Re-Distributed Multi-Authority Attribute Based Encryption in Cloud Using CP-ABE Algorithm

1Siddhardha T, 2Murugaanandam., 3Sri Nithin D, 4Raghuveer V.

1-4Department of Information Technology, SRM Institute of Science and Technology, Chennai, India.

Abstract: Cloud Computing allows us to store and share the data easily with others. Re-distributed multi-authority Attribute-Based Encryption (ABE) has importantly implemented for finding the solutions to the problem that which arises from sharing private corporate information in computing of cloud. For Re-distributed multi-authority ABE in cloud devices that don't believe in a single main authority, collusion resistance are often done employing a universal identifier, so for that reason, identity must be globally managed, that ends up within the critical issues of privacy and protection. The new scheme is implemented that doesn't use a single main authority in order to co-ordinate users and keys, and only normal trust relations got to be done with sharing the general public key in between each attribute authority (AA). The identities of the user are different and different by combination of the user's identity along the identity of the AA where the user is found. If a key request must be made to the authority outside of the domain, the request must be done by the authority within the present domain instead of by the client's, so, the user identities should remain secured to the AA outside the domain that can strengthen privacy and protection. Along with that, the main issuing protocol in between Attribute Authority is straight forward because of the results of trusted AA relationship. On top of that, the authority’s extensibility is also supported by the method presented in our paper. The scheme is predicated on order of Composite in which the groups are bilinear. Validation of protection is given which uses the twin system methodology of encryption.

Keywords— Cloud Computing, Data Sharing, Cipher text-Policy Attribute-Based Encryption (CP-ABE), Key Distribution, Encryption, Decryption, Group Creation.

1. Introduction
Cloud computing in these days is the most essential service and the cloud services are being available all over the globe irrespective of the location. Cloud computing gives us many services where, allocation of storage, encryption of data are some of the examples. These cloud services are provided by many different cloud service providers and all are not trust-worthy. These cloud services may be free or either some paid services. The cloud space being provided will decide the cost of the particular person’s cloud space. In these days cloud space is the most used service for the purpose of data storage and data transfer.

Cloud capacity is very major benefit and vital benefit worldview of cloud computing. Advantages by utilizing cloud capacity incorporate more noteworthy openness, higher unwavering quality, fast deployment and stronger security, to title fair a couple of. In spite of the mentioned benefits, this worldview too brings forward modern challenges on information get to control, which could be a big or major to guarantee information secured or privacy. Since cloud capacity operations done by cloud benefit the one who is providing service, who are more often than not exterior the trusted space of...
information proprietors, the conventional get to control strategies within the Server/Client demonstrate for cloud capacity environment. The information get to control in cloud capacity environment has in this way ended up a challenging issue. To address the issue of information access control in cloud capacity, there have been very numbers of. Plans proposed, among which (CP-ABE) is respected as one of the foremost promising procedures. The striking advantage of CP-ABE that is awards information proprietors coordinate control

As we are able see the high utilization of these cloud administrations there emerges a few security issues where a few of the possible and frequently happening issues are that the data may well be misplaced or the information may well be stolen, that's the third party enters without the consent of the information proprietor. There are tall chances for the information to be misplaced with the utilize of any untrusted cloud spaces or the cloud space having less security.

In spite of the fact that the control plans that which are present or based on the CP-ABE, they has a lot of plus points and also the plans are not robust and at the same time they are not effective also whey they have to generate key.

Actually there is only one single in charge is present in almost all single authority plans, offline/crash of this authority makes all secret key demands inaccessible during that period. We face nearly similar issue available or present in multi-authority plans, since each of different authorities oversees attribute set.

Cloud space suppliers ought to make sure that the space provided to any specific individual should be possessing the highlights of giving the security for both information capacity and information exchange. There are numerous possibilities for the information to be stolen in case of the cloud space being utilized by the suppliers which are not trust-worthy, those are just like the third party entrance into the personal data is simple in the event that there exists no security, and the information could be stolen.

Secure Computing is known as the security which is connected to the data in all areas. This security provides protection from any sort of unplanned circumstances. It primarily concentrates on the provision of information encryption and security. For numerous reasons passwords are being shaped in such a way that they are extreme to break out. It is known as the bridge between the client and any sort of framework.

In order to make sure that the information is secured a few essential detailing for the information encryption is done, where the information assurance isn't so simple. There are numerous cloud space suppliers and a few security frameworks joined to it such as Data Encryption Standard(DES), and Cipher text-Policy Attribute-Based Encryption (CP-ABE) etc where they given a specific key on the ask of the client to the proprietor.

