International Journal of Engineering Research & Management Technology ISSN: 2348-4039
May-2016 Volume 3, Issue-3
Email: editor@ijermt.org www.ijermt.org

EFFICIENT DATA ACCESS CONTROL FOR MULTIAUTHORITY CLOUD STORAGE SYSTEM

Rashmi Jadhav
SRCOE
Department Computer Engineering
Savitribai Phule Pune University
Pune

Deepti Varshney
Assistant Professor
Department Computer Engineering
Savitribai Phule Pune University
Pune

***ABSTRACT*:** *Cloud computing is a type of computing that depends on sharing computing resources rather than having local servers or personal devices to handle applications. It provides cloud storage service for data owners to host their data in the cloud. This new technology of data hosting and data access services introduces a great challenge to data access control. Cipher text policy attribute-based encryption technique use for providing data access control in cloud storage. But it is hard to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. The proposed scheme provides solution to the attribute revocation problem. The system consists of multiple authorities each authority is responsible for performing distinctive task. The proposed scheme renovate the components of the revoked attribute only and generates latest secret keys for the revoked attribute and forwards it to the non-revoked. System can efficiently achieve forward security and backward security.*

KEYWORDS: *Multi-Authority, CP-ABE, Certificate Authority, Attribute Authority, Access control, Attribute revocation.*

I. INTRODUCTION

Modern computing technology [10] attracted more peoples to store their private data on third party servers. Number of peoples can store their data or application for cost saving over cloud. Data outsourcing [5] system require flexible access control approach for accessing data from various locations. For providing data access control different data access policies or data access services are defined according to user role within system by the servers. But cloud server cannot be fully trusted by data owner all the time. Data owner can no longer rely on servers to do data access control. CPABE [5][2][3] technique provides efficient data access control method in cloud storage system. The technique gives more direct control on access polices. By using CPABE technique encrypted data can be kept confidential even if the storage server is untreated. There are two method of CPABE technique Single authority CPABE [4][11][13] in which all attributes are manage by single authority & Multi authority CPABE[1][7][8] where attributes are manage by various authority. Multi authority CPABE is more appropriate for data access control of cloud storage because user may hold attribute[5] by multiple authority & data owner may share data using access policy method define over attribute from different authorities. But, the existing CPABE [4][5] is difficult to apply in multi authority cloud storage due to its attribute revocation problem.

The proposed system updates components of revoked attribute [12] only and generate new secret key for revoked attribute [6] and forward that key to non-revoked users of the system. The proposed system assured forward security [6] and backward security. The system efficiently solved attribute revocation problem in multi authority cloud storage. It eliminates high communication overhead between data owners and cloud servers.

II. LITERATURE SURVEY

M. Chase, [7] [8] proposed a scheme acquaint a global identifier to tie user's keys together. Proposed scheme relies on a central authority to provide a final secret key to integrate the secret keys from different attribute authorities. But, the central authority would be able to decrypt all the cipher text in Chase's scheme, since it holds the master key of the system. Thus, the central authority would be a unsafe point for security attacks and a performance bottleneck for large scale systems. Muller et al. [11] proposed a scheme for implementing fine-grained cryptographic access control. The system uses cipher text- policy ABE scheme with user accountability, which reduces both the trust assumption on the authorities and that on the users. System security is based on the Decisional Bilinear Diffie-Hellman assumption. It uses a new tracing algorithm with a lower computational cost when compared with existing account table ABE schemes.

J. Bethencour t[4] suggested a scheme for recognize complex access control on encrypted data. System kept encrypted data confidential even if the storage server is entrusted. B. Waters [7] recommended technique in which single authority provides attributes to multiple users and simultaneously manage assign attributes. But, it produced a security complications and overhead to the authority as all the users need to be maintained and managed by central authority only. Yu [12], M. Li [9] provide definition for attribute revocation in CP-ABE with honest-but-curious severs, and formulate the security model to reflect possible attacks. The scheme enables the authority to revoke any attribute of users at any time while placing a minimal load on him. Scheme is secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

III.PROPOSED MODEL

Proposed system solves the attribute revocation problem in multi authority cloud storage system. System provides backward security and forward security. Model is consisting of five different entities: Certificate authority, Attribute authority, Data owner, User and Cloud service provider. Each entity is responsible for performing distinct task in the system. The Certificate authority is global trusted certificate authority in the system. It sets up the system and accepts the registration from the users and attributes authority in the system [6]. For each legal user in the system certificate authority assign global unique user identifier. Certificate authority is not involved in any attribute management and generation of secret keys.

