International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

Multiauthoroity Access Control Mechanism For Secure Cloud Storage

Ms. A. Sravya[1], Dr. A. Veerabhadra Rao[2]

#1Student, Department Of Computer Science Engineering,Jogaiah Institute of Technology and Science College of Engineering, Kalagampudi, Near Palakol, West Godavari District, Andhra Pradesh – 534268 . Email:- sravyaachyutha@gmail.com

#2HOD, Department Of Computer Science Engineering,Jogaiah Institute of Technology and Science College of Engineering, Kalagampudi, Near Palakol, West Godavari District, Andhra Pradesh – 534268 Email:- badrialumuri2005@gmail.com

***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. In this paper, we present verify and financially savvy property based information get to control for distributed storage frameworks. In particular, we build a multiauthority CP-ABE conspire that highlights: 1) the framework needn't bother with a completely confided in focal power, and all property specialists autonomously issue mystery keys for clients; 2) each characteristic authority can progressively expel any client from its space with the end goal that those renounced clients can't get to in this manner redistributed information; 3) cloud servers can refresh the scrambled information from the present timespan to the following one to such an extent that the denied clients can't get to those beforehand accessible information; and 4) the update of mystery keys and ciphertext is performed in an open way.

***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

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

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

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

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

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

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.EXISTING SYSTEM

Attribute-based Encryption (ABE) is regarded as one of the most suitable schemes to conduct data access control in public clouds for it can guarantee data owners' direct control over their data and provide a fine-grained access control service. Till now, there are many ABE

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

schemes proposed, which can be divided into two categories: Key-Policy Attribute-based Encryption (KP-ABE) and Ciphertext-Policy Attribute-based Encryption (CP-ABE).

In KP-ABE schemes, decrypt keys are associated with access structures while ciphertexts are only labeled with special attribute sets. On the contrary, in CP-ABE schemes, data owners can define an access policy for each file based on users' attributes, which can guarantee owners' more direct control over their data. Therefore, compared with KP-ABE, CP-ABE is a preferred choice for designing access control for public cloud storage.

4.PROPOSED SYSTEM

Fig 1:Architecture

1.Data Access Control Scheme:

we propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, , to deal with the single-point bottleneck on both security and performance in most existing schemes. In this paper, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t;n) threshold secret sharing into our scheme to share the secret key among authorities. In PROJECT, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t;n) threshold secret sharing guarantees that the master key cannot be obtained by any authorityalone. PROJECT is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. To the best of our knowledge, this paper is the first try to address the singlepoint bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

2.Certificate authority :

The certificate authority is a global trusted entity in the system that is responsible for the construction of the system by setting up system parameters and attribute public key (PK) of each attribute in the whole attribute set. CA accepts users and AAs' registration requests by assigning a unique uid for each legal user and a unique aid for each AA. CA also decides the parameter t about the threshold of AAs that are involved in users' secret key generation for each time.

However, CA is not involved in AAs' master key sharing and users' secret key generation. Therefore, for example, CA can be government organizations or enterprise departments which are responsible for the registration. certificate authority is responsible for the construction of the system, which avoids the extra overhead caused by AAs' negotiation of system parameters. CA is also responsible for the registration of users, which avoids AAs synchronized maintaining a list of users.

3.Attribute authorities:

The attribute authorities focus on the task of attribute management and key generation. Besides, AAs take part of the responsibility to construct the system, and they can be the administrators or the managers of the application system. Different from other existing multi-authority CP-ABE systems, all AAs jointly manage the whole attribute set, however, any one of AAs cannot assign users' secret keys alone for the master key is shared by all AAs. All AAs cooperate with each other to share the master key. By this means, each AA can gain a piece of master key shares its private key, then each AA sends its corresponding public key to CA to generate one of the system public keys. When it comes to generate users' secret key, each AA only should generate its corresponding secret key independently. the master key shared among multiple attribute authorities. In traditional (t;n) threshold secret sharing, once the secret is reconstructed among multiple participants, someone can actually gain its value.

