and Foundational Work:*

- Sahai and Waters (2005): The pioneering paper "Fuzzy Identity-Based Encryption" laid the groundwork for ABE. This work introduced the concept of using attributes to control access, forming the basis for subsequent research in the field .

- Bethencourt, Sahai, and Waters (2007): This paper introduced Ciphertext-Policy Attribute-Based Encryption (CP-ABE), where data is encrypted under an access policy defined by the data owner, and users can decrypt the data if their attributes satisfy the policy .- Goyal et al. (2006): They proposed Key-Policy Attribute-Based Encryption (KP-ABE), where the data is associated with a set of attributes, and users' keys are generated based on access policies .

### *Enhancements and Variants of ABE:*

- Fine-Grained Access Control: Research by Yu et al. (2010) explored achieving secure, scalable, and fine-grained data access control in cloud computing, enhancing the practicality of ABE in dynamic environments . - Revocation Mechanisms: Revocation of access rights is a critical challenge. Wang et al. (2011) proposed

efficient user revocation schemes in CP-ABE, addressing the need for dynamic user management in ABE systems .- Outsourced ABE: Green et al. (2011) introduced the concept of outsourcing decryption to reduce the computational burden on users, making ABE more practical for devices with limited resources .

***.Applications of ABE in Cloud Computing:***

- Healthcare: Li et al. (2013) demonstrated the use of ABE for secure sharing of personal health records in cloud environments, emphasizing the importance of privacy in sensitive data sharing scenarios .- Data Sharing and Collaboration: Ruj, Nayak, and Stojmenovic (2011) proposed Distributed Access Control in Clouds using ABE, highlighting its applicability in collaborative cloud environments .- IoT Security: Recent research has focused on integrating ABE with Internet of Things (IoT) to secure data transmission and storage in IoT networks. Works by Liu et al. (2018) explore efficient ABE schemes tailored for IoT devices .

***Challenges and Future Directions:***

- Scalability: Ensuring that ABE systems can handle large numbers of users and attributes efficiently remains an ongoing research area. Techniques such as hierarchical ABE (HABE) have been proposed to address scalability issues.
- Performance Optimization: Reducing the computational overhead associated with encryption and decryption in ABE systems is critical for their widespread adoption. Outsourcing computations and optimizing cryptographic operations are active research areas.- Quantum-Resistant ABE: With the advent of quantum computing, developing ABE schemes that are secure against quantum attacks is becoming increasingly important.The literature on Attribute-Based Encryption has evolved significantly since its inception, with numerous enhancements and applications demonstrating its potential in providing fine-grained access control in various domains. Ongoing research aims to address existing challenges, optimize performance, and explore new applications, ensuring that ABE remains a robust and versatile tool for data security in the cloud and beyond.

## III EXISTING SYSTEM

A straightforward encryption approach to prevent DO’s data disclosure and to keep DO’s data private from CSP or from any other entity, causes the provider cannot manipulate data, that is, loss of utility appears as the encrypted data cannot be used by the CSP for retrieval/searching purposes. Due to that inconvenience, DUs should download large volume of encrypted data, decrypt, and then search over the plaintext data (locally), re-encrypt and upload again its data to the cloud. Of course, so one approach incurs in huge communications and computations overhead and is completely inefficient. Searchable encryption (SE) has been the most known approach to cope with the problem of searching over encrypted data stored in untrusted servers. SE is defined as the ability to identify and retrieve a set of objects from an encrypted collection that satisfy a query. In SE, the CSP executes DU’s encrypted queries over encrypted data without decryption, so it does not learn anything

about the data content, search criteria, nor search patterns.

***Disadvantages***

- Chance of manipulation of Data if the key is disclosed.
- Security and Privacy of the data is breached.
- Maybe loss ofdataoccurs.