Attribute authority is responsible for entitling and revoking users attribute according to their role. Every attribute is associated with single attribute authority but each attribute authority can manage arbitrary number of attributes. Attribute authority has control over structure and semantics of its attribute. Attribute authority generate public attribute key for each attribute it manage and secret key for each user attribute. Every user has unique identity in system. User can hold set of attribute which are assign from multiple authority. Attribute authority issues secret key associates with its attribute to each user of the system. Data owner of the system fragments data into various components according to logic granularity and encrypt each data components with different content key using symmetric encryption technique. Then data owner define access polices over attribute.

Stage 1- Registration and Authentication

New user enter into the system are provide their details for the registration to certificate authority. After completion of registration procedure certificate authority assign unique identity number to each user. User enter his UID while login into the cloud service provider. Cloud service provider validates UID using details stored into database. User get enter into cloud service provider only if he is and valid user of the system. After successfully login into cloud service provider user provide his UID to attribute authority. Attribute authority verifies information provided by user and assign attribute and generate secret key.

Stage 2- Encryption and Decryption

According to logical granularity data owner divides the data into multiple components. Then these data components are encrypted using encryption algorithm and store over cloud service provider. If user attribute and access control rights are satisfied user can download data from cloud.

Stage 3- Attribute Revocation

To get solution to attribute revocation problem, proposed system assign version number to each attribute. If any attribute revoked from system the corresponding attribute authority generate an updated version number for that particular revoked attribute only. Then attribute authority generates updated version of secret key and forward it to the user entitled with revoked attribute belonging to that attribute authority. Using new updated secret key user can decrypt the data.

