Data Security Using Multi-Authority Data Access Control for Cloud Storage System

[1]P. Maneepa, [2]Dr. P. Venkateswara Rao,[3]Dr. V. Sucharita,
[1]Scholar ,[2]Professor&HOD,[3]Professor,
Computer Science Engineering Department,
[1] Narayana Engineering College, Gudur-524101, Nellore –Dist., A.P.

Abstract: **The Data access control is an effective way to ensure the data security in the cloud. Due to the data outsourcing and the un-trusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. The Attribute based Encryption on multi owner data access was the method with low cost and good efficiency but it has some security problems. In this paper I design a secure data access control mechanism for multi – authority cloud storage, where a file can be uploaded to cloud environment and it can also be shared by the data owner, the people who are all sharing the file will be getting the secret key which is an encrypted one. I increase the security on the Multi – Authority system by two methods 1: Attribute based, 2: Encryption of attribute by secret key. Test results show our system is secure and efficient.**

Keywords **– Cloud Storage, CP-ABE, Data Access Control, Multi Authority.**

I.INTRODUCTION

Now a day's cloud computing is an intelligently developed technology to store data from number of client. The Cloud computing allows users to remotely store their data over cloud. With the Remote backup system which 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 centers. Moreover an individual or an organization does not require purchasing the storage devices. Instead they can also 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 the security and the privacy are available for the outsourced data becomes a serious concern.

To achieve secure data transaction in cloud, relevant cryptography method is used. The data owner later 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 strategy 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 Cipher text Policy Attribute-based Encryption (CPABE). In KP-ABE schemes, decrypt keys are combined with access structures and in cipher texts 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 here defines the access policies and encrypts the data according to the defined policies. Every type of 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 approach nail down that authorized user access data of the system. Access control is a guideline that allows, denies or restricts access to system. It also guides and record all attempts made to access a system. Access Control can also identify unauthorized users attempting to access a system. It is a structure 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 but also to host their data over cloud environment. A big challenge to data access control scheme is the data hosting and data access services. Because the 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 type of data access control scheme is introduced.

II.SYSTEM AND SECURITY MODEL

System Model for data access control in multi-authority cloud storage is considered. There are five types of entities in the system.

1. A certificate authority (CA)
2. Attribute authorities (AAs)
3. Data owners or vendors (owners)
4. Cloud server (server)
5. Data consumers (users)

CA could be an international credible certificate authority within the system. It sets up the system and acquire the registration of all the users and AAs. For every legal user within the system, the CA assigns a worldwide discrete user identity and additionally

generates a global public key for the user. Every user are going to be disseminated a Social Security range (SSN) as its international identity. Every AA is Associate in nursing freelance attribute authority that's responsible for entitling and revoking user's attributes according to their role or identity in its domain. In the proposed theme, each attribute is related to a multiple AA, however every AA will manage Associate in nursing discretionary number of attributes. AA has full management over the structure and rudiments of its attributes each AA has full control over the structure and linguistics of its attributes. Each AA is liable for generating a public attribute key for every attribute it manages and a Secret key and update key for every user reflective his/her attributes.

Each user contains a international distinctiveness within the system. User may be cumulating a collection of attributes which can come back from multiple attribute authorities. The user can revive a secret key related to its attributes entitled by the corresponding attribute authorities.

