IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 6.252

Volume 2, Issue 1, April 2022

Cloud-Based Data Security with Efficient Revocable Multi-Authority Attribute Encryption

E Ramkrishna[1] and Dr. Narender Kumar[2]
Research Scholar, Department of Computer Science and Engineering[1]
Supervisor, Department of Computer Science and Engineering[2]
NIILM University, Kaithal, Haryana, India

Abstract*: For safe data storage in clouds, we deployed a decentralized access control system that provides user identification, key creation and administration, and multi-authority data storage and retrieval. In a multi-authority system, many authorities may access the same data copy, but only under different attribute regulations. Ciphertext-Policy Attribute based Encryption (CP-ABE) is regarded as one of the finest methods for data access control in cloud storage because it gives data owners more direct control over access limits. However, due to the attribute revocation issue, directly adapting known CPABE approaches to data access control for cloud storage systems is difficult. We are largely focusing on revocable multi authority scheme with the aid of CPABE algorithm in the recommended system to construct an expressive, effective, and revocable data access control scheme for multi-authority cloud storage systems with data mirroring. We explicitly propose and employ a revocable multiauthority CP-ABE scheme as the basic techniques for developing the data access control system. Our attribute revocation method includes data mirroring, forward security, and reverse security.*

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

I. INTRODUCTION

Cloud computing is a cutting-edge technique that has been meticulously developed to safely and securely store data for a large number of users. Users of cloud computing have the option of remotely storing data in a shared repository. Businesses can save money on memory upgrades by switching to an online backup system. Businesses and government agencies might use it to reduce data management costs. They can outsource data backups to a cloud storage provider rather than maintain their own data centers. It is not necessary for an individual or company to purchase the storage devices. Instead of risking data loss if their hardware or software fails, users may simply back up their files to the cloud. Data security and privacy concerns have been raised despite the convenience of cloud storage. The correct kind of cryptography is employed to keep cloud-based data exchanges secure.

Once a file has been encrypted, it must be stored on the cloud for safekeeping. The information can be viewed by anyone who has the file and understands how to decode it. Cloud computing, which uses a large, open, distributed system, is one of the newest solutions to address the issue. Users' personal information and security must always be protected. One of the most effective methods of providing granular access control services in public clouds and ensuring that data users have direct control over their data is to employ attribute-based encryption. Key Policy Attribute-based Encryption (KP-ABE) and Ciphertext Policy Attribute-based Encryption (CPABE) are just two of the many ABE techniques that have been demonstrated so far. Decryption keys and access structures are combined in KP-ABE systems, and ciphertexts are given unique names based on their properties. Attributes and access keys are administered by an authoritative body. The office of registration at a university, human resources at a business, or some other entity may serve as the authority. The data's owner encrypts it in accordance with the established permissions.

Everyone will be given their own private key. When the data's characteristics coincide with the authorization policies, the data can be decrypted. The purpose of access control mechanisms is to limit access to sensitive system data to authorized users only. An access control policy or process determines which users can access a system and under what conditions. Additionally, it logs and stores information about each login attempt. Whoever is trying to gain unauthorized access to your system can also be identified with the help of access control. It's crucial to your computer's

DOI: 10.48175/568

security. Cloud storage is a crucial component of the cloud computing infrastructure. Cloud storage allows the data's owners to safely keep their files online. Controlling access to data is complicated by data hosting and access services. Data owners can't rely on computers to handle access control, thus it's difficult to regulate who has access to what in cloud storage systems. Access permissions are managed in a decentralized manner.

II. LITERATURE SURVEY

1) DAC-MACS: Controlling who can access what in a cloud storage system when numerous parties are responsible Data access control is a useful tool for ensuring the security of cloud data. However, data outsourcing and unreliable cloud servers have brought forth a debate over who has access to what in cloud storage systems. Because cloud storage systems either make numerous encrypted copies of the same data or require a cloud server that can be trusted completely, access control measures that used to work are no longer useful. To restrict access to encrypted data, one option is to use Ciphertext-Policy Attribute-based Encryption (CP-ABE). The keys must be dispersed across the system, and all of the characteristics must be managed by a dependable authority. In cloud-based storage systems, many authorities exist, each with the ability to independently distribute characteristics. Due to the ineffectiveness of decryption and cancellation in multi-authority cloud storage systems, traditional CP-ABE methods cannot be employed to regulate user access. In this paper, we discuss DACMACS (Data Access Control for Multi-Authority Cloud Storage), a DACS that provides efficient decryption and revocation of access. We present a new multi-authority CP-ABE system that is both decoder and attribute revocation efficient. Safety can be provided in both directions using this approach. Research and simulations show that our DAC-MACS is very efficient and completely secure within the context of the security paradigm.

