IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 53-59
www.iosrjournals.org

Multi-Authority Data Access Control For Cloud Storage System With Attribute-Based Encryption

G. V. Kapse[1], Dr. V. M. Thakare[2,] Prof. S. S. Sherekar[3], A. V. Kapse[4]
[1](kapsegayatri8@gmail.com, *Department of computer science, S. G. B, Amravati University, Amravati, India)*
[2](vilthakare@yahoo.com , *Department of computer science, S. G. B, Amravati University, Amravati, India)*
[3](ss_sherekar@rediffmail.com , *Department of computer science, S. G. B, Amravati University, Amravati, India)*
[4](abhishekkapse4@gmail.com, *Shankarlal khandelwal senior college of Art, Commerce and Science, Akola, India)*

Abstract: *Data access control is an efficient way to provide the data security in the cloud but due to data outsourcing over untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Attribute-based Encryption (ABE) technique is regarded as a most trustworthy cryptographic conducting tool to guarantee data owner's direct control on their data in public cloud storage. The previous ABE schemes involve only one authority to maintain the complete attribute set, which can bring a single-point hindrance on both security and performance. Paper proposed the design, an expressive, efficient and revocable decentralized manner data access control scheme for multi-authority cloud storage systems, where there are multiple authorities exist and every authority is able to issue attributes independently.*

Keywords - *Access control, Attributes-Based Encryption, data storage, Multi-Authority*

I. INTRODUCTION

Now a day's cloud computing is an intelligently developed technology to store data from number of client. Cloud computing allows users to remotely store their data over cloud. Remote backup system is the progressive technique which minimizes the cost of implementing more memory in an organization. It helps government agencies and enterprises to reduce financial overhead of data management. They can extract their data backups remotely to third party cloud storage providers than maintaining their own data centres. An individual or an organization does not require purchasing the storage devices. Instead they can store their data to the cloud and archive data to avoid information loss in case of system failure like hardware or software failures. Cloud storage is more flexible, but security and privacy are available for the outsourced data becomes a serious concern.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must after encryption of the file, store to the cloud. If a third person downloads the file, they can view the record if they had the key which is used to decrypt the encrypted file. To overcome the problem Cloud computing is one of the emerging technologies, which contains huge open distributed system. It is important to protect the data and privacy of user.

Attribute-based Encryption is one of the most suitable schemes for data access control in public clouds for it can ensures data owners direct control over data and provide a fine-grained access control service. Till now, there are many ABE schemes proposed, which can be divided into two categories; Key Policy Attribute-based Encryption (KP-ABE) as well as Ciphertext Policy Attribute-based Encryption (CPABE). In KP-ABE schemes, decrypt keys are combined with access structures and in ciphertexts it is labeled with special attribute sets, for attribute management and key distribution an authority is responsible. The authority may be the human resource department in a company, the registration office in a university, etc. The data owner defines the access policies and encrypts the data according to the defined policies. Every user will be issued a secret key reflecting its attributes. A user can decrypt the data whenever its attributes match the access policies.

Access control methods ensure that authorized user access data of the system. Access control is a policy or procedure that allows, denies or restricts access to system. It also monitors and record all attempts made to access a system. Access Control can also identify unauthorized users attempting to access a system. It is a mechanism which is very much important for protection in computer security. The Cloud storage is a very important service in cloud computing. The Cloud Storage offers services for data owners to host their data over cloud environment. A big challenge to data access control scheme is data hosting and data access services. Because data owners do not completely trust the cloud servers also they can no longer rely on servers to do access control, so the data access control becomes a challenging issue in cloud storage systems. Therefore the decentralized data access control scheme is introduced.

II. BACKGROUND

A threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, in which multiple authorities jointly manage a uniform attribute set. In TMACS, taking advantage of (*t; n*) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any *t* authorities. Security and performance analysis results show that TMACS is not only verifiable secure when less than *t* authorities are compromised, but also robust when no less than *t* authorities are alive in the system. Further, by efficiently combining the traditional multi-authority scheme with TMACS, construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness [1].