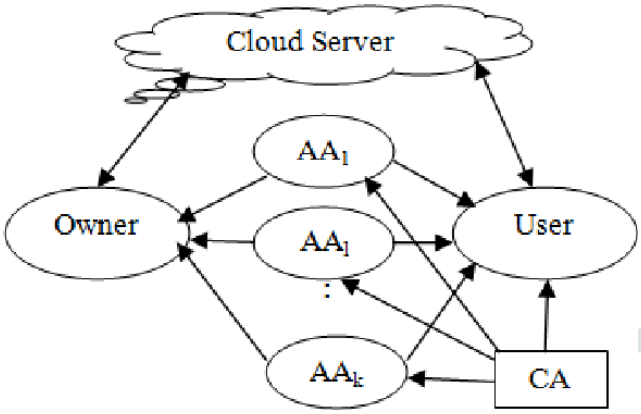

Figure-1: System layout of DAC in multi-authority cloud storage

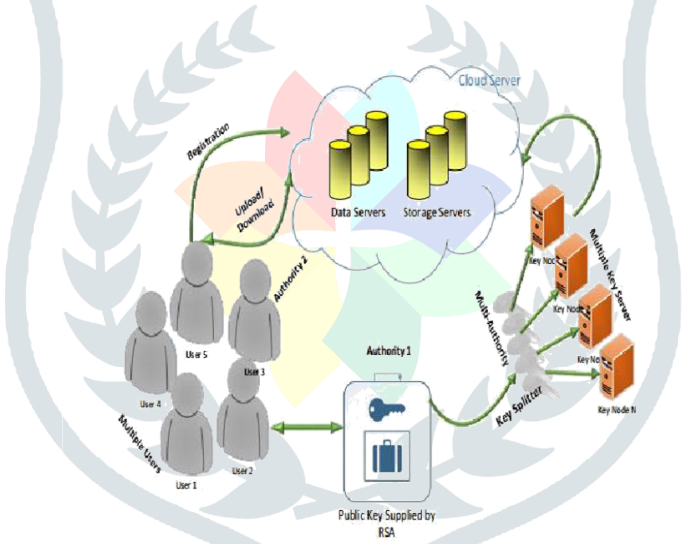

Figure-2: Proposed security framework (FAC-MACS)

The key secret's breach into N items and keep into multiple key servers. Each head most owner distributes the information into many hunks according to the logic granularity encrypts every knowledge component with totally different content keys by profiteering regular encryption tactics. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys below the protocols.

Then, the owner sends the encrypted knowledge to the cloud server in connection with the cipher texts. They are doing to not trust the server to try and do knowledge the access management. But, the access mainframe happens within the cryptography.

If the user's attributes satisfy the access policy outlined within the cipher text; the user is in a position to unravel the cipher text. Thus and so users with completely contrasting attributes will decode different number of appeased keys and therefore get totally different granularity of information from a similar data. The proposed stuff is in a position to surface the below challenges:

1. Protect user's privacy against each single authority.

2. Indulgent against authority compromise, and conciliate of up to (N − 2) authorities does not bring the whole system down.

3. Provides the detailed scrutiny on security and performance to show feasibility of our scheme.

4. The real toolkit of multi-authority based encryption scheme is actualized.

A.Security framework:

The groundwork has been designed to misconduct the below outlined elements of layers. The planned theme is employed to regulate the deployed data and supply the quality of the cloud storage service for the cloud users with Associate in Nursing economical encoding and decryption ciphering and multiple key server with key fissure techniques. This multi-authority CP-ABE provides permits that in control of attribute management, economical computation, key distribution and the revocation ways. The Area are unit of seven layers outlined within the planned theme. The practicality of these layers is summarized as follows:

i) **Proxy layer:** This proxy layer acts as articulate between the users and the rest of the servers available in the cloud.

Ii) **Cloud data server layer**: Data server has two different quantity can be recognized as the cloud users and the cloud service provider. Multiple data servers are advised in this scheme to avoid the traffic.

iii) **Cloud data storage server layer**: All the data and the files are stored in these storage retainers which are stored by the both individual client and organizations. Identical to the data server there are diverse storage servers are introduced to handle big volume of data.

iv) **Cloud Key Server layer**: Multiple key servers are proposed in this scheme for efficient computation and attribute revocation method. Key server is accustomed store the secret key that are encrypted or fragmented by the key plotter.

v) **Key sputter**: Key sputter is used to divide cryptographic key K in n safe pieces K 1, K 2, Kn Such that knowledge of any J pieces can be used to compute K easily. These pieces are assigned to N nodes. The Algorithm is to divide Key in n parts, K z, Kn such that there is a special part Kt which contains the information of all alternate parts, and K cannot be computed without Kt. However, K cantor to be computed without a special part Kt.

vi) **Cloud Consumers Layer**: Cloud buyers are the one who have the data to be stored in the cloud and depend on cloud for data computation and transformation. Cloud consumers can be both consumers and individual organizations.

vii) **Cloud Service Provider (CSP):** This layer inherits, built and manages the storage servers in distributed manner and functions as live cloud computing systems.

III.ANALYSIS AND DISCUSSION

Author come up with a new threshold multi-authority CP-ABE access control scheme TMACS in public cloud storage, in which all AAs 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 AAs, 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 inquiry results show that author's access control scheme is robust and secure. It can easily find relevant 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 merging 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 contrasting authorities, security and system-level robustness [1].

