Multi-Authority Cipher Text Policy Attribute Base Encryption On Cloud Storage

[1]Fulsoundar Priyanka Sunil, [2]Mr. Rathod V .U

pfulsoundar99@gmail.com, vijayrathod25bel@gmail.com

[1]Students, Department of Computer Engineering,

[2]Prof., Department of Computer Engineering,

Vishwabharati Academy's College of Engineering, Ahmednagar (MH), India

Abstract : Cloud computing provides Cloud storage as a service to the users for hosting their data in the cloud. Data access control is the well-organized method to provide data security in cloud. The proposed revocable multi-authority CP-ABE scheme provides solution to the attribute revocation problem. The proposed scheme updates the components of the revoked attribute only and generates latest secret keys for the revoked attribute and forwards it to the non-revoked users who have the attributes as revoked attributes. The backward security and Forward security is assured. If the revoked user enters into the system again by doing the registration process means, the particular user is identified via the identity card detail in the revocation list and will not be added to the system, so that they are stopped at the registration phase itself.

Keyword: Data encryption, Attribute-based Encryption, data security ,cloud computing

I. INTRODUCTION

Cloud computing is an developed technology to store data into from number of client. Cloud computing users allows to store their data over cloud. The progressive technique is remote backup system which minimizes the cost of implementing more memory in an organization. It can be helps government agencies and enterprises to reduce the financial overhead of data management. They can extract data backups remotely to third party cloud storage providers than maintaining their own data center. An individual organization does not require purchasing the storage devices. Instead of they 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 flexible, but security and privacy are available for the outsourced data becomes a serious issues. To achieve the secure data transaction in cloud, suitable cryptography method tobe used. The data owner must after encryption of the file, store the cloud. If a third person downloads the file, they can view the record and if they had the key which is used to decrypt the encrypted file. To overcome this problem Cloud computing is one of the best technologies, which is contains huge open distributed system. It is an important to protect the data and privacy of user.

Attribute-based Encryption is one of the best most suitable schemes for the data access control in public clouds for it can be ensures data owners direct control over the data and it can be provide a fine -grained access control service. Now, there are many ABE schemes that is proposed in cloude , which can be divided into two types categories; Key Policy Attribute -based Encryption (KP-ABE) and the Ciphertext Policy Attribute-based Encryption (CPABE). In KP-ABE schemes, decryped keys are combined with access structures and in cipher texts it is labeled with special attribute sets , for the 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 can be defines the access policies and encrypts the data according to the defined policies. Every user that will be issued a secret key reflecting its attributes. A user can be decrypt the data whenever its attributes match the access policies. Access control methods that can be ensure that authorized user access data of the system.

Access control is a policy or procedure that can be allows, denies or restricts access to system. It also monitors and record all attempts made to access a system. Access Control can also identify the unauthorized users attempting to access a system. It is mechanism which is very much important for protection in computer security. The Cloud storage is an very important service in cloud computing. The Cloud Storage offers services for data owners to host their data over cloud computing environment. A big challenge of the 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 is becomes a challenging issue in cloud storage systems. Therefore the decentralized data access control scheme to be introduced.

II. LITERATURE SURVEY

A. Multi-authority access control system

In this paper [1] they have explained access control systems for the public cloud storage, brings a single-point bottleneck on both side security and performance against the single authority for any specific attribute. Firstly design multi -authority access control architecture to deal with the problem. By introducing the combining of (t, n) threshold value 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 authoritie and achieving security and system-level robustness.

B. Attribute Revocation

In this paper [2] they proposed demonstrated that, with the component CUK a revoked user can be transform the new encrypted cipher text to a previous version, which can be further data decrypted with his/her revoked old-version secret keys.

C. Data access privilege and anonymity

In this paper [3] they proposed a semi-anonymous attribute-based privilege scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. In this 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 the feasibility of the scheme. Also it can be implements the real toolkit of a multi-authority based encryption scheme AnonyControl and AnonyControl-F.

D. Efficient and revocable data access

In this paper [4] they proposed a revocable multi -authority CP-ABE scheme, where efficient and secures revocation technique introduced to solve the attribute revocation problem in the system. Attribute revocation method is an 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 the 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. At that time, apply proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for the multi-authority cloud storage systems.

