International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/17
DOI: https://doi.org/10.5281/zenodo.19130625

EFFICIENT REVOCABLE MULTI-AUTHORITY ATTRIBUTE-BASED ENCRYPTION FOR CLOUD DATA SECURITY

[#1]**P. LAVANYA,** ***Assistant Professor,***
[#2]**GUNTUKU AVINASH,** ***B.Tech Student,***
[#3]**KANDULA SHYAMALA,** ***B.Tech Student,***
[#4]**GOPAGONI ASMITHA,** ***B.Tech Student,***
[#5]**MARKA DEEPIKA,** ***B.Tech Student,***
[#6]**LONARE THIRUPATHI,** ***B.Tech Student,***
Department of AIML,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: Secure cloud data storage, user identity, key generation/management, and multi-authority data storage and retrieval are all features of the decentralized access control system that we set up. In a multi-authority system, different authorities can view the same copy of the data, but only under certain rules. Cipher text-Policy Attribute-based Encryption (CP-ABE) is thought to be one of the best ways to control who can access data in the cloud because it gives data users more direct control over who can see their data. Still, because of the problem of attribute revocation, it is hard to quickly apply well-known CPABE strategies to cloud storage systems that control who can view data. In the proposed system, we are focused on revocable multi-authority schemes that use the CPABE algorithm to come up with an expressive, efficient, and revocable data access control scheme for multi-authority cloud storage systems that mirror data. A revocable multi authority CP-ABE plan is what we think should be used as the main way to set up the data access control system. Our method for revocating attributes includes data mirroring, forward security, and backward security.

Keywords: Access Control, Multi-Authority, CP-ABE, Attribute Revocation, Cloud Storage.

1. INTRODUCTION

Cloud computing is a state-of-the-art, meticulously planned method of storing data for several users in a safe and secure environment. One such use case for cloud computing is remote data storage in a shared repository. Using an online backup system instead of upgrading RAM can help businesses save money. It might help businesses and government bodies save money on data management. It is not their responsibility to ensure the availability of their own data centers.

A cloud storage provider is an alternative that they can consider when planning for data backup. The storage equipment is not mandatory for individuals or corporations to purchase. Instead of taking the chance of losing data in the event that user hardware or software fails, users may simply back up their information to the cloud. Although cloud storage is user-friendly, concerns about privacy and data security have been raised. Use of appropriate cryptography ensures the security of data transmissions hosted in the cloud.

The cloud is the best place to keep encrypted files after they have been encrypted. Data can be seen by anyone

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/17
DOI: https://doi.org/10.5281/zenodo.19130625

with the file and decoding skills. One of the most recent approaches to this issue is cloud computing, which relies on a large-scale, publicly-accessible, decentralized infrastructure. Users' privacy and security must always be protected. Using attribute-based encryption is a fantastic method for providing public cloud users with fine-grained access control services and ensuring that data users have complete control over their data. Two ABE methods that have been proven so far are Ciphertext Policy Attribute-based Encryption (CPABE) and Key Policy Attribute-based Encryption (KP-ABE). Combining access structures with decryption keys, KP-ABE systems assign unique names to ciphertexts according to their characteristics. The management of access keys and attributes is overseen by an official body. The registration office at the university, the HR division of a company, or some other entity could be the one with the final say. The owner of the data encrypts it using the specified permissions. A private key will be distributed to all participant. Data can be decrypted when its attributes fit the permission policies. In order to prevent authorized users from gaining access to sensitive system data, access control systems are designed. Who can access a system and when is determined by an access control policy or mechanism. Information regarding each login attempt is also recorded and stored by it.

Access control is another tool you can use to identify unauthorized users attempting to access your system. For the sake of your computer's security, it is vital. The cloud computing architecture relies on cloud storage. Users are able to securely store their files online with cloud storage. Data hosting makes it more difficult to control who has access to what information. Data owners have little faith in computers to manage access control, making it difficult to enforce strict permissions in cloud storage systems. Access privileges are managed via a decentralized way.

2. LITERATURE SURVEY

DAC-MACS: Data access control is an effective method for guaranteeing the security of cloud data when a number of individuals are responsible for managing a cloud storage system. Due to data outsourcing and unreliable cloud servers, many people are concerned about the security of their data stored on the cloud. Cloud storage systems either require a completely trustworthy cloud server or create several encrypted copies of the same data, rendering outdated access control mechanisms useless. Ciphertext-Policy Attribute-based Encryption (CP-ABE) allows you to restrict access to encrypted data. The features can't be controlled by just anyone, and the keys can't be kept in one place. Each of the numerous authorities in cloud-based storage systems is able to independently share data. Since decryption and cancellation do not function in multi-authority cloud storage systems, conventional CP-ABE methods cannot be used to control user access. In this research, we discuss DACMACS, an easy-to-use DACS that allows you to decrypt and revoke access to data stored in multi-authority cloud storage. An efficient multi-authority CP-ABE system with an attribute revocation and decoder is introduced. By employing this tactic, we can ensure the

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/17
DOI: https://doi.org/10.5281/zenodo.19130625

safety of all those involved. Based on our research and simulations, our DAC-MACS is fully secure and performs admirably within the security paradigm.