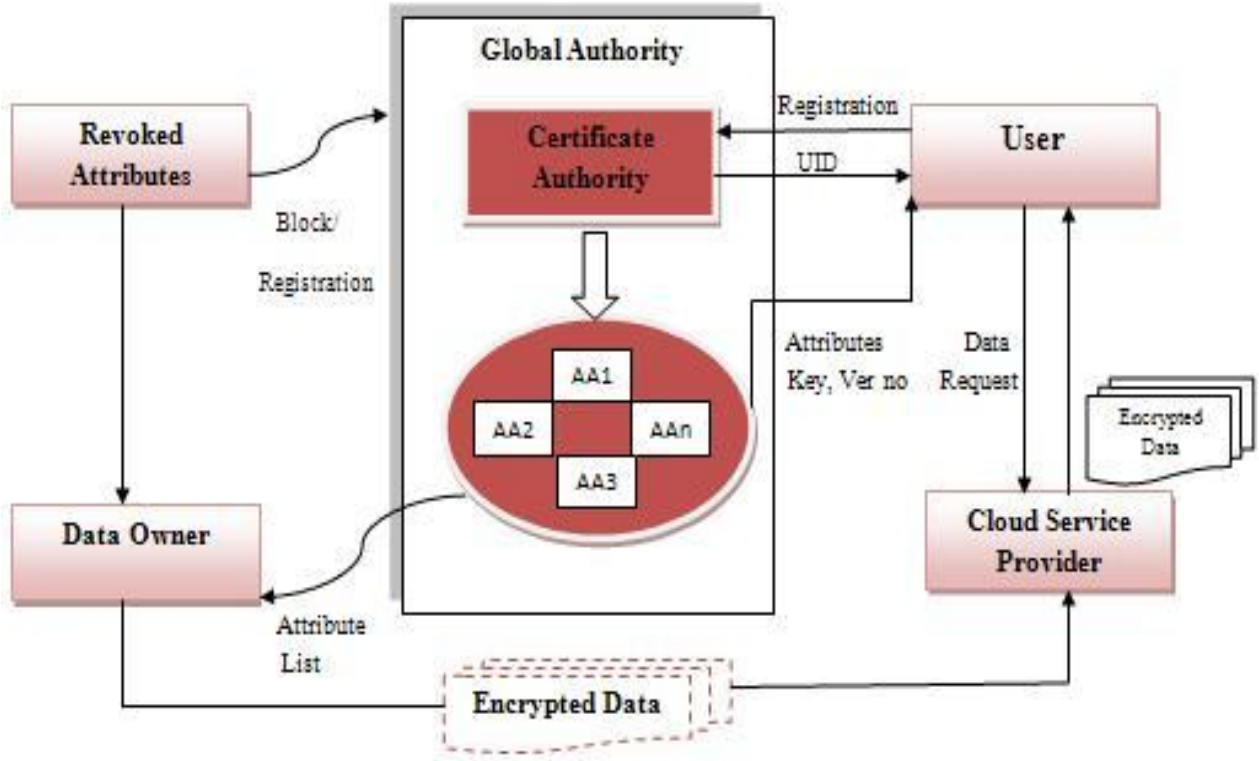

Fig1:
Block diagram of Efficient Data Access Control for Multi authority Cloud Storage System

IV. SECURITY ANALYSIS

The system efficient data access control for multi authority cloud storage system is secure as it achieves both forward security and backward security.

A] Forward Security

If any newly join user has sufficient attributes assign by attribute authority, secret keys and unique identification number then user can also decrypt the previously publish cipher text which are encrypted by using previous public attribute keys.

B] Backward Security

In backward security revoked user can not decrypt any new cipher text that is encrypted with new public attribute key. The system only updates those components which are associated with revoked attribute of cipher text and remaining components which are not related to the revoked attributes are not change. Because of this feature system greatly improve efficiency of attribute revocation in multi authority system.

V. RESULTS AND DISCUSSION

The system recommends a revocable multi authority cipher text policy attribute encryption technique. It provides efficient, expressive and secure revocation method to solve attribute revocation problem. Scheme requires less communication cost and computation cost. The system can apply as underlying technique to construct the expressive and secure data access control scheme for multi authority cloud storage.

A] Cloud Service Provider Window

B] Certificate Authority Window

C] Attribute Authority Window

D] Attribute Authority Details

E] Comparison Results at Deployment Time

Following results shows comparison of computation efficiency for encryption time and decryption time for existing system and proposed system.