E. Secure multi-owner data sharing for dynamic groups

In this paper [5] they proposed to achieve secure source of 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 revocation ,user registration, file generation, file deletion, file access and the traceability. Also this scheme can be provides security to Mona in terms of access control, data confidentiality, anonymity and traceability.

F. Provably secure scheme under keyword guessing attack

In this paper [6] they proposed allows a third party knowing the search trapdoor ofa keyword to search encrypted documents containing that keyword without decrypting the documents .However, it is shown that the keyword will be compromised by a malicious third party under a keyword guess attack (KGA) if the keyword space is in a polynomial size. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. Cloud service providers are separate administrative entities, moving to the commercial public cloud deprives users of direct control over the systems that manage their data and applications. To enable ranked searchable symmetric encryption for the effective utilization of the outsourced cloud data under the different model. Exploitring the signatures to compute verification metadata needed to audit the correctness of shared data.

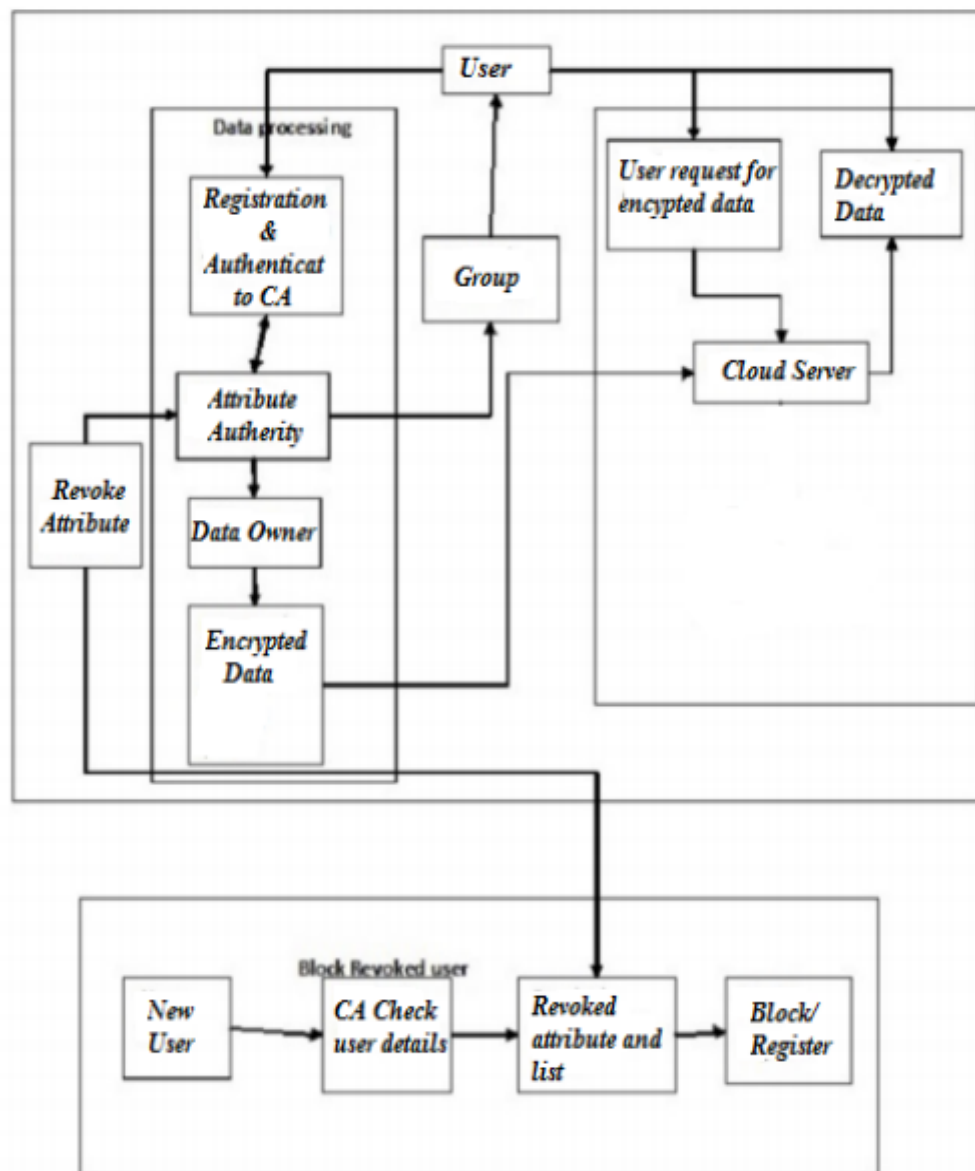**III. PROPOSED METHODOLOGY**

    A.   Architecture

Fig .1. System Architecture

1.   Registration :

Each user registers to the CA by providing their details. CA provides a global unique ID and certificate for each user who entering into the system. AA should also be registered to the CA. For each AA, CA provides Global unique ID and submits the certificates provided for each user in the system. The user details, AA details are stored in database.