## IV PROBLEMSTATEMENT

In cloud computing, ensuring secure and controlled access to sensitive data is a significant challenge due to the dynamic and multi-user environment. Traditional encryption methods fall short in providing the necessary fine-grained access control and scalability. Attribute-Based Encryption (ABE) offers a solution, but its implementation in cloud environments faces issues such as performance overhead, complexity in key management, and the need for robust, efficient, and adaptable access policies. Therefore, there is a need to develop efficient ABE frameworks that can seamlessly integrate with cloud services, ensuring secure, scalable, and flexible data access and management in the cloud computing of the ABE system

## V PROPOSEDSYSTEM

We present a security approach for storing, sharing and retrieving of encrypted data in the cloud, fully constructed on the basis of attribute-based encryption (ABE). Our approach is well suited for a known cloud-based storage and sharing model, where DO ploads encrypted data to the cloud to ensure confidentiality (by means of symmetric data encryption) and establishes access control mechanisms for data sharing using attribute based encryption; DU can selectively locate specific documents using an index-based structure and retrieve documents of interest in encrypted form, without revealing any information to the CSP and under a fine-grained search control. Our proposed approach aims at meeting the following four requirements to enable practical storage, sharing and retrieval of encrypted data in the cloud:

R1 - DO can execute Ek1 (D) efficiently to provide confidentiality over outsourced data to the cloud at the same time that enables fine-grained data access control and secure distribution of k1 for DUs, thus enabling secure data sharing.

R2 - DUs can query Ik2 (W) (via the CSP) by computing and using Tk3 (wq) at the time that secure fine-grained search control is enabled.

R3 - DUs can ask the CSP to return the k-most relevant documents from the retrieval task results, ordered accordingly to their relevance to the query.

R4 - Both R1 and R2 comply with recommended security levels1 (i.e. $\lambda \geq 128 -$ bit).

We called our approach FABECS (Fully Attribute-Based Encryption scheme for Cloud Storage, Sharing and Retrieval) which fulfills requirements R1-R4. FABCS includes a novel Cipher-text policy ABSE (CP-ABSE) construction to achieve R2 and R3 requirements. At the same time, FABECS reuses the settings of ABSE (pairings and curve parameters) for the set up of DET-ABE which provides cryptographically enforced fine-grained access controls needed to meet requirement.

## VI IMPLEMENTATION

***Registration:*** You can create a new account by providing necessary details and selecting attributes relevant to your access permissions

***Login:*** Enter your credentials to access your secure account. Our ABE framework ensures that only users with the correct attributes can decrypt sensitive data.

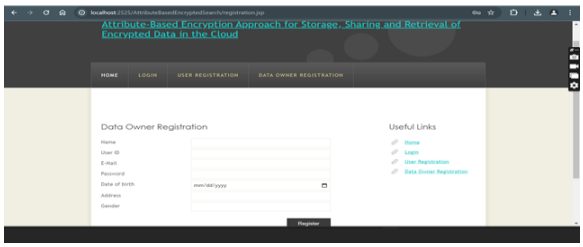
***Set keyword:***Set keyword refers to the set of attributes assigned to users or encrypted data. Each user possesses a unique set of attributes, and access to encrypted information is granted only if the user's attribute set matches the access policy defined in the encryption

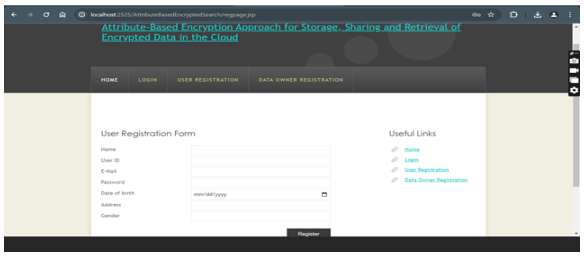
***Search Key:*** The search key is generated based on user attributes and search criteria, ensuring that only authorized users with matching attributes can locate and access the desired information securely

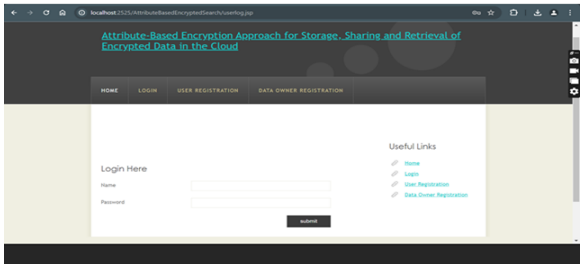
***View request:***Feature allows administrators to review and manage user access requests.