2) Dacc: Large-scale population control clouds We provide a novel approach to cloud computing for the storage and retrieval of information. Using our strategy, we eliminate the need for storing several encrypted versions of the same information. Our plan for secure data storage is to maintain encrypted files in the cloud. The most notable improvement in our model is the incorporation of critical distribution locations. To distribute keys to data owners and users, we recommend the DACC (Distributed Access Control in Clouds) approach. KDC is authorized to disclose some but not all of the records' fields. One key, rather than a set, is provided to the owner. The characteristics of the owners and the users are same. The owner stores the data on the cloud after encrypting it with the data's properties. Information stored in the cloud can be accessed by users who match certain criteria. We employ bilinear pair-based attribute-based encryption on elliptic curves. Because it's impossible for any two users to decode data that neither of them is authorized to see, the approach prevents anyone from cooperating. Using DACC, you can stop a cloud service without telling everyone who uses it. We demonstrate that compared to competing models and approaches, ours requires less data transmission, processing, and storage space.

3) Cloud storage with transparent, efficient, and multi-user data access control Data access control is a useful tool for ensuring the security of cloud data. Data outsourcing and unreliable cloud services have made it difficult to manage who has access to what in a cloud storage system. One of the most effective methods of limiting access to data stored in the cloud is Ciphertext-Policy Attribute-based Encryption (CP-ABE), which offers data owners more direct control over access constraints. However, it is challenging to use preexisting CP-ABE methods directly to manage who has access to data in cloud storage systems due to the issue of attribute revocation. In this research, we present a reversible, expressive, and efficient approach to data access control for distributed databases. Multiple authorities exist in these systems, with the ability to independently issue characteristics. We advocate for and implement a multi-authority CP-ABE scheme that can be revoked as the primary approach for securing access to sensitive data. Our attribute revocation technique makes it simple to have both forward and reverse security. Our proposed data access control mechanism outperforms previous attempts based on the random oracle model in both efficiency and security, as demonstrated by our analysis and simulation findings.

III. SYSTEM DESIGN

A demonstration of authority. Because of the hierarchical nature of the MABKS system, many AAs can help the CA with the tedious tasks of authenticating user certificates and generating intermediate secret keys. As a result, less time will be spent on the computer by the CA. You can conduct search queries at the at-level. In contrast to previous CP-

DOI: 10.48175/568

ABKS systems, the secret key required to secure a file's file key is generated as part of the indexing process rather than beforehand in MABKS. Cloud customers, such as data owners and users, can leverage the MABKS system to recover ciphertext via keyword searches and regulate encryption access on a per-file basis.

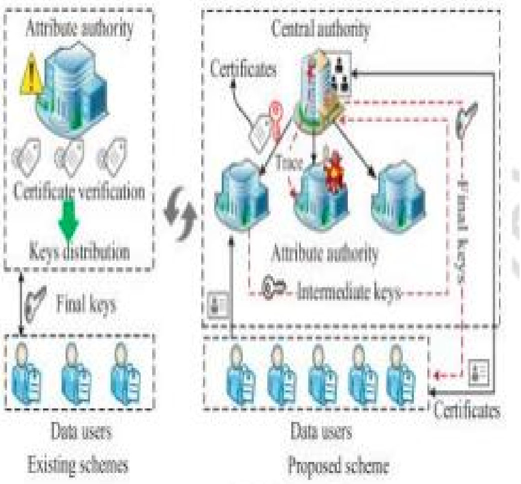


Fig 1:Architecture

A. AA (Attribute Authority)

It takes care of ensuring sure the user is legitimate and provides the CA with an intermediary key for verified users. Running AAs simultaneously can verify an individual's identity. According to AA, a notification containing the user's username is delivered to the data's owner whenever the user reads the data.