5.RESULTS AND DISCUSSIONS

Fig 2:Home Page

Fig 3:Uploaded File Details

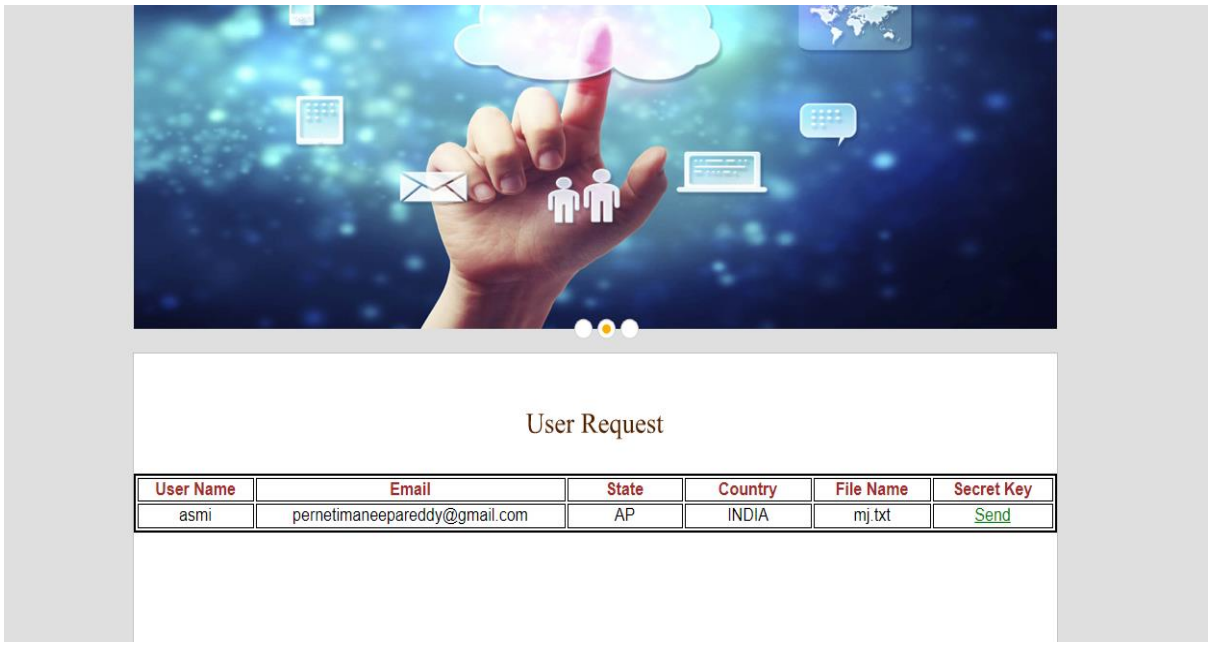

Fig 4:User Request Page

6.CONCLUSION

In this paper, to assemble a protected and savvy multiau-thority property based access control plot for information partaking in distributed storage frameworks, we proposed a

multiauthority CP-ABE conspire supporting versatile client renouncement and open figure content update. The proposed plan accomplishes the expected security properties of forward security and in reverse security, and can likewise withstand decoding key presentation. We demonstrated the secu-rity of the proposed plan in the arbitrary prophet model. Both execution discourses and usage tests show that our plan is increasingly attractive for handy applications.

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

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

Ms. A. Sravya, B.Tech in computer science and engineering from SWARNANDHRA ENGINEERING COLLEGE, affiliated to JNTU, Kakinada in 2016 , pursuing M.Tech in Computer science and engineering from JOGAIAH INSTITUTE OF TECHNOLOGY AND SCIENCE COLLEGE OF ENGINEERING affiliated to the JNTU, Kakinada in 2017-19

Dr. A. Veerabhadra Rao M.Tech., (Ph.D.,), Head of Department,Computer Science Engineering Department Jogaiah Institute of Technology and Science College of Engineering, Kalagampudi, Near Palakol, West Godavari District, Andhra Pradesh– 534268