International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 12, December 2014

A LTERATURE SURVEY ON REVOCABLE MULTIAUTHORITY CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION (CP-ABE) SCHEME FOR CLOUD STORAGE

Vinoth Kumar P, Dr.P.D.R. Vijaya Kumar
[1]*PG Student, INFO Institute of Engineering, Coimbatore*
[2]*Professor of IT department, INFO Institute of Engineering, Coimbatore*

Abstract: In a Cloud Computing the data security achieved by Data Access Control Scheme. 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. 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. Specifically, this paper surveys a revocable multi-authority CP-ABE scheme. The attribute revocation method can efficiently achieve both forward security and backward security. This survey shows that revocable multi-authority CP-ABE scheme is secure in the random oracle model and is more efficient than previous multi-authority CP-ABE.

Key Words—Access control, multi-authority, CP-ABE, attribute revocation, cloud storage

I.INTRODUCTION

Access Control in Cloud Computing:

Cloud computing is one of the emerging technologies. The cloud computing contains huge open distributed system. It is important to protect the data and privacy of users. Access Control methods ensure that authorized users access the data and the system. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security.

Cloud Storage:

The Cloud storage is an important service of cloud computing. The Cloud Storage offers services for data owners to host their data into the cloud. A great challenge to data access control scheme was data hosting and data access services. Because data owners does not fully trust the cloud servers also they can no longer rely on servers to do access control The data access control becomes a challenging issue in cloud storage systems because of data outsourcing and untrusted cloud servers. Therefore **Cloud storage** is a model of data storage where the digital data is stored in logical pool.

ISSN: 2278 – 909X

CP-ABE:

One of the most suitable technologies for data access control in cloud storage systems is Cipher text-Policy Attribute-based Encryption (CP-ABE). This scheme provides the data owner more direct control on access policies.

The Authority in CP-ABE scheme is responsible for attribute management and key distribution. The authority may be the university registration office, the human resource department in a company, etc. The data owner in CP-ABE scheme defines the access policies and encrypts data according to the policies.

CP-ABE TYPES:

In CP-ABE scheme each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies.
There are two types of CP-ABE systems:

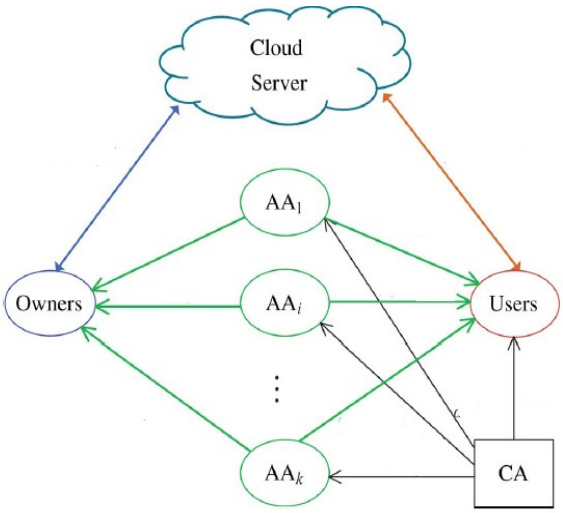
- Single-authority CP-ABE
- Multi-authority CP-ABE

In Single-authority CP-ABE scheme, where all attributes are managed by a single authority.

In a Multi-authority CP-ABE scheme where attributes are from different domains and managed by different authorities. This method is more appropriate for data access control of cloud storage systems. Users contain attributes those should be issued by multiple authorities and data owners. Users may also share the data using access policy defined over attributes from different authorities.

DATA ACCESS CONTROL SYSTEM IN MULTI AUTHORITY CLOUD STORAGE

There are five types of entities in the system AS IN Fig 1: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users). The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity. Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain.



ISSN: 2278 – 909X

In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key. For each user reflecting his/her attributes.

II.EXISTING SYSTEM

In a multi-authority cloud storage system, attributes of user's can be changed dynamically. A user may be join some new attributes or revoked some current attributes.

[1]In 2010, S. Yu, C. Wang, K. Ren, and W. Lou, worked on ''**Attribute Based Data Sharing with Attribute Revocation**,''. This paper use 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.

Drawback:

The storage overhead could be high if proxyservers keep all the proxy re-key.

[2]In 2011, S J. Hur and D.K. Noh, worked on ''**Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems**,''. This paper proposes an access control mechanism based on cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation method. The fine-grained access control can be achieved by dual encryption scheme. This dual encryption mechanism takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. The advantage of this scheme is securelymanaging the outsourced data. This scheme achieve efficient and secure in the data outsourcing systems.