B. CA (Central Authority)

It generates both private and public keys and is responsible for their security. With the help of the intermediate key it obtained from the AAs, it generates a secret key. While AA's identity is being verified, CA will be able to keep an eye on his or her potentially criminal activity.

C. Data Owner (Owner)

One who conceals data via symmetric encryption. According to the rules, the owner must encrypt the symmetric key using a public key obtained from the CA. The owner then uploads the encrypted data together with the symmetric key to the cloud.

D. User

Both the characteristic set and the associated secret key are held by the user. Cloud-based encrypted content is readily available to the user, but can only be decrypted if the user's attribute set satisfies the access rules for encrypted data.

E. Cloud Server

It provides a universally accessible and usable method for sending encrypted data to the cloud. Information that has been encrypted can be accessed by anyone..

IV. SYSTEM ANALYSIS

In order to improve security for data stored in the cloud, the author proposes a novel threshold multi-authority CP-ABE access control system (TMACS) in which all AAs manage the entire set of attributes jointly and share the master key. An authorized user can generate a secret key by exchanging threshold secrets with any of the t AAs in the (t, n) threshold secret sharing protocol. Therefore, TMACS guarantees that there will be no slowdown or vulnerability in any one AA. The analysis demonstrates the validity and security of the author's approach to access control. When fewer than t authorities have been compromised, it can quickly identify the proper values for (t, n) to secure TMACS, and when fewer than t authorities are still operational, it can quickly find the right values for (t, n) to make the system strong. When the traditional multi-authority scheme is combined with TMACS, a hybrid scheme is created that is more practical. This strategy considers safety, external attributes, and system resilience. The shortcomings of DAC-MACS are discussed, as is the mechanism of attribute cancellation. The only way a banned user can access restricted content is if they cooperate with the cloud service provider to obtain enough ciphertext update keys to apply the author-suggested attack algorithm to convert the new-version ciphertext to the old-version one. An insecure aspect of DAC-MACS is the use of bidirectional re-encryption in the ciphertext updating procedure. This vulnerability allows an attacker to re-encrypt the ciphertext between the old and new versions if they obtain the CUKs. Although the user's identification is required for privilege control, the author's proposed techniques nevertheless allowed for granular permission management without compromising user privacy. In Internet-based cloud computing settings, the fact that this system can tolerate up to N2 authority compromises is a major plus. Researchers found that AnonyControl successfully maintains the safety and efficiency of cloud storage systems. The AnonyControl-F receives the same level of security as the AnonyControl, despite incurring more communication overhead during the 1-out-of-n oblivious transfer. The author demonstrated a multi-authority CPABE scheme that may be revoked, allowing for effective attribute cancellation and facilitating an effective method of regulating access to data in multi-authority cloud storage environments. The author additionally demonstrated the technique's security in the context of the random oracle model. Revocable CPABE has been cited as a secure method compatible with a wide variety of popular platforms, including social media sites and cloud storage services. The authors created Mona, a safe platform enabling dynamic groups to communicate data in an unpredictable cloud environment. Mona users can safely communicate data with one another within their team without revealing their identities to the cloud. Mona is also skilled at replacing old acquaintances with fresh ones. In particular, a public revocation list allows a user to be removed without requiring other users to change their private keys. This means that cloud-stored files encrypted by new users can be opened without assistance. The cost of computing encryption is always the same as the cost of storage. The analysis demonstrates that the proposed approach satisfies the needs for both effectiveness and safety.

