Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

COMBINING DATA OWNER SIDE AND CLOUD SIDE ACESS CONTROL FOR ENCRYPTED CLOUD STORAGE

[#1]GOLI ANAND, *M.Tech Student,*

[#2]Dr.G.PRABHAKAR RAO, *Associate Professor*,

DEPARTMENT OF CSE ,

SCIENT INSTITUTE OF TECHNOLOGY,IBRAHIMPATNAM, RANGAREDDY,T.S.

ABSTRACT: In public cloud storage system protecting the data and controlling the data access is a challenging issue. Cipher text Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers**.** Attribute-based cryptographic (ABE) technique is taken into account as a most trustworthy cryptographical conducting tool to make sure data owner's direct control on their info in public cloud storage. The previous ABE schemes involve just one authority to require care of the whole attribute set, which could bring a single-point hindrance on every security and performance. Paper planned an efficient revocable decentralized manner CP-ABE information access management technique for multi-authority systems, wherever there exist multiple authorities and every authority is prepared to issue attributes independent to each other.

Keywords—Cloud Storage, Access control, Time-sensitive data, Fine granularity.

I. INTRODUCTION

Cloud computing has drawn extensive attentions from both academic and industry to satisfy the requirement of data storage and high performance computations. Distributed storage is an essential administration of distributed computing which gives administrations to information proprietors to outsource information to store in cloud through Internet.

Data are no longer in data owner's trusted domain, and he/she cannot trust the cloud server to conduct secure data access control. Therefore, the secure access control problem has become a challenging issue in cloud storage. There have been numerous works [1–5] on privacy preserving data sharing in cloud based on various cryptographic primitives, in which the schemes [1–3] based on CP-ABE [6] attract extensive attentions, since they can guarantee data owner fine-grained and flexible access control of his/her own data. However, these schemes determine user's access privilege only based on his/her inherent attributes without any other critical aspects, such as the time factor. In reality, the time factor usually plays an important role in dealing with time sensitive data [7] (e.g. to publish a latest electronic magazine, to expose a company's future business plan). When uploading time-sensitive data to the cloud, the data owner may want different users to access the content after different time. However, to the best of our knowledge, existing CP-ABE based schemes cannot meet such requirement.

To address the issue of information get to control in distributed storage, there have been many plans proposed, among which Cipher content Policy Attribute-Based Encryption (CP-ABE) is viewed as a standout amongst the most encouraging procedures. A notable component of CP-ABE is that it awards information proprietors coordinate control in view of access strategies, to give adaptable, fine grained and secure access control for distributed storage frameworks. In CP-ABE plans, the entrance control is accomplished by utilizing cryptography, here a proprietors information is scrambled with an entrance structure over qualities, and a clients mystery key is named with his/her own properties. Just if the traits related with the clients mystery key fulfill the entrance structure, can the client decode the comparing figure content to acquire the plain-text. Up until now, the CP-ABE based access control plans for distributed storage have been produced into two integral classifications, to be specific, single-

specialist situation and multi expert situation. In most existing CP-ABE conspires there is just a single specialist in charge of trait administration and key circulation. This one and only specialist situation can bring a solitary point bottleneck on both security and execution. Once the expert is traded off, a foe can without much of a stretch acquire the one and only specialists ace key, and afterward he/she can create private keys of any ascribe subset to unscramble the particular encoded information. Also, once the one and only expert is slammed, the framework totally can't function admirably. Accordingly, these CP-ABE plans are still a long way from being broadly utilized for get to control openly distributed storage. Albeit some multi-specialist CP-ABE plans have been proposed, despite everything they can't manage the issue of single-point bottleneck on both security and execution specified previously. In these multi-expert CP-ABE plans, the entire trait set is isolated into numerous disjoint subsets and each quality subset is as yet kept up by just a single specialist. A clear plan to evacuate the single-point bottleneck is to enable various specialists to together deal with the all inclusive property set, such that each of them can circulate mystery keys to clients freely. In this work ,it has been proposed a novel access control heterogeneous structure to address the low effectiveness and single-point execution bottleneck for open distributed storage. It proposes a vigorous and proficient heterogeneous system with single CA (Central Authority) and numerous AAs (Attribute Authorities) for open distributed storage. The overwhelming heap of client authenticity confirmation is shared by different AAs, each of which deals with the all inclusive trait set and can autonomously total the client authenticity check, while CA is in charge of computational assignments which create mystery keys for authenticity confirmed clients. To upgrade security, we additionally propose an inspecting system to distinguish which AA (Attribute Authority) has inaccurately or noxiously played out the authenticity confirmation method.