Drawback:

- Huge issue in Enforcement of authorization policies and the support of policy updates

[3]In 2011, S. Jahid, P. Mittal, and N. Borisov, worked on ''**Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation**''.The proposed Easier architecture that 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. We achieve this by creating a proxy that participates in the decryption process and enforces revocation constraints. The advantage of this scheme is the Easier architecture and construction provides performance evaluation, and prototype application of our approach on Face book.

Drawback:

- Does not Achieve Stronger Security Guarantees

ISSN: 2278 – 909X

[4], In 2013, S. Jahid, P. Mittal, and N. Borisov, worked on ‘‘**Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-BasedEncryption**,’’This model proposes the use of dual system encryption methodology. The encryption techniques from Multi-authority ABE and Key-Policy ABE are combined into a single module. Use of MA-ABE technique proves beneficial for key management and flexible access and potential security threat of colluding users is 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.

Drawback:

- Existing attribute revocation methodsrely on a trusted server orlack of efficiency also theyare not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems.
- Each Attribute authorities (AAs) is trusted but can be corrupted by the adversary. Each user is dishonest and may try to obtain unauthorized access to data.

[5][6]**“Attribute-Based Encryption with Verifiable Outsourced Decryption”**. This scheme changes the original model of ABE with outsourced decryption to allow for verifiability of the transformations in existing system. This new model constructs a concrete ABE scheme with verifiable outsourced decryption also does not rely on random oracles.

Drawback:

Security Issue:

Multi-authority CP-ABE protocol allows the central authority to decrypt all the cipher texts, because it contains the master key of the system;

Revocation Issue:

Protocol does not support attribute revocation.

III.PROPOSED SYSTEM

This paper, surveys a revocable multi-authority CP-ABE scheme [5], to solve the attribute revocation problem in the system. This method is an efficient and secure revocation method. The attribute revocation method can efficiently achieve both forward security and backward security. In backward security scheme the revoked user cannot decrypt any new Cipher text that requires the revoked attribute to decrypt. In Forward security the newly joined user can also decrypt the previously published ciphertexts, if it has sufficient attributes. Moreover, while updating the cipher texts, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys.

OVERVIEW OF PROPOSED SYSTEM

- Attribute revocation method can efficiently achieve both forward security and backward security.
- 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.

ISSN: 2278 – 909X

COMPARATIVE STUDY OF EXISTING (MULTIAUTHORITY CP-ABE SCHEME) VS PROPOSED (REVOCABLE MULTIAUTHORITYCP-ABE SCHEME)

SNO	Methods	EXISTING(Multiauthority CP-ABE Scheme)	PROPOSED(revocable multiauthorityCP-ABE scheme)
1	**Entities**	Certificate authority (CA), Attribute authorities (AAs), Data owners (owners), Cloud server(server) Data consumers (users) [5][6].	Global Certificate authority (CA), Multiple Attribute authorities (AAs), Data owners (owners), Cloud server(server) Data consumers (users).
2	**Attribute**	Every secret key is associated with a single AA.[2]	Every secret key is associated with a Multiple AA.
3	**Certificate authority (CA),**	The CA sets up the system and accepts the registration of all the users and AAs in the system [3].	The CA sets up the system and accepts the registration of users and AAs in the system. CA assigns global authority identity aid to each attribute in the system.
4	**Data consumers (users).**	For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user[4].	For each legal user in the system, AA assigns a global user identity **uid** to each user
5	**Attribute authorities (AAs),**	Every AA is an independent attribute authority that is Responsible for entitling and revoking usersattributes [1].	The uid is globally unique in the system .Secret keys are issued by different AAs for the same uid
6	**Data owners (owners),**	Each owner first divides the data into several components and encrypts each data component with different content keys by using symmetric encryption techniques [2].	Data owners may share the data using access policy definedover attributes from different authorities.
7	**Cloud server**	Cipher Text stored and updated into the Cloud Server[4]	Cipher text updated into the cloud server.

ISSN: 2278 – 909X

IV.CONCLUSION

This survey explains a revocable multi-authority CP-ABE scheme that can support efficient attribute revocation. Then the effective data access control scheme for multi-authority cloud storage systems is proposed. It eliminates 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 revocable multi-authority CPABE scheme with Verifiable outsourced decryption and proved that it is secure and verifiable .The revocable multi-authority CPABE is a efficient technique, which can be applied in any remote storage systems and online social networks etc.

REFERENCES

[1]. 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.

[2]. 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.

[3].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.

[4].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,

[5].Kan Yang, and 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.

[6] MrSanthoshkumarB.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.

[7]Tejaswini R M1, Roopa C K2 , Ayesha Taranum "Securing Cloud Server & Data Access withMulti-Authorities" International Journal of Computer Science and Information Technology Research ISSN 2348-120X Vol. 2, Issue 2, pp: (297-302), Month: April-June 2014, Available at: www.researchpublish.com

ISSN: 2278 – 909X