Here the author analyzes the short-comings 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 cipher text to the old-version one if he/she can collude with the cloud service provider to get enough cipher text update keys. The security vulnerability exists because DAC-MACS wrongly use a bidirectional re-encryption scheme in the cipher text updating procedure. This vulnerability allows any party to re-encrypt the cipher text 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 crucial is, this system can tolerate up to N − 2 authority accord, which is mostly prefer specially in Internet-based cloud computing environment. Also conducted security and performance analysis which shows that Anomaly Control both secure and efficient for cloud storage system. The Anomaly Control-F acquires the security from the Anomaly Control 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 volatile 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 [4].

Authors devised a secure data sharing scheme Mona for dynamic groups in an un-trust cloud. In Mona, users are able to share data with others in the group without revealing identity privacy to the cloud. Also, Mona is capable 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 decrypted files stored in the cloud without their participation. Moreover, the storage hanging and the encryption computation cost are constant. By analysis it is proved that proposed scheme was amusing the security requirements and efficiency [5].

Data Access Control techniques	Advantages	Disadvantages
Threshold multi-authority Cipher text-policy(CP)ABE access control scheme(TMACS	1) It satisfies the scenario of attributes from different AAs 2) It can achieve security and system-level robustness.	Reusing of the master key shared among multiple attribute authorities (AAs).
Comments and corrections of CP-ABE	Analyse the shortcoming of DAC-MACS in dealing with attribute revocation, main construction proved it Secure.	Security vulnerability.

Table-1: Advantages and Dis-advantages

Privilege Control scheme Anomy Control-F	1. Able to protect user's privacy against single authority. 2. Tolerant against authority.	1. Data confidentiality. 2. Person information is 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 MONA.	1. Reduce the computation overhead to encrypt files and cipher text-size. 2. The cipher text size is constant and independent of revocation user.	1User compute revocation parameters to protect the confidentiality. 2. Computation overhead of the encryption.

Table-2: Comparison between various data access control scheme with Attribute-Based Encryption

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 credible certificate authority in the system is CA. CA composes 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 a self-reliant 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 correlate with a single AA, but each AA can manage an arbitrary number of attributes. And each AA has total govern over the structure and explication 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.

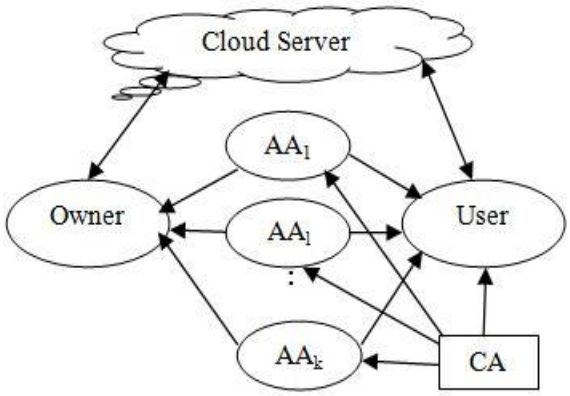

Figure-3: Decentralized manner data access controlling

V. OUTCOME AND POSSIBLE RESULT

In a multi-authority decentralized data access controlling system the attributes are from the different fields and managed by different type of authorities. This methodology 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 be shared the data using access policy defined with attributes from multiple authorities.

VI.CONCLUSION

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

VII. FUTURE SCOPE

One of the exposition 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. By making this scheme compatible with existing ABE schemes, support efficient user revocation.

VIII. ACKNOWLEDGMENT

I sincerely express gratitude to my supervisor Prof. Dr. P .Venkateswara Rao for his guidance, invaluable input, suggestions, generous help and inspiration in all stages of my work. I was introduced about very interesting topic of, “Data Security Using Multi-Authority Data Access Control for Cloud Storage System”. His intellectual abilities have always rescued me in the difficult situations. It would not have been possible for me to complete this thesis without the guidance and support of him. Dr.P.Venkaeswara Rao is ME., Ph.D. with total 20 Years of Teaching Experience, 1 year industry experience in Malaysia and 7 years research experience. He published 25 papers in various reputed journals and 1 Book and 2 Book Chapters Published so far and 30 conference proceedings. Currently working as a professor and Head in CSE Department in Narayana Engineering College, Gudur.

IX. 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]. 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 FullyAnonymous 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.

[6]. A.Sahai, H.Seyalioglu, and B.Waters, “Dynamic credentials and ciphertext delegation for attribute-based encryption,” in Proc. Adv. Cryptol. — CRYPTO 2012. New York, NY, USA: Springer, 2012, pp. 199–217.