Dacc: Large-scale cloud-based population control systems Cloud computing provides an entirely novel approach to storing and retrieving data. You are not obligated to keep numerous encrypted versions of the identical data while using our technology. Our intention is to utilize the cloud to securely store encrypted files. The simplest approach to enhancing our model would be to include key distribution locations. Distributed Access Control in Clouds (DACC) is a method that we provide for assigning keys to users and data owners. KDC is limited in its ability to display record fields; it cannot display all of them. A single key is given to the owner rather than a set. The functionalities are identical for both the owners and the users. The data is encrypted with its properties before being saved to the cloud by the owner. Information kept in the cloud is accessible to those who meet specific requirements. When it comes to elliptic curve attribute-based encryption, we use bilinear pairings. This method discourages collaboration since it is impossible for two users to decipher encrypted data. With DACC, you can quietly terminate a cloud service without informing the users. We demonstrate that compared to competing models and methodologies, our model requires significantly less computing power, data transfer, and storage space.

3) Cloud Data access control is a helpful method for guaranteeing the security of data stored in the cloud, especially when it allows numerous users to access the data in a clear and effective manner. Because of data outsourcing and unreliable cloud services, it is now difficult to govern who can access what in a cloud storage system. When it comes to protecting sensitive information kept in the cloud, ciphertext-policy attribute-based encryption (CP-ABE) is a top choice. It provides data owners with greater direct control over the visibility of their data. However, the present CP-ABE approaches make direct control over who can access data in cloud storage systems difficult due to the attribute revocation issue. An efficient, expressive, and reversible approach to managing data access in distributed databases is proposed in this research. In these systems, various levels of authority can bestow unique features. Our primary security measure is a revocable multi-authority CP-ABE system, which we endorse and use. Having forward and reverse security is made straightforward by our attribute revocation approach. Compared to earlier efforts that relied on the random oracle model, our suggested data access control mechanism is more effective and safe, according to our research and simulation results.

3. SYSTEM DESIGN

A demonstration of power. With the hierarchical structure of MABKS, the CA can delegate the time-consuming processes of generating intermediate secret keys and verifying user certificates to a large number of AAs. Thus, the CA's time spent in front of the computer will decrease. At the at-level, you can do search queries. MABKS generates the necessary secret key to secure a file's file key while indexing, not beforehand. Earlier CP-

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/17
DOI: https://doi.org/10.5281/zenodo.19130625

ABKS systems were different from this. Users and data owners who use the cloud can utilize MABKS technology to limit access to encryption for individual files and to retrieve ciphertext through keyword searches.

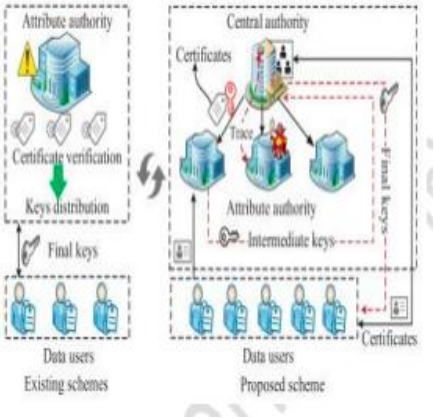

Fig 1: Architecture

A. AA (Attribute Authority)

It verifies the user's identity and provides the CA with an intermediary key for verified users. Concurrently running AAs can confirm an individual's identity. According to AA, the data owner receives a notification with the user's username every time the user views the data.

B. CA (Central Authority)

The generation and storage of public and private keys are within its purview. After receiving an intermediate key from the AAs, it uses it to generate a secret key. It will be possible for CA to monitor any suspicious activity while AA's identification is being finalized.

C. Data Owner (Owner)

A symmetric encryption user who hides data. The owner is required by the regulations to encrypt the symmetric key using a public key from the CA. The next step is for the owner to upload the encrypted data together with the spare key to the cloud.

D. User

The user possesses both the set of characteristics and the associated secret key. While encrypted content in the cloud is easily accessible, decryption is conditional on the user's attribute set matching the requirements for accessing encrypted data.

E. Cloud Server

An accessible and user-friendly method of transferring encrypted data to the cloud is provided. Unencrypted data can still be accessed.