In security analysis of attribute revocation in multi-authority data access control for cloud storage systems proposed the mechanism in dealing with attribute revocation could achieve both forward security and backward security. Analysis and investigation show that the work adopts a bidirectional re-encryption method in ciphertext updating, so security vulnerability appears. Also proposed attack method demonstrates that a revoked user can still decrypt new ciphertexts that are claimed to require the new version secret keys to decrypt [2].

In a semi anonymous privilege control scheme Anony Control to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. The AnonyControl-F, which was fully prevents the identity leakage and achieve the full anonymity. Author's security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption, and author's performance evaluation exhibits the feasibility of scheme [3].

Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. For that designed an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where multiple authorities co-exist and each authority was able to issue attributes independently. Specifically, it proposed a revocable multi-authority CP-ABE scheme, and applies it as the underlying techniques to design the data access control scheme [4].

Sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is a challenging issue, due to the frequent change of the membership. For that proposes a secure multi-owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of this scheme are independent with the number of revoked users [5].

This paper introduces multi-authority data access control for cloud storage system with Attributes-Based Encryption and these are organizes as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected. **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this paper.

III. PREVIOUS WORK DONE

Wei Li, et al. [1] in access control systems for public cloud storage, brings a single-point bottleneck on both security and performance against the single authority for any specific attribute. First design multi-authority access control architecture to deal with the problem. By introducing the combining of (*t, n*) threshold secret sharing and multi-authority CP-ABE scheme, then proposes and realizes a robust and verifiable multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set. Further by efficiently combining the traditional multi-authority scheme with this scheme, construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

Hong, et al. [2] demonstrated that, with the component CUK a revoked user can transform the newly encrypted ciphertext to a previous version, which can be further decrypted with his/her revoked old-version secret keys.

Jung, et al. [3] proposed a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. The proposed scheme was able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F.

The scheme was tolerant against authority compromise, and compromising of up to (N −2) authorities did not bring the whole system down. Author provides detailed about security and feasibility of the scheme. Also implements the real toolkit of a multi-authority based encryption scheme AnonyControl and AnonyControl-F.

Yang, et al. [4] proposed a revocable multi-authority CP-ABE scheme, where efficient and secures revocation method introduced to solve the attribute revocation problem in the system. 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 and forward security. This 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, this scheme can still guarantee the backward security. Then, apply 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.

Liu, et al. [5] to achieve secure data sharing for dynamic groups in the cloud, combined the group signature and dynamic broadcast encryption techniques. This scheme describes the details of Mona including system initialization, user registration, user revocation, file generation, file deletion, file access and traceability. Also this scheme provides security to Mona in terms of access control, data confidentiality, anonymity and traceability.

IV. EXISTING METHODOLOGIES

The scheme structure of TMACS summarised in Fig. 1. In TMACS, *AA*s must firstly register to *CA* to gain the corresponding identity and certificate (aid, aid.cert). Then *AA*s will be involved in the construction of the system, assisting *CA* to finish the establishment of system parameters. *CA* accepts users' registration and issues the certificate (uid, uid.cert) to each legal user. With the certificate, the user can contract with any *t AA*s one by one to gain his/her secret key (*SK*). Owners who want share their data in the cloud can gain the public key (*PK*) from *CA*. Then the owner can encrypt his/her data under predefined access policy and upload the ciphertext (*CT*) to the cloud server. User can freely download the ciphertexts (*CT*) that he/she is interested in from the cloud server. However, he/she can't decrypt the ciphertext (*CT*) unless his/her attributes.

