Journal of Science Engineering Technology and Management Science
Volume 02, Issue 08, August 2025 *ISSN: 3049-0952*
www.jsetms.com *DOI:10.63590/jsetms.2025.v02.i08.371-379*

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

[1]M.SOWMYA,[2]M.NIKHILA,[3]G. VIGNESHWAR,[4]Mrs.S.PAVANI
[123] Students, [4] Assistant Professor
Department Of Information Technology
Teegala Krishna Reddy Engineering College, Meerpet, Balapur, Hyderabad-500097

To Cite this Article
M.Sowmya, M.Nikhila, G.Vigneshwar, Mrs.S.Pavani, "Attribute-Based Encryption Approach For Storage, Sharing And Retrieval Of Encrypted Data In The Cloud", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 08, August 2025,pp: 371-379, DOI: http://doi.org/10.63590/jsetms.2025.v02.i08.pp371-379
Submitted: 12-07-2025 *Accepted: 18-08-2025* *Published: 25-08-2025*

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 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

I. INTRODUCTION

MOTIVATION

Here's the motivation behind using ABE for storage, sharing, and retrieval of encrypted data in the cloud:

1. Fine-grained access control: ABE enables you to define access policies based on user attributes (e.g., job role, department, clearance level). This allows for more granular control over who can access the data.
2. Scalability: In cloud environments, where the number of users and data files can be very large, ABE provides a scalable solution for access control. Adding or removing users doesn't require re-encryption of the data.

3. Data sharing: ABE makes it easier to share data securely. The data is encrypted based on attributes, so anyone with the appropriate attributes can decrypt it. This simplifies the process of sharing data with different groups of users.
4. Data confidentiality: ABE ensures that data stored in the cloud remains confidential, even if the cloud provider is untrusted. Only users with the correct attributes can decrypt the data.
5. Flexibility: ABE supports dynamic access control policies. You can change the attributes associated with a user or the access policies associated with data without having to re-encrypt the data.

PROBLEM STATEMENT

The challenge lies in developing a secure and flexible Attribute-Based Encryption (ABE) system for cloud environments, where traditional access control methods struggle with scalability and complexity. This system must enable fine-grained access control based on user attributes, ensuring data confidentiality even with untrusted cloud providers. It should also efficiently handle a large number of users and data files, support dynamic access policy changes, and provide a secure key management mechanism, all while minimizing computational overhead to ensure efficient data storage, sharing, and retrieval.

OBJECTIVE

To design, implement, and evaluate an ABE-based system that provides secure and flexible access control for data stored in the cloud, enabling efficient storage, sharing, and retrieval while ensuring data confidentiality and scalability. This involves developing a system that allows data owners to define access policies based on user attributes, supports dynamic access control, and offers a secure key management mechanism, all while minimizing computational overhead and maximizing performance in a cloud environment.

II. LITERATURE SURVEY

Attribute-Based Encryption (ABE) offers a flexible way to manage access control for data stored in the cloud. It allows data owners to define access policies based on user attributes, rather than specific identities. This means that users can decrypt data if their attributes satisfy the policy defined by the data owner. This approach enhances security and simplifies key management because the encryption keys are derived from the attributes. This system is particularly useful for secure storage, sharing, and retrieval of encrypted data, offering a fine-grained access control that is essential in cloud environments.

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.

DRAWBACKS

ABE's key challenges include complex key management, potentially high computational overhead for encryption and decryption, and difficulties in revoking user access. Scalability can also be an issue, and the size of the ciphertext can grow with the complexity of the access policies, which could affect

performance.

PROPOSED SYSTEM

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 uploads 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 setup of DET-ABE which provides cryptographically enforced fine-grained access controls needed to meet requirement R1

ADVANTAGES

Attribute-Based Encryption (ABE) provides flexible access control based on user attributes, simplifying key management and enhancing security in cloud environments. It supports scalable data sharing and ensures only authorized users can access the data.

III. SYSTEM DESIGN

SYSTEM ARCHITECTURE

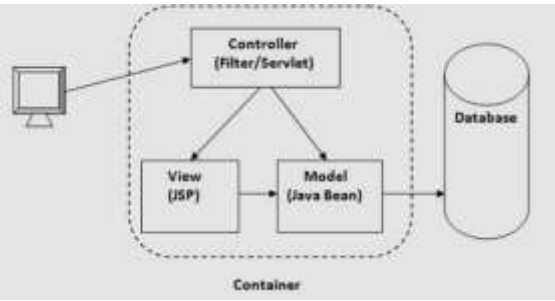


FIG: SYSTEM ARCHITECTURE

IV. MODULE DESCRIPTION

DO (Data Owner)

- DO is fully trusted in the system model.
- DO encrypts the data set and creates the searchable index II.
- -DO uses semantically secure ciphers for: Key management

- Encryption and decryption of documents Secure index generation
- It is assumed that DO can authenticate each actor in the system.
- It is assumed that there is a secure way for DU to generate and obtain encrypted queries (usually facilitated by DO).

DU (Data User)

-DU generates encrypted queries (trapdoors) securely.

-DU uses authenticated channels to interact with the system.

-DU relies on secure encryption mechanisms to maintain the privacy of their queries.

-DU is protected against the CSP learning the content of the queries and search results, apart from possible leakage from access patterns and statistical correlations.

CSP (Cloud Service Provider)

-CSP is the **adversary** in this model.

-CSP is assumed to have:

-Access to encrypted data sets.

-Access to the searchable index II (known ciphertext model).

-Modify or destroy stored data.

CSP can:

- Derive sensitive information based on search queries (trapdoors) and their correlation.
- Utilize statistical information about the data set (known background model).

CSP tries to compromise confidentiality by:

- Deriving information from stored documents, queries, and search outcomes.
- Forging existing access policies (generated by DO) to gain unauthorized access.

