Multi Authority Access Control Mechanism over Encrypted Cloud Data

[1]Chittikanna Prajwala [2]B.Anvesh kumar

[12] Vaageswari College of Engineering, karimnagar, Telangana, India

[1]nethraprajwala@gmail.com [2]anveshboddupalli@gmail.com

***Abstract*—** Data security and usability in the cloud are mutually reliant on the implementation of searchable encryption (SE). Achieving both keyword-based retrieval and fine-grained access control at the same time, the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) system makes use of Ciphertext-Policy Attribute-Based Encryption (CP-ABE). However, in current CP-ABKS schemes, the sole attribute authority must perform the time-consuming and resource-intensive tasks of verifying users' certificates and disseminating secret keys. Furthermore, in distributed cloud systems, this causes a single point of failure. In light of these constraints, we introduce a secure Multi-authority CP-ABKS (MABKS) system in this study, which can reduce the computational and storage demands placed on devices with constrained resources in cloud-based environments. In addition, the MABKS framework is augmented to permit tracking the origin of malicious attributes and updating these attributes. In both the selective-matrix and selective-attribute models, our thorough security analysis demonstrates that the MABKS system is selectively secure. The effectiveness and usefulness of the MABKS system in real-world applications are shown by our experimental results utilising real-world datasets..

1.INTRODUCTION

Cloud computing has evolved into a sophisticated method of storing information for a wide variety of users. The cloud is a distant server where users can store data. A remote backup system is a cutting-edge method that reduces the expense of adding extra RAM to a computer system. It helps businesses and government bodies save money on data management costs. In lieu of managing their own own data centres, they can instead remotely extract data backups to third-party cloud storage providers. The storage devices are not necessary for an individual or a business to have. As an alternative, they can back up their data to the cloud and archive it so that they don't lose any information in the event of a system failure like hardware or software malfunction. While cloud storage offers greater adaptability, concerns about the safety and privacy of data that is transferred to a third party have grown in recent years.

A suitable cryptographic approach is employed to ensure the security of cloud-based data transactions. The file's owner is responsible for both the encryption and subsequent cloud storage. If a third party downloads the file and has the key needed to decrypt the encrypted file, they can view the record. In order to solve the issue As a relatively new field of study, cloud computing features a massive, open, and decentralised network of computers and other nodes. Users' information and personal privacy must be safeguarded.

To ensure data owners have direct control over their data and to provide a fine-grained access control service, attribute-based encryption is one of the most suitable systems for data access control in public clouds. To date, numerous ABE schemes have been developed, and they can be broadly classified into two groups: Key Policy Attribute-based Encryption (KP-ABE) and Ciphertext Policy Attribute-based Encryption (CP-ABE) (CPABE). KP-ABE systems have an authority in charge of attribute management and key distribution, and ciphertexts that can be decrypted are tagged with unique sets of attributes. The relevant office or department could be the HR division of a firm, the registrar's office at a school, or any other similar entity. The data is encrypted and the access policies are set by the data owner. An individual's unique secret key will be generated based on their profile. If the data's characteristics fit the access policies, the user can decrypt it.

Only authorised users can view the system's data, and this is what access control mechanisms are for. A system's level of accessibility is managed by means of an access control policy or set of procedures. In addition, it keeps track of and logs any and all login attempts. Unauthorized users who try to log in to a system might be uncovered with the use of access control. When it comes to keeping your data safe online, this process is crucial. When it comes to cloud computing, cloud storage is king. Owners of data can take advantage of Cloud Storage's services to store their information in the cloud. Data hosting and data access services present a significant challenge to data access control schemes. In cloud storage systems, data access control is complicated since data owners do not fully trust the cloud servers and can no longer rely on the servers to perform access control. To address this issue, we propose a system for decentralised control of data access..

