Journal of Advances in Science and Technology
Vol. 12, Issue No. 25, (Special Issue) December-2016, ISSN 2230-9659

Responsive, Efficient, and Reversible Data Access Control for Multi-Authority Cloud Storage

Shruti A. Upari[1]*, Vivekanand Reddy[2]

[1]Department of Computer Science and Engineering, Centre for PG-Studies, Visvesvaraya Technological University, Belagavi, Karnataka, India

[2]Faculty in Department of Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India

Abstract – Abstract- Cloud Storage is an easy and convenient way for storing and accessing data, it is one of the services that offers various facilities to the data owners. Data Access Control is one of the most successful ways to ensure data security in the cloud. However, due to various issues such as data expansion and un-trusted, un-authorized cloud server, accessing of the data has become the most challenging issue. The Ciphertext Policy- Attribute Based Encryption (CP-ABE) scheme is regarded as the most prominent because it provides owners direct control on access policies. In this paper, CP-ABE scheme has been proposed for solving the problem of attribute revocation method. It is used as an underlying technique during the design of data access control scheme which achieves forward and backward security.

Index Terms - CP-ABE, Cloud Storage, Attribute Revocation, Data Access Control, Access Policies.

----------♦----------

I. INTRODUCTION

Cloud Computing is the most promising and evolving paradigm. Cloud Storage is one of the most important services of Cloud Computing [1]. It offers services for Data Owners to host their data in the Cloud, this new model of Data Hosting and Data Access Services are considered to be the matter of contention to Data Access Control. This Data Access Control is an effective and successful way for accessing data but this accessing has become a major issue due to security threats such as un-trusted cloud server. Because Cloud server cannot be trusted by the data owners, these owners do not depend on the servers to do access control. Attribute Based Encryption (ABE) is a new concept of Encryption Algorithm which allows the Authority or the Owner to describe a set of policies. This ABE reconsiders the concept of Public Key Cryptography but makes use of attributes rather than identity of the user as a secret key. This proposed work allows the Consumer or end users to access data by communicating with the Data Owner and the Server being used need not be completely trusted i.e., they can be semi-trustable. The main focus of this project is to provide Attribute Revocation which achieves both backward securities i.e., a revoked user cannot decrypt any new ciphertext, and forward security i.e., newly joined user can decrypt the already existing ciphertext.

Attribute Based Encryption [2] defines each of the identity as a set of attributes where the roles, and messages are encrypted using the subset of attributes or as per the policies defined over the set of attributes. There are usually two types of ABE's and they are Key Policy-Attribute Based Encryption and Ciphertext Policy-Attribute Based Encryption. In case of Key Policy- Attribute Based Encryption, attributes are encrypted along with the data giving an access structure to each of the user as a part of their secret key whereas in case of Ciphertext Policy-Attribute Based Encryption a user's secret key is correlated with the set of attributes and an ciphertext is generated which refers to the access policy over a defined set of attributes within the system.

II. CLOUD STORAGE

Cloud Storage is a service of Cloud Computing that offers services for owners to host their data in the cloud. Cloud Storage is a service where data is remotely maintained, managed, and backed up. The service allows the users to store files online, so that they can access them from any location via the Internet. The Cloud Storage Server sometimes

cannot be trusted and hence in this paper we have constructed the CP-ABE scheme which solves the problem of Revocation method.

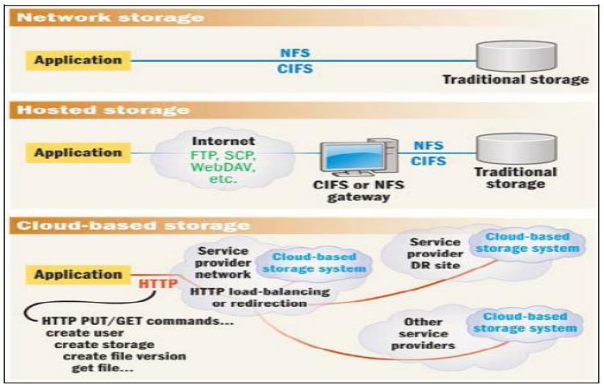

Figure – 1, Cloud Storage

A. Ciphertext Policy- Attribute Based Encryption

Ciphertext Policy Attribute Based Encryption is a scheme for data access control in cloud storage as it gives the owners more direct control on access policies.

In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently the only method for enforcing such policies is to store the data and mediate access control. In this project, a technique used is CP-ABE using which encrypted data can be kept confidential even if the storage sever is untrusted and also is secure against attacks.

There are two types of CP-ABE systems: single-authority CP-ABE [2], [3], [4], [5] where all attributes are managed by a single authority, and multi-authority CP-ABE [6], [7], [8] where attributes are from different domains and managed by different authorities. Multi-authority CP-ABE is more appropriate for data access control of cloud storage systems, as users may hold attributes issued by multiple authorities and data owners may also share the data using access policy defined over attributes from different authorities.