II. RELATED WORK

The most suitable schemes for the data access controlling mechanism in public clouds is an Attribute based Encryption. It ensures the data owners to have the direct control over the data by providing a fine-grained access control service on data. There are different ABE schemes were proposed, which can be further divided into two different categories; KP-ABE as well as CPABE.

In the KP-ABE schemes, the decrypt keys are combined with the access structures and the ciphertexts are labeled with a special attribute set, for attribute management and then for the distribution of keys, an authority is responsible. That authority may be HRD in a company, any office of registration in a university etc. The data owner defines the access policies and encrypts the info in consistent with the outlined policies. Each user is going to be issued a secret key for its attributes. A user would decipher the info whenever its attributes match the access policies. Access control strategies make sure that Authorized user access information of the system. Access control is a procedure that allows or restricts the access. Access Control identifies the unauthorized users who attempt to access a system. This mechanism plays a vital role for protection as well as it provides computer security. In CP-ABE technique, there exists an authority which may be responsible for the attribute management and then provide key distribution. There are a 2 different CP-ABE systems: single authority[2], [3], [4], [5] CPABE, where all the attributes can be managed by only 1 authority, and multi authority [6], [7], [8] CPABE, where all the attributes are from completely different domains and can

be managed by different authorities. Multiple-authority based CPABE is acceptable mostly for obtaining the data access control over cloud, because the users might hold the attributes issued by multiple authorities and the data owners may additionally share the information using access policy outlined over attributes from completely different authorities.

III. PROPOSED METHOD

The new worldview of outsourcing information to the cloud is a twofold edged sword. From one viewpoint, it liberates information proprietors from the specialized administration, and is less demanding for information proprietors to impart their information to proposed clients. Then again, it

postures new difficulties on security and security insurance. In the current framework a productive time and property factors joined access control plot for time-delicate information out in the open cloud, named TAFC. Our plan has two critical limits: on one side, it acquires the property of fine granularity from CP-ABE; on the opposite side, by presenting the trapdoor component, it additionally has the element of coordinated discharge from TRE. In our plan, the presented trapdoor component is just identified with the time factor, in which just a single comparing mystery ought to be distributed at each opportunity to uncover the related trapdoors. This makes our plan profoundly proficient, with just minimal additional overhead added to the first CP-ABE based plan.

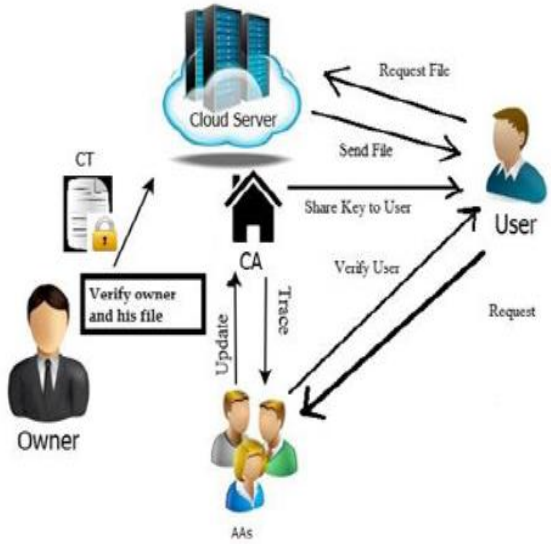


Figure:1. Proposed System Architecture

IV. PROPOSED CONCEPT

We consider a data access control system in multi-authority cloud storage, as described in Fig.2. There are 5 kinds of entities within the system: a certificate authority, attribute authorities, data owners, the cloud server and the data consumers. The Certificate Authority could accepts the registration of all the users and Attribute Authorities within the system. The Certificate Authority assigns globally unique identity for users and Attribute authorities and generates a global public key for the user.