2.   Authentication :

Users provide the id obtained from CA, while login for the data access in CSP. CSP validates the id using the details stored in database. If the id is valid, users are allowed for the data access in cloud, Otherwise access is denied for the user.

3.   Data Processing and Encryption by owner:

Data Processing The data owners first split the data into multiple components according to logical granularity. Data owner collects the attributes generated by the AA and design the access policy for each attributes.

4.   Encryption by Owner:

The data owner encrypts the data with content keys using symmetric encryption algorithm. Then the content keys are encrypted based on access policies of each attribute and send the encrypted data together with Cipher texts to the cloud.

5.   Decryption by user

The user requests for the data to the cloud. If the users attribute and access control rights are satisfied, user can download the data from the cloud. User first decrypts the data for the content keys using their secret keys. Using the content keys user decrypts the original data.

B. FLOW CHART
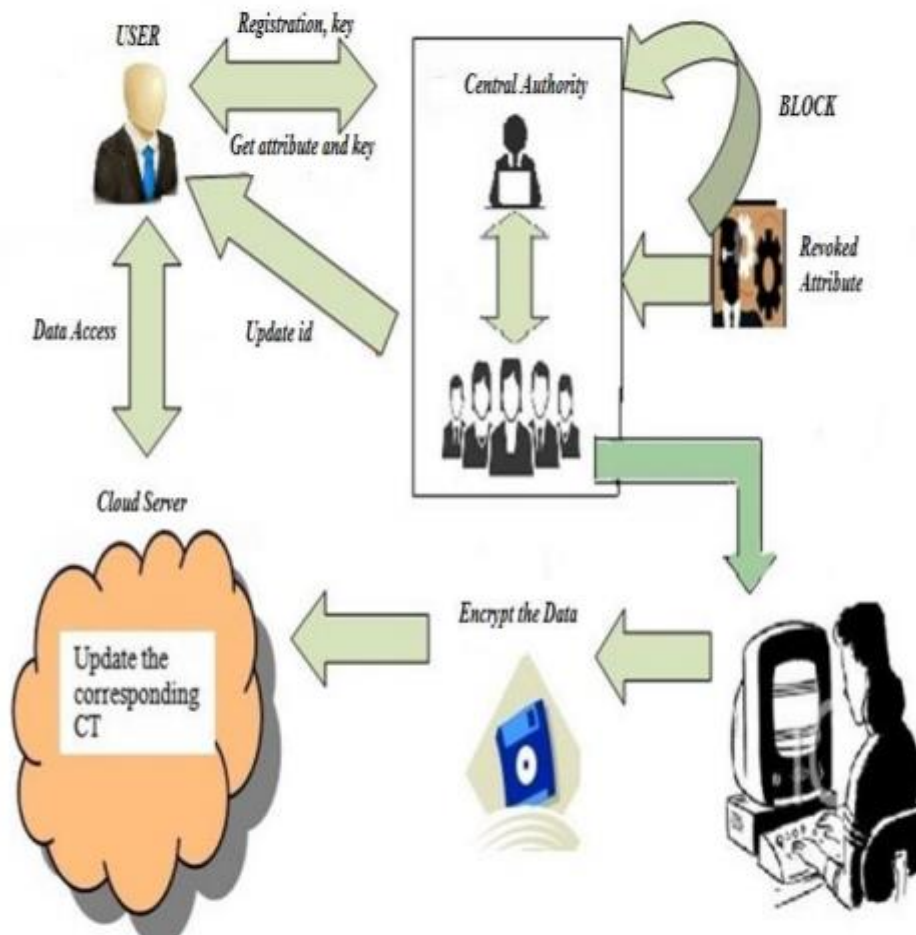
Proposed Description

1) Data Owner: They are responsible for uploading the files and granting access permission to the users of the respective group user. Admin has the main access permission for maintaining the files over cloud. Admin can navigate through the group as well. Admin can view the log details of the activities carried on the cloud file storage.