V. RESULTS

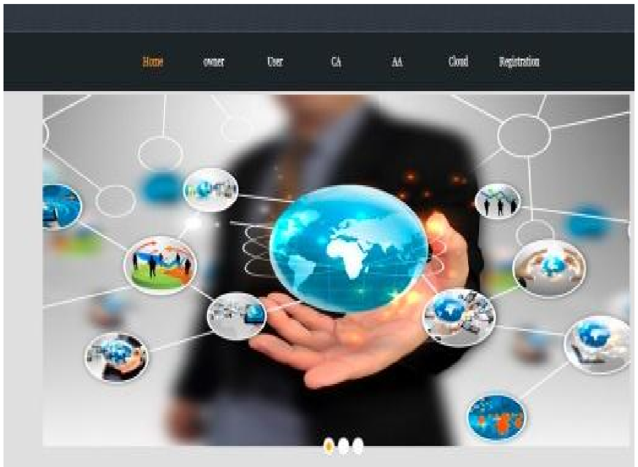
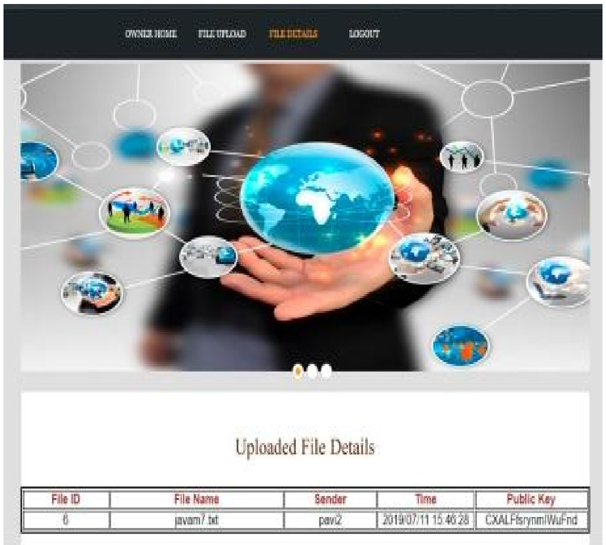


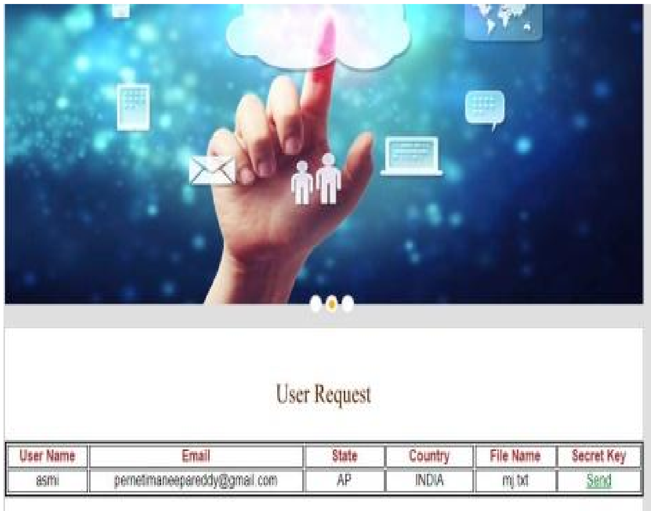
Fig 2: Home Page



Uploaded File Details

File ID	File Name	Sender	Time	Public Key
6	javam7.txt	pavi2	2019/07/11 15:46:28	CXALFfsrynmIWuFnd

Fig 3: Uploaded File Details



User Request

User Name	Email	State	Country	File Name	Secret Key
asmi	pemetimaneepareddy@gmail.com	AP	INDIA	mj.txt	Send

Fig 4: User Request Page

VI. CONCLUSION

Through this research, we were able to develop a practical MABKS system. This infrastructure would alleviate the single-point performance bottleneck in cloud systems while also supporting many authorities. Furthermore, the MABKS system enables us to monitor harmful AAs (for instance, to prevent collusion attacks) and alter properties (for instance, to prevent unauthorized entrance using old secret keys). Next, we demonstrated the system's selective security using the selective-matrix and selective-attribute models, as well as the decisional q-parallel BDHE and DBDH assumptions. We analyzed the system's performance and demonstrated the significant savings in compute and storage expenses compared to traditional ABKS methods. Search queries with multiple meanings, such as conjunctive keyword search, fuzzy search, subset search, etc., are not supported by the MABKS system. MABKS plans to develop an efficient and adaptable index structure in the future so that it may fulfill a variety 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 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

DOI: 10.48175/568