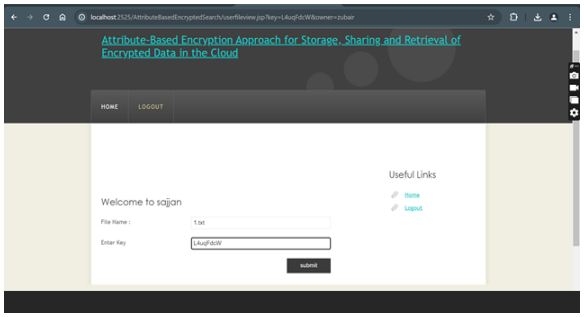
***Result:*** Displays the outcome of encryption and decryption operations.

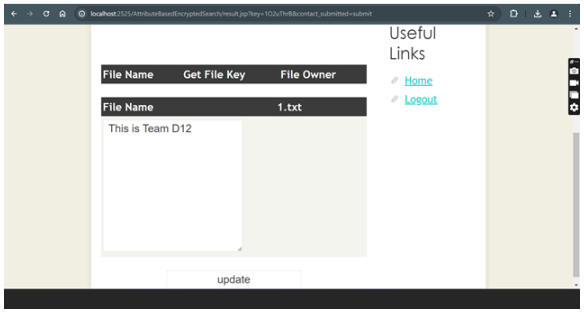
## VII RESULTS

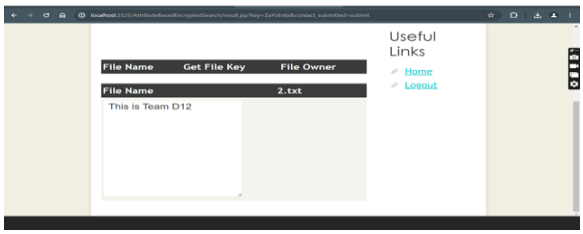



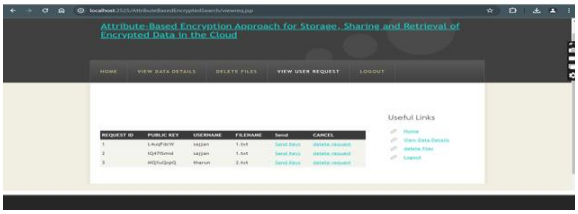






## VIII CONCLUSION

In conclusion, attribute-based encryption (ABE) offers a promising approach for securing data storage, sharing, and retrieval in cloud environments. By leveraging attributes to define access policies, ABE provides fine-grained control over who can access encrypted data, enhancing privacy and security. This flexibility enables organizations to enforce complex access policies based on various attributes such as user roles, organizational affiliations, or other contextual information.Moreover, ABE facilitates secure data sharing among multiple users with diverse access requirements, eliminating the need for cumbersome key management schemes. Users can decrypt data only if their attributes match the access policy associated with the encrypted content, ensuring that sensitive information remains protected even in shared environments.Furthermore, ABE enhances data retrieval efficiency by enabling selective access to encrypted data based on specific attributes, reducing the overhead associated with traditional encryption schemes.However, challenges such as scalability, key management complexity, and performance overheads still need to be addressed to fully realize the potential of ABE in cloud environments. Despite these challenges, the benefits of attribute-based encryption make it a compelling solution for securing sensitive data in the cloud while enabling efficient storage, sharing, and retrieval processes.

## REFERENCES

[1] Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07), 321-334.

[2] Wang, G., Li, Q., Ren, K., & Lou, W. (2010). Towards Secure and Scalable Computation in Cloud Computing. IEEE Transactions on Services Computing, 5(2), 220-232.

[3] Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM), 1-9.

[4] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. IEEE Transactions on Parallel and Distributed Systems, 24(1), 131-143.

[5] Ruj, S., Nayak, A., & Stojmenovic, I. (2011). DACC: Distributed Access Control in Clouds Using Attribute-Based Encryption. In Proceedings of the 10th IEEE/ACM International Conference on

Grid Computing (GRID), 41-48.

[6] Goyal, Vipul, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In Proceedings of the 13th ACM conference on Computer and communications security, pp. 89-98. 2006.

[7] Hur, Junbeom, and Hyunsoo Yoon. "Attribute-based access control with efficient revocation in data outsourcing systems." IEEE Transactions on Parallel and Distributed Systems 24, no. 7 (2013): 1357-1366.