Journal of Engineering Sciences

Vol 13, Issue 06, JUNE /2022

ISSN NO:0377-9254

Multi Authority Access Control Mechanism over Encrypted Cloud Data

G.Tirumala1,P. Srishita Reddy2 , G. Sivani3 , K. Gayathri4, N. Vishnu vardhan Reddy5
1Assistant professor, Department of CSE, VEC Engineering College,kavali. 2,3,4,5 Students, Department of CSE, VEC Engineering College,kavali.

ABSTRACT—Cloud stockpiling encourages the two people and ventures to cost adequately share their information over the Internet. However, this additionally brings troublesome difficulties to the entrance control of shared information since not many cloud servers can be completely trusted. Security and usability in the cloud can be achieved through the use of Searchable Encryption (SE). Encryption and access control can be achieved at the same time using Ciphertext Policy Attribute-Based Encryption (CP-ABE), the Ciphertext Policy Attribute-Based Keyword Search (CP-ABKS) method. However, in existing CP-ABKS schemes, the single attribute authority is entrusted with the costly tasks of verifying user certificates and distributing secret keys. As a result, distributed cloud systems have a single point of failure. A secure Multi-Authority CP-ABKS (MABKS) solution is presented in this study to solve these restrictions and reduce the computational burden on resource-limited devices in cloud systems. Malicious attribute authority tracing and updating are now supported by the MABKS system. The MABKS system has been found to be selectively secure in both selective-matrix and selective-attribute models, according to our in-depth security research. The MABKS system's efficiency and utility have been demonstrated through our experiments with real-world datasets..

***index Terms*—Access control, cloud storage, multiauthority ciphertext-policy attribute-based encryption (CP-ABE), public update, revocation.**

1.INTRODUCTION

Now a day's cloud computing is an intelligently developed technology to store data from number of client. Cloud computing allows users to remotely store their data over cloud. Remote backup system is the progressive technique which minimizes the cost of implementing more memory in an organization. It helps government agencies and enterprises to reduce financial overhead of data management. They can extract their data backups remotely to third party cloud storage providers than maintaining their own data centres. An individual or an organization does not require purchasing the storage devices. Instead they can store their data to the cloud and archive data to avoid information loss in case of system failure like hardware or software failures. Cloud storage is more flexible, but security and privacy are available for the outsourced data becomes a serious concern.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must after encryption of the file, store to the cloud. If a third person downloads the file, they can view the record if they had the key which is used to decrypt the encrypted file. To overcome the problem Cloud computing is one of the emerging technologies, which contains huge open distributed system. It is important to protect the data and privacy of user.

Attribute-based Encryption is one of the most suitable schemes for data access control in public clouds for it can ensures data owners direct control over data and provide a fine-grained access control service. Till now, there are many ABE schemes proposed, which can be divided into two categories; Key Policy Attribute-based Encryption (KP-ABE) as well as Ciphertext Policy Attribute-based Encryption (CPABE). In KP-ABE schemes, decrypt keys are combined with access structures and in ciphertexts it is labeled with special attribute sets, for attribute management and key distribution an authority is responsible. The authority may be the human resource department in a company, the registration office in a university, etc. The data owner defines the access policies and encrypts the data according to the defined policies. Every user will be issued a secret key reflecting its attributes. A user can decrypt the data whenever its attributes match the access policies.

Access control methods ensure that authorized user access data of the system. Access control is a policy or procedure that allows, denies or restricts access to system. It also monitors and record all attempts made to access a system. Access Control can also identify unauthorized users attempting to access a system. It is a mechanism which is very much important for protection in computer security. The Cloud storage is a very important service in cloud computing. The Cloud Storage offers services for data owners to host their data over cloud environment. A big challenge to data access control scheme is data hosting and data access services. Because data owners do not completely trust the cloud servers also they can no longer rely on servers to do access control, so the data access control becomes a challenging issue in cloud storage systems. Therefore the decentralized data access control scheme is introduced.

2.LITERATURE SURVEY

1) DAC-MACS: Effective data access control for multi-authority cloud storage systems

Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a promising technique for access control of encrypted data. It requires a trusted authority manages all the attributes and distributes keys in the system. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently. However, existing CP-ABE schemes cannot be directly applied to the access control for multi-authority cloud storage systems, due to the inefficiency of decryption and revocation. In this paper, we propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multi-authority CP-ABE scheme with efficient decryption and also design an efficient attribute revocation method that can achieve both forward security and backward security. The analysis and the simulation results show that our DAC-MACS is highly efficient and provably secure under the security model.