2.LITERATURE SURVEY

2.1. DAC-MACS: Effective data access control for multi-authority cloud storage systems

AUTHORS: K. Yang, X. Jia, and K. Ren

Limiting access to certain individuals is a crucial aspect of keeping cloud data secure. However, due to data outsourcing and unreliable cloud servers, the challenge of data access control is a real issue for cloud storage solutions. Traditional access control mechanisms are not applicable to cloud storage systems because they either produce numerous encrypted copies of the same data or require a completely trusted cloud server. Ciphertext-Policy Attribute-based Encryption is a promising approach to controlling access to encrypted data. In such a configuration, all system attributes and key distribution must be under the strict control of a trustworthy organisation. Attributes can be issued independently by many authorities in cloud storage systems. For multi-authority cloud storage systems, however, conventional CP-ABE schemes are not a viable option for access control due to the inefficiency of decryption and revocation. Data Access Control for Multi-Authority Cloud Storage (DAC-MACS) is a mechanism for controlling access to data in the cloud with a focus on decryption and revocation, and it is the subject of this study. For this reason, we develop a new multi-authority CP-ABE scheme that features fast decryption and an equally speedy attribute revocation strategy that safeguards data in both directions. Analysis and simulation results demonstrate that our DAC-MACS is highly effective and provably secure in accordance with the security model..

2.2. Dacc: Distributed access control in clouds

AUTHORS: S. Ruj, A. Nayak, and I. Stojmenovic

We introduce a novel method for handling data in the cloud. Our solution eliminates the need to store several encrypted copies of the same data. Our system encrypts data before storing it in the cloud to prevent unauthorised access (without being able to decrypt them). Our model's main innovation is the way it accounts for key distribution nodes (KDCs). The DACC (Distributed Access Control in Clouds) approach, which proposes the use of key distribution centres (KDCs) to issue access keys to data owners and users, is one solution to this problem. On occasion, KDC may provide access to specific fields in all files. This means that from now on, each person needs to remember only one key. Owners and users are each given their own set of characteristics. Owner-added encryption is used for cloud-based data storage. Anyone with the right set of skills can access the data stored in the cloud. Our attribute-based encryption system relies on elliptic curve bilinear pairings. Since it is impossible for two users to jointly decode information to which they each only have partial access, the system is collusion-proof. In addition to facilitating the deletion of users, DACC also permits the continued usage of revoked keys within preexisting cloud environments. We show that our method has lower communication, computation, and storage overheads compared to existing models and schemes.

2.3. Access control for multi-authority cloud storage that is expressive, efficient, and reversible

By K. Yang and X. Jia

Limiting access to certain individuals is a crucial aspect of keeping cloud data secure. Because of data outsourcing and unreliable cloud servers, it can be difficult to regulate who has access to what in a cloud storage system. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is one of the best solutions for data access control in cloud storage because it gives data owners more direct control over access policies. However, existing CP-ABE techniques pose a challenge when applied directly to data access control for cloud storage systems due to the attribute revocation problem. In this study, we develop an expressive, efficient, and reversible mechanism for data access control in cloud storage environments where multiple authorities coexist and can issue attributes independently of one another. We propose a revocable multi-authority CP-ABE scheme as the foundational approaches for developing a secure data access control system. Our revoked attributes technique provides strong forward and backward security. To prove the safety and efficacy of our proposed data access control method in the random oracle model, we analyse and simulate it.

3.PROPOSED SYSTEM

Architecture with several levels of authority. For the first time, the MABKS system's hierarchical structure allows numerous AAs to perform time-consuming user certificate verification and intermediate secret key generation on behalf of the CA, minimising the CA's computing requirements. At the file level, keywords can be searched. MABKS differs from traditional CP-ABKS methods in that the secret key required to encrypt a file's file key is integrated inside the indexing process rather than being performed separately. [4], [5], [12] This means that cloud clients (such as data owners and users) can use the MABKS system to perform keyword-based ciphertext retrieval as well as file-level fine-grained encryption access control.