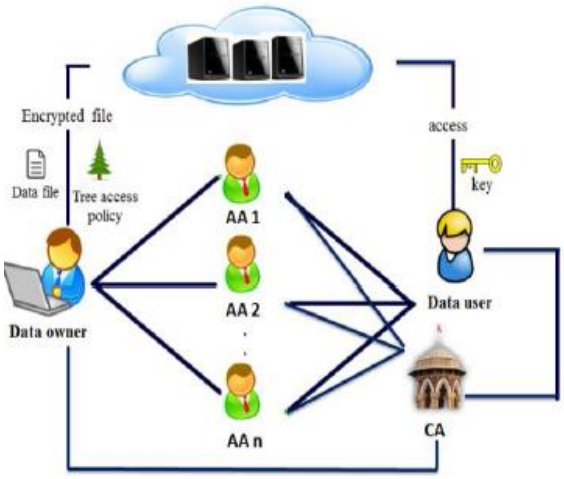


Fig 2: System model of data access control in multi-authority cloud storage

The attribute authorities are responsible for attribute management and key generation. In contrast from the other existing multi-authority CP-ABE systems, all AAs jointly manage the whole attribute set, i.e., any single AA 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. Each AA gain a piece of master key share as its private key, then each AA sends its corresponding public key to CA to generate one of the system public keys. Each AA only should generate its corresponding secret key independently for the users.

The data owner (Owner) encrypts his/her file and defines access policy that can get access to his/her data. Each owner encrypts his/her data with a symmetric encryption algorithm like AES and DES. Then the owner formulates an access policy over an attribute set and encrypts the symmetric key under the policy according to attribute public keys that were gained from CA. Here, the symmetric key is the key used in the former process of symmetric encryption. After that, the owner sends the whole encrypted data and the encrypted symmetric key to store in the cloud server. The data consumer (User) is assigned with a global user identity uid from CA, and applies for his/her secret keys from AAs with his/her identification. The user can decrypt the encrypted data if and only if his/her attribute set satisfies the access policy hidden inside the encrypted data.The cloud server provides a platform for the owners for storing and sharing their data that is in encrypted

form. The encrypted data which is stored in the cloud server can be downloaded/ accessed freely by any data consumer who accepts the policy.