In multi-authority cloud storage systems, users' attributes can be changed dynamically. A user may be entitled some new attributes or revoked some current attributes. And his permission of data access should be changed accordingly. However, existing attribute revocation methods [9], [10], [11], [12] either rely on a trusted server or lack of efficiency, they are not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems. In this paper, we first propose a revocable multi-authority

CP-ABE scheme, where an efficient and secure Revocation method is proposed to solve the attribute revocation problem in the system. Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt) and forward security (The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient attributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi-trusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

III. RELATED WORK

S. Yu et al. [9] proposed Attribute Based Data Sharing with Attribute Revocation. Authors mainly used semi-trustable on-line proxy servers. This server enables the authority to revoke user attributes with minimal effort. This scheme was uniquely integrating the technique of proxy re-encryption with CP-ABE, and also enables the authority to delegate most of laborious tasks to proxy servers. The advantages of this scheme is More Secure against chosen cipher text attacks. Provide importance to attribute revocation which is difficult for CP-ABE schemes. The one of the drawback is the storage overhead could be high if proxy-servers keep all the proxy re-key.

S J. Hur and D.K. Noh, [11] worked on Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems. They presented an access control mechanism based on cipher text-policy attribute-based encryption to implement access control policies with efficient attribute and user revocation method. The fine-grained access control can be achieved by dual encryption scheme. The dual encryption mechanism gets advantage of the attribute-based encryption and selective group key distribution in each attribute group. This method is securely managing the outsourced data and achieved efficient and secure in the data outsourcing systems.

M. Li, S. Yu, Y. Zheng, K. Ren, and W.Lou, [10] presented Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. They considered the use of dual system encryption methodology. The encryption techniques from Multi-authority ABE and Key-Policy ABE are combined into a single module. The proposed MA-ABE technique proves useful for key management and flexible access handled by KP-ABE. The proposed framework has attempted to achieve data security by MA-ABE and data privacy by KP-ABE scheme. The overall security of the system has been improved. Existing attribute revocation methods rely on a trusted server or lack of efficiency also they are not suitable for dealing with the attribute

revocation problem in data access control in multi-authority cloud storage systems.

IV. SYSTEM MODEL

The system model of data access control is as shown in the below figure 2.

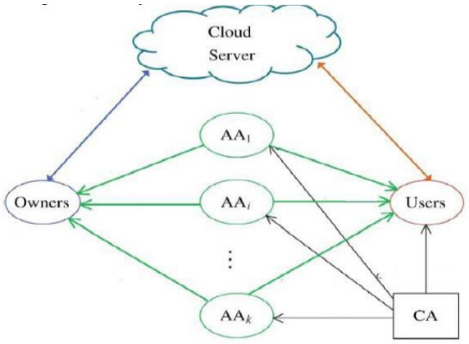

Figure – 2. Cloud Storage model for data access control

There are five types of entities in the system: a certificate authority (CA), attribute authority (AA), data owners (owners), the cloud server (server) and data consumers (users).

A. Certificate Authority

The CA is a global trusted certificate authority in the system. It builds up the system and accepts the registration of every user and AAs within the system. It assigns a global unique user id and global attribute authority id for every user and attribute authority. This CA is not involved is any attribute management and in the generation of secret keys to the user which are associated with the attributes.

B. Attribute Authority

The AA is a unique and independent attribute authority who is responsible for generating and cancelling user's attributes based on the roles of the user or the identity in the domain. It is the one who generates a public key for each attribute it manages and a secret key for each user reflecting their attributes.

Data Owners

The owner here is independent of every other owner. The owner first divides the data into components and encrypts each data with different set of keys using symmetric encryption techniques. Then owner defines access policies over attributes from multiple attribute authorities and encrypts the set of keys under the policies. The owner send the encrypted data to cloud server along with the ciphertexts. They do not rely on cloud server for data access control as this access control happens inside the cryptography. The user can decrypt the data only if it satisfies the set of keys and set of attributes.

C. Cloud Server

The place where data is stored.

D. Data Consumers

Each user has a global identity in the system. The user is entitled a set of attributes which is given by the authorities. The user will receive a secret key which is associated with the attributes entitled by the responding attribute authorities.

V. PROPOSED WORK

In the proposed system the problem occurred in the survey paper [4] is resolved to achieve attribute revocation method. It allows updating of ciphertext when the user revokes his/her attributes which was not possible in the existing system. The revocation method is proved efficient meaning that it incurs very less communication and computation cost. This scheme does not need the server to be completely trusted as key update takes place by the attribute authorities. The following figure 3, 4, 5 shows the block diagram and sequence diagram of the system.