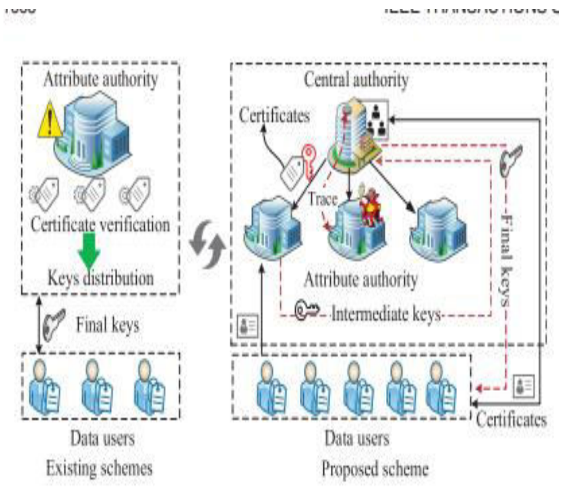


Fig 1:Architecture

A. AA (Attribute Authority) It is in charge of the user validity verification procedure, as well as transmitting an interim key to the CA for legitimately validated users. AAs can undertake user validity verification at the same time. When a user accesses any sort of data, AA notifies the data's owner via a message specifying the user's username..

5.RESULTS AND DISCUSSIONS

B. CA (Central Authority) It is in charge of producing secret and public keys. It produces a secret key based on the intermediate key received from AAs. CA, being a critical component of the system, has the ability to track AA misconduct during the user validity verification procedure..

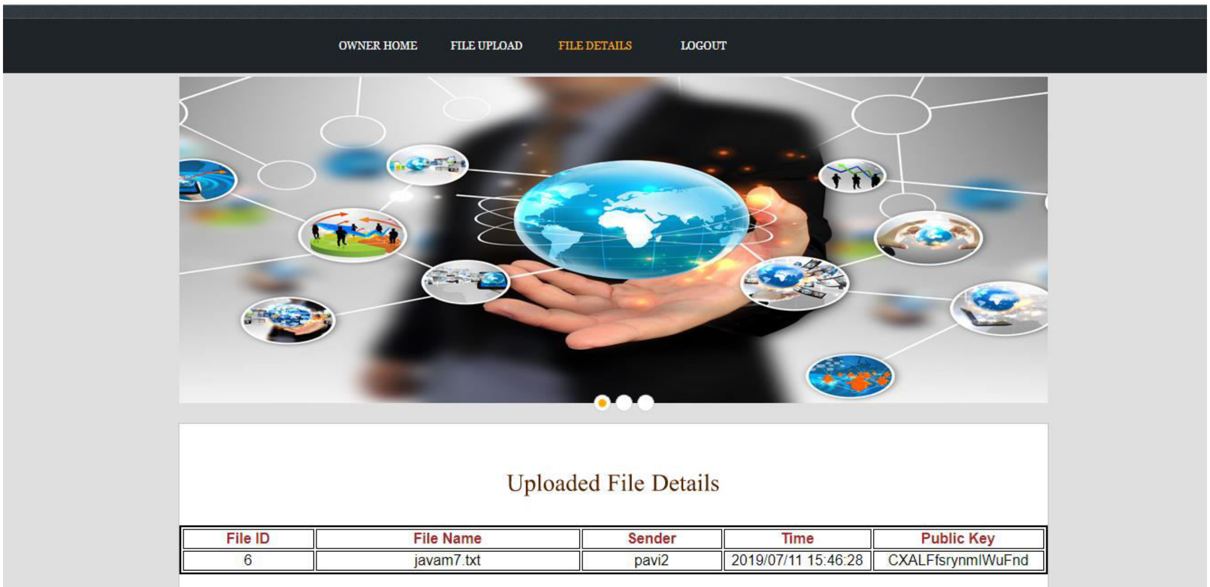
C. Data Owner (Owner) A person who uses a symmetric encryption algorithm to encrypt data. The policy also requires the owner to encrypt the symmetric key using a public key obtained from the CA. Owner then uploads this encrypted symmetric key and data to the cloud.