V. OUTPUT SCREENS


Data Owner Registration
Useful Links

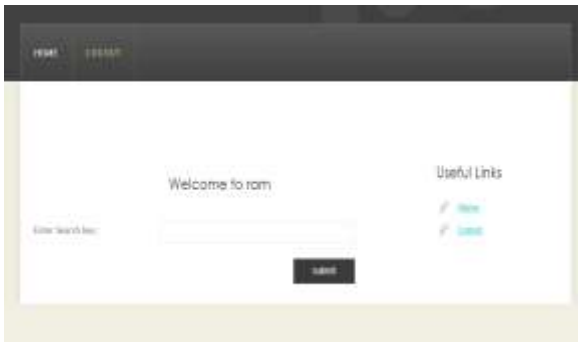

User Registration Form
Useful Links


Useful Links
Login Here

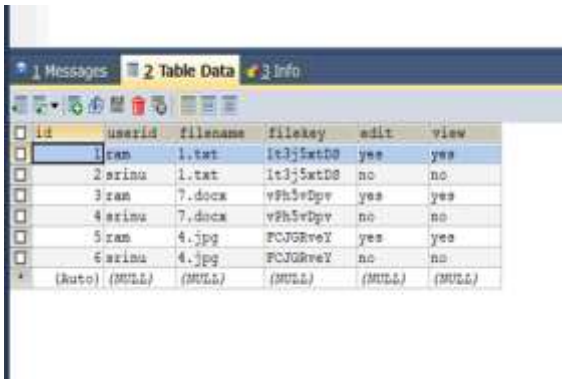

Welcome to prasad
Useful Links


Useful Links


Useful Links



Database Tables



VI. CONCLUSION

We presented for the first time a secure scheme fully based on attribute-based encryption to ensure both, the confidentiality and access control over data outsourced (in encrypted form) by data owners to the cloud and the fine-grained search control for data users when retrieving encrypted data from the cloud; we called this scheme FABECS. Through a formal analysis and experimentation, we proved the correctness and efficacy of FABECS to be used for storing, sharing and retrieval of documents in a cloud based environment. Furthermore, we provided for the first time Type-III constructions for CP-ABSE and DET-ABE as main building blocks of FABECS. This setting allows using more efficient pairing-friendly curves to achieve recommended security levels, as minimum of 128-bits. These constructions where detailed and their efficacy proved by means of experimentation, over the LISA benchmark for the retrieval task. Further work is focused in the efficiency aspect, as the results presented in this paper did not consider acceleration strategies. For example, parallelization at several levels is possible, besides the scheme is

friendly enough to be deployed using parallel patterns such as the manager-worker (for processing a group of attributes at a time) or data encryption (AES on GPUs). Also, as FABECS can be realized with other efficient pairing friendly curves, experimental evaluation could consider the Barreto- Lynn-Scott Curve (BLS) that is also being promoted to be used in practical applications.

FUTURE SCOPE

1. Adoption of Advanced Cryptographic Curves:
   Explore implementing FABECS using Barreto-Lynn-Scott (BLS) curves and other modern pairing-friendly curves for even stronger security and better performance.
2. Integration with Blockchain:
   Combine FABECS with blockchain technology to create a tamper-proof audit trail for file access, sharing, and modification events.Support decentralized cloud storage environments with smart contracts for attribute-based access control.
3. Enhanced Search Capabilities:
   Extend the search functionality from keyword-based search to semantic search using natural language processing (NLP) techniques.Implement fuzzy search capabilities to tolerate misspellings and partial matches during keyword queries.

REFERENCES

1. A. Bagherzandi, B. Hore, and S. Mehrotra, Search over Encrypted Data. Boston, MA, USA: Springer, 2011, pp. 1088–1093.
2. H. Pham, J. Woodworth, and M. A. Salehi, ‘‘Survey on secure search over encrypted data on the cloud,’’ Concurrency Comput. Pract. Exper., vol. 31, p. 1– 15, Apr. 2019.
3. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, ‘‘Searchable symmetric encryption: Improved definitions and efficient constructions,’’ in Proc. 13th ACM Conf. Comput. Commun. Secur., New York, 2006.
4. M. Zeng, H.-F. Qian, J. Chen, and K. Zhang, ‘‘Forward secure public key encryption with keyword search for outsourced cloud storage,’’ IEEE Trans. Cloud Comput., early access, Sep. 27, 2019.
5. S. Kamara, C. Papamanthou, and T. Roeder, ‘‘Cs2: A searchable cryptographic cloud storage system,’’ Microsoft Res., Redmond, WA, USA, Tech. Rep. MSR- TR-2011-58, May 2011.
6. W. Song, B. Wang, Q. Wang, Z. Peng, W. Lou, and Y. Cui, ‘‘A privacypreserved full-text retrieval algorithm over encrypted data for cloud storage applications,’’
   J. Parallel Distrib. Comput., vol. 99, pp. 14–27, Jan. 2017.
7. A. G. Kumbhare, Y. Simmhan, and V. Prasanna, ‘‘Designing a secure storage repository for sharing scientific datasets using public clouds,’’ in Proc. 2nd Int. workshop Data Intensive Comput. Clouds, 2011, pp. 31–40.
8. Z. Yang, J. Tang, and H. Liu, ‘‘Cloud information retrieval: Model description and scheme design,’’ IEEE Access, vol. 6, pp. 15420–15430, 2018.
9. H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, ‘‘CP-ABSE: A ciphertext-policy attribute-based searchable encryption scheme,’’ IEEE Access, vol. 7, pp. 5682–5694, 2019.
10. A. Sahai and B. Waters, ‘‘Fuzzy identity-based encryption,’’ in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.