2) Dacc: Distributed access control in clouds

We propose a new model for data storage and access in clouds. Our scheme avoids storing multiple encrypted copies of same data. In our framework for secure data storage, cloud stores encrypted data (without being able to decrypt them). The main novelty of our model is addition of key distribution centers (KDCs). We propose DACC (Distributed Access Control in Clouds) algorithm, where one or more KDCs distribute keys to data owners and users. KDC may provide access to particular fields in all records. Thus, a single key replaces separate keys from owners. Owners and users are assigned certain set of attributes. Owner encrypts the data with the attributes it has and stores them in the cloud. The users with matching set of attributes can retrieve the data from the cloud. We apply attribute-based encryption based on bilinear pairings on elliptic curves. The scheme is collusion secure; two users cannot together decode any data that none of them has individual right to access. DACC also supports revocation of users, without redistributing keys to all the users of cloud services. We show that our approach results in lower communication, computation and storage overheads, compared to existing models and schemes.

3) **Expressive, efficient and revocable data access control for multi-authority cloud storage**

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

3.PROPOSED SYSTEM

Architecture with many tiers of authority. For the first time, a hierarchical structure in the MABKS system enables many AAs to carry out the time-consuming user certificate verification and intermediate secret key generation on behalf of the CA, reducing the CA's computation requirements. Keywords can be searched at the file

Vol 13, Issue 06, JUNE /2022

ISSN NO:0377-9254

level. MABKS differs from standard CP-ABKS methods in that the secret key used to encrypt a file's file key is embedded within the indexing process, rather than separate operations. [4], [5], [12] For cloud clients (such as data owners and users), this means that the MABKS system allows them to execute keyword-based ciphertext retrieval, as well as file-level fine-grained encryption access control.

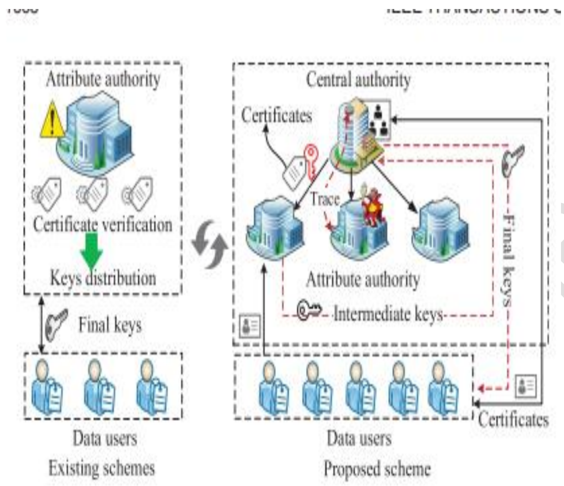

Fig 1:Architecture

A. AA (Attribute Authority) It is responsible for user legitimacy verification procedure, and then sending an intermediate key to CA for legitimacy verified users. AAs can work simultaneously to perform user legitimacy verification. When any user accesses any type of data, AA informs the owner of respective data by a message containing the username.

B. CA (Central Authority) It is responsible for generating secret keys and public keys. It generates a secret key on the basis of received intermediate key from AAs. As a main part of the system, CA has the capacity to trace misbehavior of AA during user legitimacy verification procedure.

C. Data Owner (Owner) A person who encrypts the data under symmetric encryption algorithm. The owner also encrypts the symmetric key under the policy according to a public key received from CA. After that, Owner stores this encrypted symmetric key and data onto the cloud. D. User A user has the set of attributes and the secret key associated with it. The user can easily get encrypted data from a cloud but he is able to decrypt it if and only if his/her attribute set satisfies access policy relating encrypted data.

Vol 13, Issue 06, JUNE / 2022

ISSN NO:0377-9254

E. Cloud Server

It introduces global and public platform for owners to store their encrypted data onto a cloud. Any user is able to download the encrypted data.