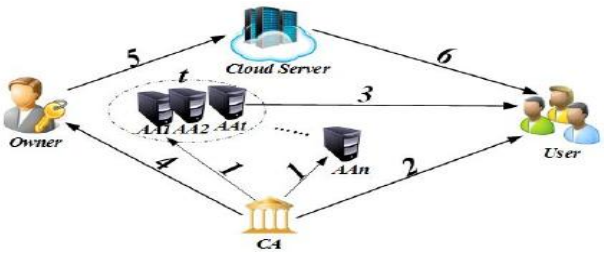

Fig. 1: Framework and Basic Protocol Flow

(1) *AA* registers to *CA* to gain (*aid; aid:cert*);
(2) User registers to *CA* to gain (*uid; uid:cert*);
(3) User gains his/her *SK* from any *t* out of *n AA*s;
(4) Owners gain *PK* from *CA*;
(5) Owners upload (*CT*) to the cloud server;
(6) Users download (*CT*) from the cloud server [1].

DAC-MACS contain five algorithms: System Initialization, Secret Key Generation, Encryption, Decryption and Attribute Revocation. To prove the security, the authors propose a game between a challenger and an adversary, and draw a conclusion that DAC-MACS are secure under the decisional q-parallel BDHE assumption. However, this game makes a connotative restriction that the adversary could not get CUKxk of any revoked attribute [2].

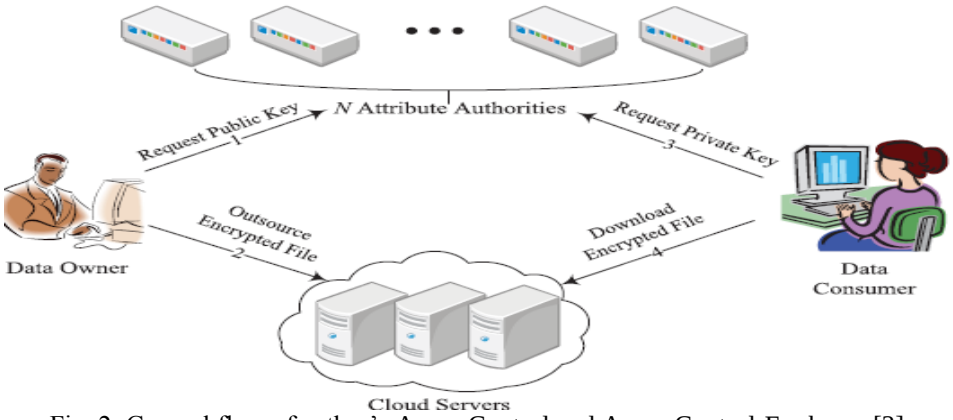

Fig. 2: General flow of author's AnonyControl and AnonyControl-F scheme [3]

In this system, there are four types of entities: N Attribute Authorities, Cloud Server, Data Owners and Data Consumers.

A user can be a Data Owner and a Data Consumer simultaneously. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them. Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree Tp can execute the operation associated with privilege p. The server is delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree Tp [3].

Author proposes a new revocable multi-authority CP-ABE protocol based on the single-authority CP-ABE proposed by Lewko and Waters. That is author extend it to multi-authority scenario and make it revocable. Author apply the techniques in Chase's multi-authority CP-ABE protocol to tie together the secret keys generated by different authorities for the same user and prevent the collusion attack. Specifically, author separate the functionality of the authority into a global certificate authority (CA) and multiple attribute authorities (AAs). The CA sets up the system and accepts the registration of users and AAs in the system. It assigns a global user identity uid to each user and a global authority identity aid to each attribute authority in the system. Because the uid is globally unique in the system, secret keys issued by different AAs for the same uid can be tied together for decryption. Also, because each AA is associated with an aid, every attribute is distinguishable even though some AAs may issue the same attribute. To deal with security issue in Multi-Authority Attribute Based Encryption, instead of using the system unique public key to encrypt data, author's scheme requires all attribute authorities to generate their own public keys and uses them to encrypt data together with the global public parameters. This prevents the certificate authority in scheme from decrypting the ciphertexts. To solve the attribute revocation problem, author assigns a version number for each attribute. To improve the efficiency, author delegate the workload of ciphertext update to the server by using the proxy re-encryption method, such that the newly joined user is also able to decrypt the previously published data, which are encrypted with the previous public keys, if they have sufficient attributes [4].

To achieve secure data sharing for dynamic groups in the cloud, Authors expect to combine the group signature and dynamic broadcast encryption techniques. This group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users.