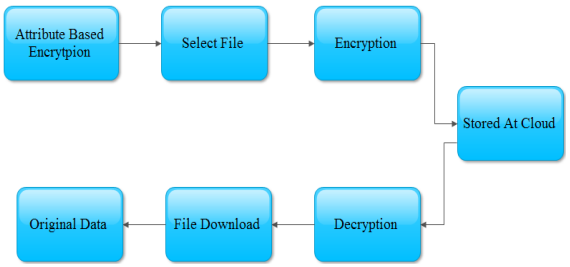

Figure – 3. Block Diagram of the System

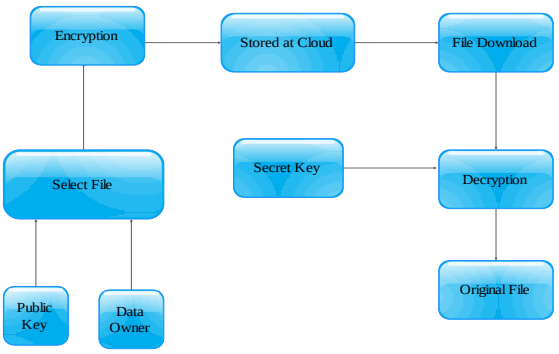

Figure – 4. Block Diagram of the Encryption Phase

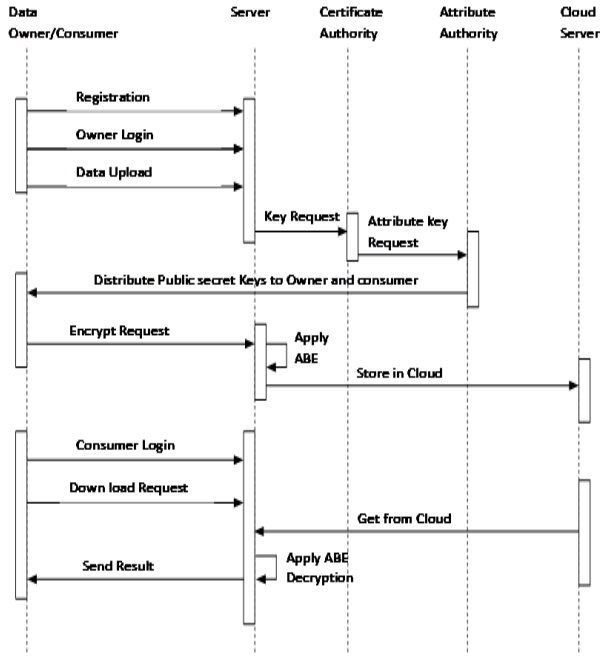

Figure – 5. Sequence Diagram of the System

CONCLUSION

In this paper, we proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. The revocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.

ACKNOWLEDGEMENT

I, Ms Shruti A. Upari owe a debt of deepest gratitude to my esteemed guide **Prof. Vivekanand Reddy**, for his guidance, support, motivation and encouragement during the course of this project work. His readiness's for consultation at all times, his educative comments, his concern during this period has been invaluable.

I express my gratitude to **Dr. Shivaprasad Dandagi,** PG-Coordinator, VTU, Belagavi, for their support during the course of this project work.

I take this opportunity to thank all the **staff members of VTU, Centre for P.G. Studies, "Jnana Sangama", Belagavi,** for their cooperation and suggestions during the period of the project work.

I thank all my **family members and friends** without whose support this project would not have been completed.

It's my pleasure to thank all those who have rendered their help in successful completion of my project work directly or indirectly and whose suggestions went a long way in achieving the objective of the project.

REFERENCES

P. Mell and T. Grance, ''The NIST Definition of Cloud Computing,'' National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-PolicyAttribute-Based Encryption,'' in Proc. IEEE Symp. Security and privacy (S&P'07), 2007, pp. 321-334.

B. Waters, ''Ciphertext-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.

V. Goyal, A. Jain,O. Pandey, andA. Sahai, ''Bounded Ciphertext Policy Attribute Based Encryption,'' in Proc. 35th Int'l Colloquium on Automata, Languages, and Programming (ICALP'08), 2008, pp. 579-591.

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.

M. Chase, ''Multi-Authority Attribute Based Encryption,'' in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC'07), 2007, pp. 515-534.

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.

A.B. Lewko and B. Waters, ''Decentralizing Attribute-Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11, 2011, pp. 568-588.

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.

M. Li, S. Yu, Y. Zheng, K. Ren, andW. 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.

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.

S. Jahid, P. Mittal, and N. Borisov, ''Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.

Corresponding Author

Shruti A. Upari*

Department of Computer Science and Engineering, Centre for PG-Studies, Visvesvaraya Technological University, Belagavi, Karnataka, India

E-Mail – shrutiupari@gmail.com