5.RESULTS AND DISCUSSIONS

Fig 2:Home Page

Fig 3:Uploaded File Details

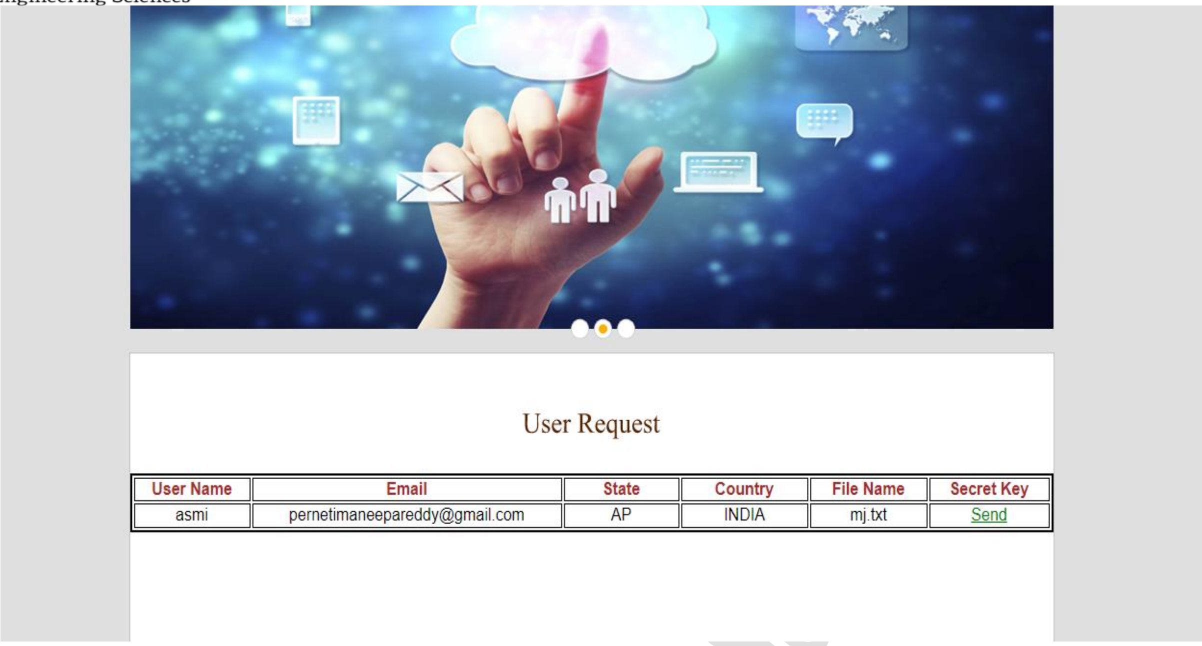

Fig 4:User Request Page

6.CONCLUSION

In this paper, we proposed an efficient and feasible MABKS system to support multiple authorities, in order to avoid having performance bottleneck at a single point in cloud systems. Furthermore, the presented MABKS system allows us to trace malicious AAs (e.g., to prevent collusion attacks) and support attribute update (e.g., to avoid unauthorized access using outdated secret keys). We then demonstrated the selective security level of the system in selective-matrix and selective-attribute models under decisional q-parallel BDHE and DBDH assumptions, respectively. We also evaluated the system's performance and demonstrated that significant computation and storage cost reductions were achieved, in comparison to prior ABKS schemes. However, the main flaw is that the MABKS system cannot support expressive search queries such as conjunctive keyword search, fuzzy search, subset search and so on. The future work will focus on building an efficient and flexible index construction so that the MABKS system is capable of supporting various search requests.

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.

Author’s Profile

G.Tirumala working as Assistant Professor in Department of CSE, VEC Engineering College,kavali. She completed her MCA in Computer Science from JNTU Hyderabad . She completed her M.Tech in Computer Science from JNTU ANANTAPUR . She has 6 years of experience in various engineering colleges.

Journal of Engineering Sciences

Vol 13, Issue 06, JUNE /2022

ISSN NO:0377-9254

P. Srishita Reddy Pursuing B.Tech With Specialization Of Department of CSE, VEC Engineering College,kavali.

G. Sivani Pursuing B.Tech With Specialization Of Department of CSE, VEC Engineering College,kavali

K. Gayathri Pursuing B.Tech With Specialization Of Department of CSE, VEC Engineering College,kavali

N. Vishnu vardhan Reddy Pursuing B.Tech With Specialization Of Department of CSE, VEC Engineering College,kavali