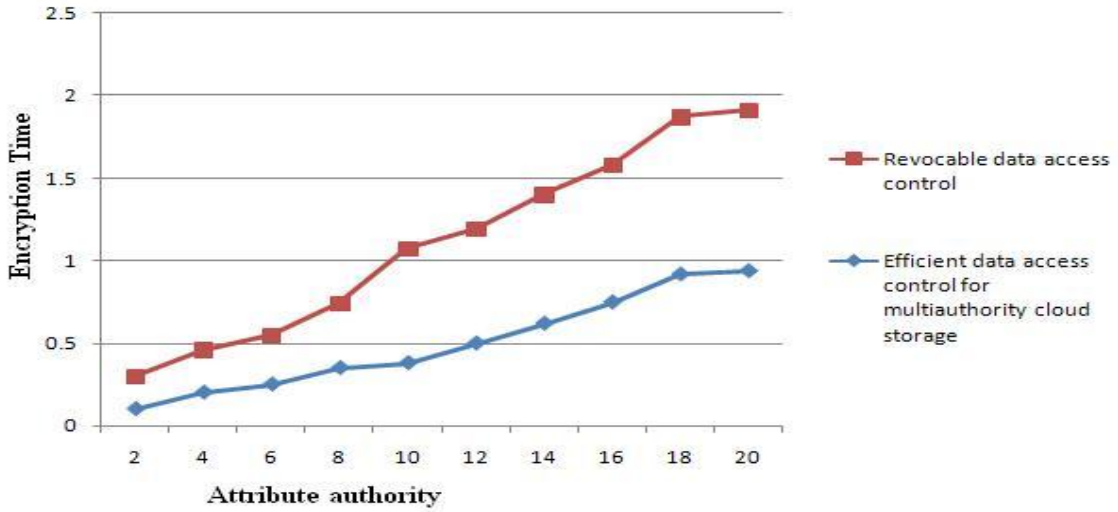

Fig: AA versus Encryption time

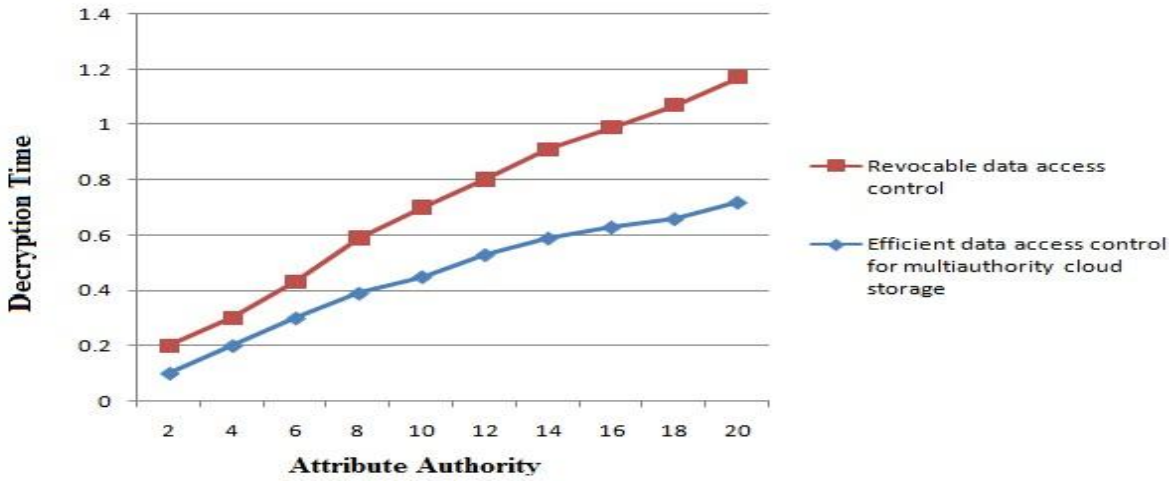

Fig: AA versus Decryption time

VI. CONCLUSION

Cloud computing provided service for stocking data of data owner over the cloud this new technique of data hosting and data access service introduced great challenge to data access control. Cipher text policy attribute based encryption is considered as suitable technology for data access control over cloud storage system. But it is difficult to directly apply CPABE scheme because of its attribute revocation problem. The proposed system contemplated revocable multi authority attribute cipher text policy attribute base encryption that can support efficient attribute revocation. System constructed effective data access control scheme for multi authority cloud storage.

ACKNOWLEDGMENT

I am overwhelmed in all humbleness to acknowledge my depth to all those who have helped me to put these ideas, well above the level of simplicity and into something concrete. I would like to thank all those people whose support and cooperation has been an invaluable asset during the course of this paper especially my project guide and HOD of Computer Engineering Department at SRCOE, Pune Prof. Deepti Varshney

who gave it the present shape. It would have been impossible to complete the paper without their support, valuable suggestions, criticism, encouragement and guidance also for her motivation and providing various facilities, which helped me greatly in the whole process of this paper. I am also grateful to all other teaching and non-teaching staff members of the Computer Engineering Department for directly or indirectly helping us for the completion of this paper and the resources provided.

REFERENCES

1. A.B. Lewko and B. Waters, ‘‘Decentralizing Attribute-Based Encryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’11, 2011, pp. 568-588.
2. A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ‘‘Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’10, 2010, pp. 62-91.
3. B. Waters, “Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization.” in *Proc.4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11),* 2011, pp. 53-70.
4. J. Bethencourt, A. Sahai, and B. Waters, “Cipher text-Policy Attribute-Based Encryption,” in Proc, IEEE Symp, Security and privacy (S&P’07), 2007, pp. 321-334.
5. J. Hur and D.K. Noh, ‘‘Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,’’ IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
6. Kan Yang,Xiaohua Jia “Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage” IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 7, July 2014.
7. M. Chase, ‘‘Multi-Authority Attribute Based Encryption,’’ in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC’07), 2007, pp. 515-534.
8. M. Chase and S.S.M. Chow, ‘‘Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,’’ in Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09), 2009, pp. 121-130.
9. 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 *Trans. Parallel Distributed Systems*, vol. 24, no. 1, pp. 131-143, Jan. 2013.
10. P. Mell and T. Grance, ‘‘The NIST Definition of Cloud Computing,’’ National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.
11. S. Muller, S. Katzenbeisser, and C. Eckert, “Distributed attribute-based encryption,” *Information Security and Cryptology*, pp. 20–36, 2009.
12. S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Attribute Based Data Sharing with Attribute Revocation,’’ in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS’10), 2010, pp. 261-270.
13. V. Goyal, A. Jain,O. Pandey, and A. Sahai, ‘‘Bounded Cipher text Policy Attribute Based Encryption,’’ in Proc. 35th Int’l Colloquium on Automata, Languages, and Programming (ICALP’08), 2008, pp. 579-591.