Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Literature review on Efficient and Revocable Data Access Control Scheme for Multi-Authority Cloud Storage Systems

Shrikant S. Patil[1], B. R. Solunke[2]
[1]*CSE, NBNSCOE, Solapur*
[2]*CSE, NBNSCOE, Solapur*

Abstract—Cloud computing is one of the emerge technologies. To protect the data and privacy of users the access control methods ensure that authorized users access the data and the system. Cipher text-Policy Attribute-based Encryption (CP-ABE) is the appropriate method for data access control in cloud storage. However, CP-ABE schemes to data access control for cloud storage systems are difficult because of the attribute revocation problem. Specifically, this paper surveys a revocable multi-authority CP-ABE scheme. The attribute revocation method can efficiently achieve both forward security and backward security.

Keywords—Ciphertext-policy Attribute-based encryption (CP-ABE), cloud storage, data access control, multi-authority CP-ABE protocol.

I. INTRODUCTION

All Data access control is an efficient way to ensure the data security in the cloud. Cloud storage services allows data owner to outsource their data to the cloud. Attribute-based encryption (ABE) [1] is a new concept of encryption algorithms that allow the encryptor to set a policy describing who should be able to read the data. In an attribute-based encryption system, private keys distributed by an authority are associated with sets of attributes and ciphertexts are associated with formulas over attributes. A user should be able to decrypt a ciphertext if and only if their private key attributes satisfy the formula. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the conventional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g. roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE).

In ciphertext-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a ciphertext specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext. Cipher text-Policy Attribute-based Encryption (CP-ABE) is considered as one of the most suitable scheme for data access control in cloud storage. This scheme provides data owners more direct control on access policies [2]. However, CP-ABE schemes to data access control for cloud storage systems are difficult because of the attribute revocation problem. So This paper produce survey on efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities cooperate and each authority is able to issue attributes independently.

CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data. Another nice feature is that users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows decrypting. Any future users that will be given a

key with respect to attributes such that the policy can be satisfied will then be able to decrypt the data.

There are two types of CP-ABE systems: single-authority CP-ABE, and multi-authority CP-ABE. In single-authority CP-ABE scheme [3], where all attributes are managed by a single authority. In multi-authority CP-ABE [4], where attributes are from different domains and managed by different authorities. This method is more suitable for data access control of cloud storage systems. Users contain attributes those should be concerned by multiple authorities and data owners. Users may also share the data using access policy defined over attributes from different authorities.

Rest of the paper structured as follows. Sections 2 gives the related work on ABE and attribute revocation methods. Section 3 gives the detailed construction of our data access control scheme for multi-authority cloud storage systems. The conclusion is given in Section 4.

II. LITERATURE SURVEY

In last few years, to design the data access control scheme for multi-authority cloud storage systems, the main challenging issue is to construct the underlying Revocable Multi-authority CP-ABE protocol.

S. Yu et al. [5] 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, [6] 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, [7] 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.

S. Jahid, P. Mittal, and N. Borisov, [8] worked on Encryption-Based Access Control in Social Networks with Efficient Revocation. The proposed architecture supports two approaches are fine-grained access control policies and dynamic group membership. Both scheme achieved by using attribute-based encryption, however, is that it is possible to remove access from a user without issuing new keys to other users or re-encrypting existing cipher texts. They proved this by creating a proxy that participates in the decryption process and enforces revocation constraints. The advantage of this scheme is that it provides performance evaluation, and prototype application of our approach on Face book.

In [9], Attribute-Based Encryption with Verifiable Outsourced Decryption method changes the original model of ABE with outsourced decryption to allow for verifiability of the transformations in existing system. This new model constructs a existing ABE scheme with verifiable outsourced decryption also does not rely on random oracles. Multi-authority CP-ABE protocol allows the central authority to decrypt all the cipher texts, because it contains the master key of the system.

In [10], Chase proposed a multi-authority CP-ABE protocol; however, it cannot be directly applied as the underlying techniques because of two main reasons: 1) Security Issue: Chase's multi-authority CP-ABE protocol allows the central authority to decrypt all the ciphertexts, since it holds the master key of the system; 2) Revocation Issue: Chase's protocol does not support attribute revocation.

The technique used in [11] by S. Ruj, A Nayak and I. Stejmenovic requires owners to re-encrypt the cipertext. K. Yang and X. Jia also suggested the method in [2] need owner to generate the update information during the revocation, where the owner should also hold the encryption secret for cipher text in the system. This incurs a heavy storage overhead on the owner, especially when the number of ciphertext is large in cloud storage system.
Though the existing methods provided solution for the attribute revocation problem they are not efficient and cause large storage overhead. Hence there is need of an improved scheme for data access controls in the cloud storage were the cloud servers are not trustworthy.