4. SYSTEM ANALYSIS

An novel threshold multi-authority CP-ABE access control system (TMACS) is suggested by the author as a means to enhance the security of data stored in the cloud. Under this setup, every AA shares a master key and collaborates to manage all attributes. In the (t, n) threshold secret sharing protocol, an AA can generate a secret key by exchanging threshold secrets with any of the t other AAs. TMACS guarantees that not a single AA will falter or be exposed. This research proves that the author has used a safe and sound approach to access control. It can swiftly determine the appropriate values for (t, n) to ensure the safety of TMACS when less than t authorities have been compromised. With less than t active authorities, it can rapidly determine the optimal values for (t, n) to fortify the system.

Combine TMACS with the tried-and-true multi-authority approach to create a superior hybrid approach. This approach considers the system's safety, external characteristics, and recovery capability. Issues with DAC-MACS and the attribute cancelation process are discussed.

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/17
DOI: https://doi.org/10.5281/zenodo.19130625

The only way for a banned user to access restricted content is for them to work with the cloud provider to obtain enough ciphertext update keys. Because of this, they can use the author-recommended attack technique to change the new ciphertext to the old one. One risky aspect of DAC-MACS is the bidirectional re-encryption that occurs when the ciphertext is updated. An adversary who gains access to the CUKs can exploit this vulnerability to re-encrypt the ciphertext that lies between the two versions. Even though privilege control has to know the user's identity, the author's proposed solutions allow for detailed permission management without compromising user privacy. Among its many advantages, this system's ability to deal with up to N2 authority compromises makes it ideal for usage in Internet-based cloud computing settings.

Cloud storage systems are kept secure and usable by AnonyControl, according to researchers. Despite having the same degree of security as the AnonyControl, the AnonyControl-F incurs higher communication overhead during the 1-out-of-n oblivious transfer.

A revocable multi-authority CPABE system that permits attribute cancellation was introduced by the author to efficiently control data access in multi-authority cloud storage situations. Additionally, the author demonstrated the strategy's safety by employing the random oracle model. Many well-known platforms, including social media and cloud storage companies, are compatible with revocable CPABE, which has been hailed as a secure solution. In order to facilitate secure information sharing amongst dynamic teams operating in an often murky cloud environment, the authors developed Mona. With Mona, team members may securely exchange files without revealing their identities to third parties in the cloud. Making new acquaintances to replace old ones is something Mona excels at as well. In instance, you can remove a user from the system without requiring other users to modify their private keys by using a public revocation list. This opens the door for new users to independently access encrypted data kept in the cloud. Both the cost of storing and the cost of encrypting are constant. According to the results, the technique that has been suggested is both safe and successful.

5. RESULTS

Fig 2: Home Page

Fig 3: Uploaded File Details

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/17
DOI: https://doi.org/10.5281/zenodo.19130625

Fig 4: User Request Page

6. CONCLUSION

The development of a fully operational MABKS system was prompted by this research. Many authorities would benefit from this design, and it would also solve the performance issue that arises in cloud systems when there is just one point of failure. Using the MABKS system, we can additionally monitor malicious AAs (to prevent collusion attacks, for instance) and modify properties (to prevent unauthorized access using outdated secret keys, for instance). To demonstrate the operation of the system's selective security, the decisional q-parallel BDHE and DBDH assumptions were utilized in conjunction with the selective-matrix and selective-attribute models. We compared the approach to conventional ABKS methods and discovered that it significantly reduced compute and storage costs. Fuzzy, subset, and conjunctive keyword searches, all of which carry more than one meaning, is outside the MABKS system's capabilities. In the future, MABKS intends to construct an index structure that is both practical and adaptable, allowing it to fulfill a range of search requirements.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Adv. Cryptol.—EUROCRYPT 2005. New York, NY, USA: Springer, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Security Privacy 2007, 2007, pp. 321–334.

[4] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 99–112.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. 5th ACM Symp. Inf., Comput. Commun. Security 2010, 2010, pp. 261–270.

[6] S. S. M. Chow, "A framework of multi-authority attribute-based encryp-tion with outsourcing and revocation," in Proc. 21st ACM Symp. Access Control Models Technol., 2016, pp. 215–226.

[7] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[8] C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan, "Arbitrary-state attribute-based encryption with dynamic membership," IEEE Trans. Comput., vol. 63, no. 8, pp. 1951–1961, Aug. 2014.

[9] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective data access control for multiauthority cloud

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/17
DOI: https://doi.org/10.5281/zenodo.19130625

storage systems," IEEE Trans. Inf. Forensics Security, vol. 8, no. 11, pp. 1790–1801, Nov. 2013.

[10] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in Proc. 2011 IEEE 10th Int. Conf. Trust, Security Privacy Comput. Commun., 2011, pp. 91–98.