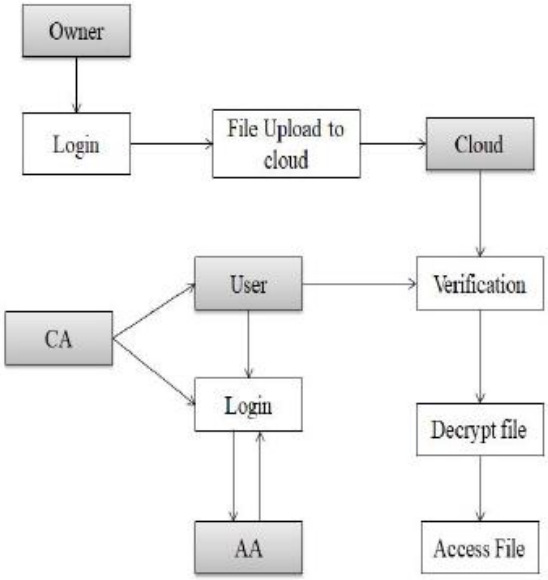


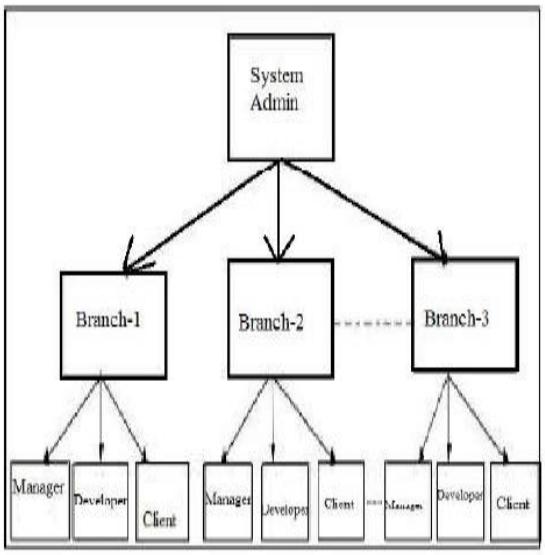
Fig 3: Data Flow Diagram

V.RESULTS

We have developed our system in java. For testing we have hosted each entity on different machines. The cloud, CA, AA and TPA has core i-3 processor with 4 gb RAM. Client system has i3 processor with 2 gb ram. On every system java runtime environment JRE-1.7 is installed. For development we have used jdk 1.7 and IDE: Eclipse and Net beans are used. For Database storage we have used mysql 5.3 database. For implementation of our system we have followed the business structure of users. Following is the system users structure with designation. Consider a scenario, if user wants to share data with manager and developer of department 1 and 2. Following attributes will be required to generate key.

Departmant1-manager Departmant1-Developer

Departmant1-manager Department2-Developer



VI. CONCLUSION

This paper aims at fine-grained access control for timesensitive data in cloud storage. One challenge is to simultaneously achieve flexible timed release and fine granularity with lightweight overhead, which is not provided in related work. In this paper, we propose a scheme to achieve this goal. Our scheme seamlessly incorporates the concept of timed-release encryption to the architecture of ciphertext-policy attribute based encryption. With a suit of proposed mechanisms, this scheme provides data owners with the capability to flexibly release the access privilege to different users at different time, according to a well-defined access policy over attributes and release time. The analysis shows that our scheme can protect the confidentiality of time-sensitive data, with a lightweight overhead on both CA and data owners, thus well suits the practical large-scale access control system for cloud storage.

REFERENCES

[1] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754, 2012.

[2] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1790–1801, 2013.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[4] Z. Zhou, H. Zhang, Q. Zhang, Y. Xu, and P. Li, "Privacypreserving granular data retrieval indexes for outsourced cloud data," in Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM2014), pp. 601–606, IEEE, 2014.

[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," in Proceedings of the 2011 IEEE Global Communications Conference (GLOBECOM2011), pp. 1–5, IEEE, 2011.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 28th IEEE Symposium on Security and Privacy (S&P2007), pp. 321–334, IEEE, 2007.

[7] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 191–233, 2001.

[8] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," tech. rep., Massachusetts Institute ofTechnology, 1996.

[9] K. Yuan, Z. Liu, C. Jia, J. Yang, and S. Lv, "Public key timed-release searchable encryption," in Proceedings of the2013 Fourth International Emerging Intelligent Data and Web Technologies (EIDWT2013), pp. 241–248, IEEE, 2013.

[10] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences, vol. 258, no. 3, pp. 355–370, 2014.

[11] L. Xu, F. Zhang, and S. Tang, "Timed-release oblivious transfer," Security and Communication Networks, vol. 7, no. 7, pp. 1138–1149, 2014.

[12] E. Androulaki, C. Soriente, L. Malisa, and S. Capkun, "Enforcing location and time-based access control on cloud-stored data," in Proceedings of the 2014 IEEE 34th International Distributed Computing Systems (ICDCS2014), pp. 637–648, IEEE, 2014.

[13] C.-I. Fan and S.-Y. Huang, "Timed-release predicate encryption and its extensions in cloud computing," Journal of Internet Technology, vol. 15, no. 3, pp. 413–426, 2014.

[14] X. Zhu, S. Shi, J. Sun, and S. Jiang, "Privacy-preserving attribute-based ring sign cryption for health social network," in Proceedings of the 2014 IEEE Global Communications Conference(GLOBECOM2014), pp. 3032–3036, IEEE, 2014.

[15] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology (CRYPTO2001), pp. 213–229, Springer, 2001.

AUTHOR'S PROFILE:

[1]. **GOLI ANAND,** Pursuing *M.Tech in CSE* **at** Scient Institute Of Technology, Ibrahimpatnam, Rangareddy, T.S.

[2].**Dr. G.PRABHAKAR RAO**, presently working as *Associate Professor in* Department Of CSE, Scient Institute Of Technology, Ibrahimpatnam, Rangareddy,T.S.