III. DATA ACCESS CONTROL SCHEME FOR MULTI-AUTHORITY CLOUD STORAGE SYSTEMS

The data access control scheme for multi-authority cloud storage systems is proposed to support the authority access control get from the many attribute authorities. The users those who are having matching attributes as in the access policy defined in the cipher text can retrieve the entire data content. It aims to allow the users with eligible attributes to decrypt the entire data stored in the cloud server.
The data access control scheme consists of five phases shown in figure 1: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users). The global trusted certificate authority in the system is the CA. It sets up the system and accepts the registration of all the users in the system. For each authorized user in the system, the CA assigns a global unique user identity to it and also generates a global public key for each user. Each user will be issued a Social Security Number (SSN) as its global identity. Every AA is responsible for entitling and revoking user's attributes according to their role or identity. Every attribute is associated with single AA, but numbers of attributes are managed by AA. The attributes‟ structure and semantics are controlled by every AA. The public attribute key for each attribute it manages and a secret key or each user is generated by each AA.

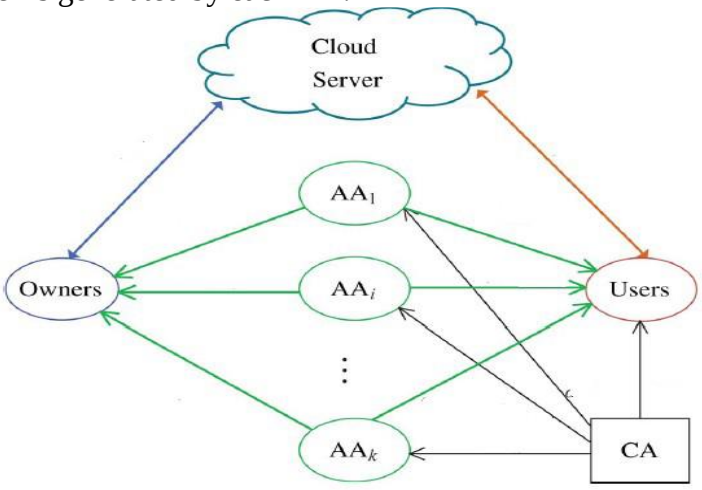

Figure1. System model of data access control in multi-authority cloud storage

When users want to access the data from cloud servers, users has to be maintained by the Certificate Authority who issues the authentication certificate to user to access data. After obtaining the certificate user and owners share the data with the attributes verification for data access. Every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key.

In this method each user has a global identity. The user can have set of attributes which come from multiple attribute authorities. The corresponding attribute authorities entitle its user associated with a secret key. The data is divided into several components by the owner and each data component is encrypted with different content keys using symmetric encryption. The access policies over the attributes are defined by the owner and encrypt the content keys in the policies. The owner then sends the encrypted data together with the ciphertexts to the cloud server. The user is able to decrypt the ciphertext only when the user's attributes satisfy the access policy defined in the ciphertext. The different number of content keys is decrypted by users with different attributes and from same data different information's are obtained.

The revocable multi-authority CP-ABE scheme is an efficient and secure revocation method. An attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, secure in the sense that it can achieve both backward security and forward security.

IV. CONCLUSION AND RESEARCH SCOPE

In this paper, we made a survey on the effective data access control scheme constructed for multi-authority cloud storage systems. Nowadays, there is an emerging trend that increasingly more customers are beginning to use the public cloud storage for online data storing and sharing; the security in cloud is major issue. The multi-authority CP-ABE reduces Decryption overhead for users according to attributes. This secure attribute based cryptographic technique for robust data security that's being shared in the cloud .This multi-authority CP-ABE scheme proved that it is secure and verifiable. The revocable multi-authority CPABE is an efficient technique, which can be appropriate in any remote storage systems and online social networks etc.

REFERENCES

[1] 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.

[2] K. Yang and X. Jia, ''Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,'' in Proc. 32th IEEE Int'l Conf. Distributed Computing Systems (ICDCS'12), 2012.

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

[4] 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.

[5] 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.

[6] S. 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.

[7] 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. no. 1, pp. 131-143, Jan. 2013. 24,

[8] 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.

[9] Mr.SanthoshkumarB.J, M.Tech, Amrita VishwaVidyapeetham, Mysore Campus, India "Attribute Based Encryption with Verifiable Outsourced Decryption." In International Journal of Advanced Research in Computer Science and Software Engineering"Volume 4, Issue 6, June 2014, ISSN: 2277 128X.

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

[11] S. Ruj, A. Nayak, and I. Stojmenovic, ''DACC: Distributed Access Control in Clouds,'' in Proc. 10th IEEE Int'l Conf. TrustCom, 2011.