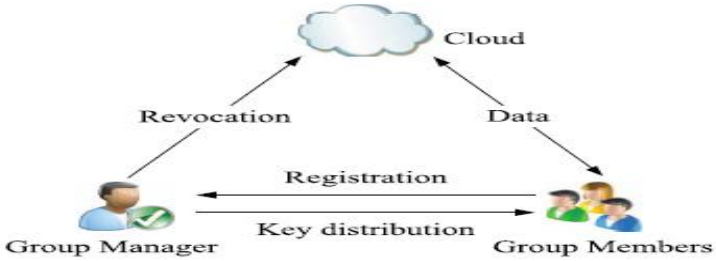

Fig. 3: System model for MONA [5]

V. ANALYSIS AND DISCUSSION

Author proposes a new threshold multi-authority CP-ABE access control scheme TMACS, in public cloud storage, in which all *AA*s jointly manage the whole attribute set and share the master key α. Taking advantage of (*t, n*) threshold secret sharing, by interacting with any *t AA*s, a legal user can generate his/her secret key. Thus, TMACS avoids any one *AA* being a single-point bottleneck on both security and performance. The analysis results show that author's access control scheme is robust and secure. It can easily find appropriate values of (*t, n*) to make TMACS secure when less than *t* authorities are compromised, also robust when no less than *t* authorities are alive in the system. Further, based on efficiently combining the traditional multi-authority scheme with TMACS, construct a hybrid scheme that is more suitable for the real scenario. This scheme addresses attributes coming from different authorities, security and system-level robustness [1].

Author analyzes the shortcoming of DAC-MACS in dealing with attribute revocation. And found that, if a revoked user wants to access the unauthorized content whose access policy can be satisfied by his/her revoked attributes, the only thing to do is to use author's proposed attack algorithm to transform the new-version ciphertext to the old-version one if he/she can collude with the cloud service provider to get enough ciphertext update keys. The security vulnerability exists because DAC-MACS wrongly use a bidirectional re-encryption scheme in the ciphertext updating procedure. This vulnerability allows any party to re-encrypt the ciphertext between old-version and new-version, only if he/she can get the CUKs between these two versions [2].

Author's proposed schemes achieved fine-grained privilege control and identity anonymity while conducting privilege control depends on user's identity. More important is, this system can tolerate up to $N - 2$ authority compromise, which is mostly prefer specially in Internet-based cloud computing environment. Also conducted security and performance analysis which shows that AnonyControl both secure and efficient for cloud storage system. The AnonyControl-F inherits the security from the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer [3].

Author proposed a revocable multi-authority CPABE scheme that could support efficient attribute revocation and constructed an effective data access control scheme for multi-authority cloud storage systems. Author also proved that this scheme was provable secure in the random oracle model. The revocable multi-authority CPABE is trustworthy technique, which can be applied in any remote storage systems and online social networks etc [4].

Authors designed a secure data sharing scheme Mona for dynamic groups in an untrusted cloud. In Mona, users are able to share data with others in the group without revealing identity privacy to the cloud. Also, Mona is efficient in user revocation and new user joining. More specially, efficient user revocation can be achieved by public revocation list without updating the private keys of the other remaining users, and new users can directly decrypt files stored in the cloud without their participation. Moreover, the storage overhead and the encryption computation cost are constant. By analysis it is proved that proposed scheme was satisfy the security requirements and efficiency [5].

Table 1: Comparison between various data access control scheme with Attribute-Based Encryption

Data access control techniques	**Advantages**	**Disadvantages**
Threshold multi-authoriy ciphertext-policy(CP)ABE accesscontrol sceme(TMACS)	1) It satisfies the scenario of attributes from different *AA*s 2) It can achieve security and system-level robustness.	Reusing of the master key shared among multiple attribute authorities (*AA*s).
Comments and corrections of CP-ABE	Analyze the shortcoming of DAC-MACS in dealing with attribute revocation, main construction proved it secure	Security vulnerability