2) User: Every user needs to register with the corresponding group for getting access permission and signature key from the same. Using the signature key they can get the access permission. They can upload the files to cloud. User from same group can view the content of the file from cloud and make changes over it and can save them. Simultaneously they can download the files as well.

3) Third Party Auditor (TPA) TPA has the rights to validate the files which are available in the cloud. TPA is the respective authority for performing the verification of files which are uploaded by any user who are registered under a single group.

4) User Operations: User can revoke their account at any cost. The file key will be generated while upload each file into the cloud. Every member can view the files which are available for the download access through the group. This is the list of files available in the cloud for members.

IV. RESULT AND DISCUSSIONS

We have created system in java. Data is stored in mysql database. We have created a web application with local server. Web application that communicates with local server and Trustee Server using REST API. We have uploaded text document on cloud. We have evaluated file audit management, user activity analysis and file key generation. In table 1 and table 2, the computational speed of encryption and decryption and the complexity analysis of the reported and proposed algorithm have been mentioned.
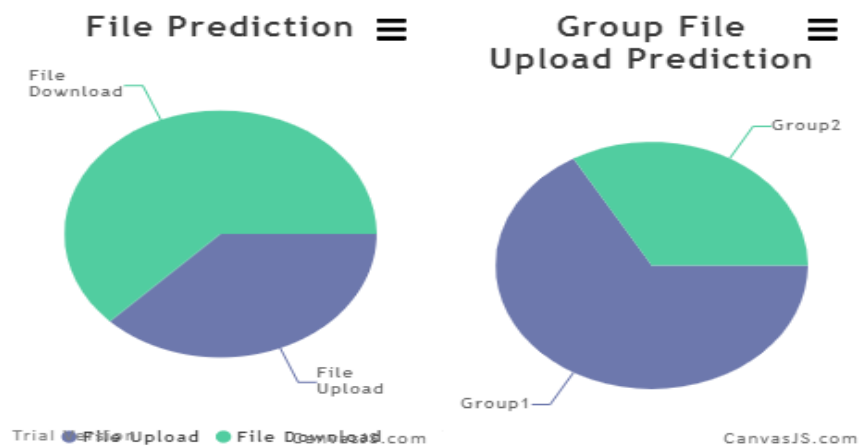
V. CONCLUSION

Revocable multi-authority CP-ABE scheme that can be support efficient attribute revocation. The constructed and effective data access control scheme for multi-authority cloud storage systems. The revocable multi-authority CP-ABE is a most promising technique, which can be applied in any remote storage systems and the online social networks etc.

REFERENCES

[1] Wei Li, and JiananHong, "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, 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 the Cloud Storage Systems", IEEE transactions on information forensics and security, VOL. 10, NO. 06, June 2015.

[3] Taeho Jung, Xiang-Yang Li, "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 XiaohuaJia, " Efficient, and Revocable Data Access Control for Multi-Authority in Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.

[5] Hideaki Ishii, 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] Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute-based encryption," in SP'07.IEEE Computer Society, 2007, pp. 321{334.

[7] BhartiRatan Madnani,Sreedevi N, Attribute Based Encryption for Scalable and the Secure Sharing of the Medical Records in Cloud Computing Design and Implementation" Interrnational Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3May 2013.

[8] B.Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and proxy-ably secure realization," in PKC'11. Springer, 2011,pp. 53.

[9] Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, B Waters - Public Key Cryptography{PKC 2011, 2011.

[10] D. Boneh and M.K. Franklin, Identity-Based Encryption from the Weil Pairing," in Proc. 21st Ann. Int'l Cryptology Conf.Advances in Cryptology - CRYPTO'01, 2001, pp. 213-229.

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

[12] 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.