D. User A user is associated with a set of qualities as well as a secret key. The user can readily obtain encrypted data from the cloud, but he can only decode it if his/her attribute set satisfies the access policy relating to encrypted data..

E. Cloud Server

It creates a public, global infrastructure where users can store encrypted data. The encrypted information is available for download by anyone.

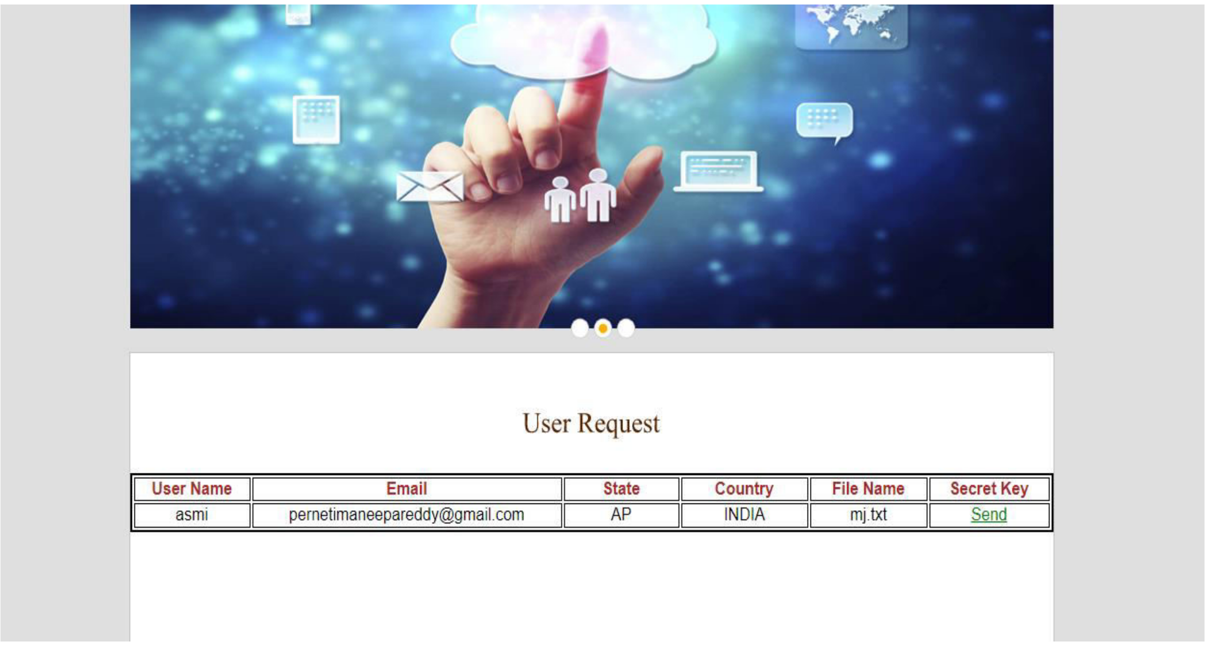
Fig 2:Home Page



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	pernetimaneepareddy@gmail.com	AP	INDIA	mj.txt	Send

Fig 4:User Request Page

6.CONCLUSION

We propose a robust MABKS solution that can cooperate with many authorities to stop a single node from dragging down the overall performance of a cloud system. As an added bonus, the new MABKS system allows for the alteration of attributes and the monitoring of malicious AAs (for the avoidance of collusion attacks, for instance) (e.g., to avoid unauthorised access using outdated secret keys). Then, using decisional q-parallel BDHE and DBDH models, we demonstrated the system's selective security. We also ran an efficiency analysis of the system, showing that it is more cost-effective than previous ABKS approaches while maintaining or even improving performance. One major drawback of the MABKS system is that it cannot process queries that make use of more than one search term (conjunctive keyword search, fuzzy search, subset search, etc.). Future work on the MABKS system will focus on improving its index construction so that it is both powerful and flexible enough to meet a variety of search needs.

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 revo-cation 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.