Privilege control scheme AnonyControl AnonyControl-F	1) Able to protect user's privacy against single authority. 2) Tolerant against authority	1)Data confidentiality 2)Personal information defined by each user's attributes set is at risk 3) Resilient in security breach.
Attribute revocable multi-authority CP-ABE scheme	1) It incurs less communication cost and computation cost, and is secure 2) It can achieve both backward and forward security	Lack of efficiency
Secure multi-owner data sharing scheme MONA	1. Reduced the computation overhead to encrypt files and cipher text size. 2. The ciphertext size is constant and independent of revocation users.	1)User compute revocation parameters to protect the confidentiality 2) computation overhead of the encryption

VI. PROPOSED METHODOLOGY

6.1 Data access control system in multi owner cloud storage

There are five entities in system as shown in Fig. 2, a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users). A global trusted certificate authority in the system is CA. CA sets up the system and also accepts the registration of all the users as well as AAs in the system. For each legal user in the system, the CA assigns a unique user identity to it and also generates a unique public key for that user. However, the CA do not involved in attribute management and creation of secret keys that are associated with attributes.

For example, the CA may be the Social Security Administration, an independent agency of the United States government. Every user can be issued unique Social Security Number (SSN) as its global identity. Each AA is an independent attribute authority that is responsible for entitling and revoking users attributes according to their role or identity in its domain. In this proposed scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. And each AA has total control over the structure and semantics of its attributes. Every AA are responsible for generating a public attribute key for every attribute it manages and a secret key for each user reflecting their attributes.

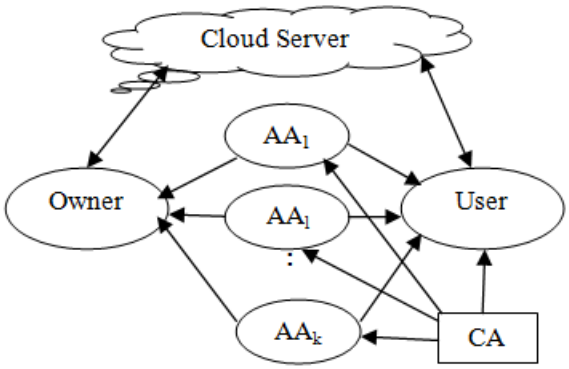

Fig. 2: Decentralized manner data access controlling

VII. OUTCOME AND POSSIBLE RESULT

In a multi-authority decentralized data access controlling system attributes are from different fields and managed by different authorities. This method is most appropriate for the data access control of cloud storage systems. Users contain attributes that would be issued by multiple data owners. Users can also share the data using access policy defined with attributes from multiple authorities.

VIII. CONCLUSION

Proposed a revocable decentralized data access control system can support efficient attribute revocation for multi-authority cloud storage systems. It eliminates decryption overhead of users according to attributes. This secure attribute based encryption technique for robust data security that is being shared in the cloud. This revocable multi-authority data access scheme with verifiable outsourced decryption and it is secure and verifiable. This scheme will be a promising technique, which can be applied in any remote storage systems and online social networks etc.

IX. FUTURE SCOPE

One of the promising future works is to introduce the efficient user revocation mechanism on top of proposed anonymous ABE. Supporting user revocation is an important issue in the real application, and this is one of the greatest challenges in the application of ABE schemes. Making this scheme compatible with existing ABE schemes, support efficient user revocation.

REFERENCES

[1]. Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", *IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2015.*

[2]. [7] Jianan Hong, Kaiping Xue and Wei Li, "Comments on "DAC-MACS: Effective Data Access Control for Multi-authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi-authority Data Access Control for Cloud Storage Systems", *IEEE transactions on information forensics and security, VOL. 10, NO. 06, June 2015.*

[3]. Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", *IEEE transactions on information forensics and security, VOL. 10, NO. 01, January 2015.*

[4]. 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. 07, July 2014.*

[5]. Hideaki Ishii, Roberto Tempo, and Er-Wei Bai, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", *IEEE Transactions on parallel and distributed systems, VOL. 24, NO. 06, June 2013.*