The main aim of the proposed framework is the information security and it is done utilizing this type of encryption is this type foremost broadly utilized and adopted algorithm for the encryption of the information which are in charge these days. The main use or the advantage of CP-ABE is it allows Information proprietors coordinate control depends on some of the defined policies

- In CP-ABE, we have given with some attributes that which are nearly or equal to the decryption key of the user, and then the policy also results in change of the cipher text.
- The brief knowledge that have about the CP-ABE has been switched: presently cipher text related with the granted access and the encrypting party decides the approach by the information that which has can be changed, whereas we’ve hidden key that attached with the present attribute set

**Objective:**

1. Attribute based Encryption for different group security
2. Over all Authority control by central authority
3. Secure the data in cloud environment like college and company on large data sharing

**2. Literature Survey**

D.Wei Li, [1] The prior ABE plans include single particular specialist that who checks and coordinates the complete set, which will have the result in a one-point bottleneck which will provide both the security and as well as the performance. Afterwards, a few dual-authority plans came into existence, among the different specialists independently keeping the no joint attribute subsets. In any
In our present paper, different point of view, that which have an edge dual-authority control access scheme to the open cloud capacity, among the different authorities mutually oversee normal set with the attributes

Gangeshkumar C Rahangdale [2] said that almost all the systems that which are already existed and also depend on the (ABE) plans, there is having just one expert specialist within system and remaining common keys are that which has been issued by the authorised person so that’s the reason why that leads to the cipher text estimate and which leads to the extra costs within the encryption and the operations which hasn’t been scrambled yet. so that’s the drawback why he proposed a dual or double-Authority scheme so of all the specialists not relate to make the information which is open in the midst of the system initiation stage.

Khaled Riad [3] he made some discussions about the drawbacks or the problems of multiple people also can be able to get the permission for authorization so that is the reason why most of the people are facing the serious problem in the cipher text-policy attribute-based encryption. So that’s the reason why came up with a new dual-authority access scheme control model for cloud capacity double-authority framework scheme was discussed depends on which the user’s attributes for trust calculation. And his new model make sure allowing get to for the trusted clients whereas securing the clients given identity

Ruqayah R. Al-Dahhan,[4] proposed that the new scheme which they have been developing in the conference that the scheme is really a huge advantage, strong method and also supported to build safe access control system. Anyway this technique is really different and preserving the information only on a the private system that which can handled by the single person. So an unused new scheme is presented so that it handles almost all the present given work’s restrictions and safely permits protecting information on open cloud capacity system by utilizing different authorized persons for the single set.

Xiaoyu Li, Shaohua Tang, [5] made profound research about Attribute-based encryption, particularly for this type of encryption that which is made on attribute based, can utilize the working and to have the control over the cloud capacity frameworks. In our paper we did some research and came up with the idea of the two-factor security for the double-authority cloud capacity frameworks. In the new scheme that which we proposed , any person can recuperate information that which is outsourced in the event that and only in the event that this client have the capacity that can handle the keys which has been kept secret with regard to the get to approach authorization key in respect with the outsourced information.

F Huang,[6] In cloud computing, the encryption scheme was developed for the data that which is outsourced. during this paper, for the primary time, we have a tendency that can be studied and also have the capacity to solve difficulty in the customized pair of key words positioned look about the disorganized information whereas protecting and also providing the security or the privacy in cloud computing also important. So that’s the reason why we discuss about two PRSE plans various searchable engines. Broad tests are conducted on the data sets that which are available approve the investigation and also looks like that our projected arrangement exceptionally effective.

ZFu, X. Sun, [7] With the expanding selection in the department or the domain of the cloud computing, one can see the rapid increase in the growing of clients and also their datasets are outsourced. So the data that which is in the form of sets ordinarily they scrambled some time recently outsourcing to protect security. We did some research and came up with the idea, we developed an imaginative new look scheme that which nearly equal to the hierarchy also the possible relationship among the concepts within data that which are scrambled.

K.Xue, [8] he said that the cloud computing is a very large domain sharing the information is very frequent and in order to solve it we have to come with a design and we got two major problems in this thing and a test is done the scheme that we have proposed and it is giving good accurate results.

Wu, Z. Wei, and H. Deng [9] they proposed a unique Multi-message Cipher text Approach Attribute-Based encryption (MCP-ABE) procedure, and utilizes the MCP-ABE to design an get to control scheme for sharing scalable media based on info consumers’ attributes. Besides, the paper shows a
way to support resource-limited versatile devices by offloading computational seriously operations to cloud servers whereas while not compromising information privacy. S. Aljawameh [10] made a study about the proposed algorithms before the threat to the stored data is less. Then the study makes sure that the features of the existing and recently proposed are completely different and the proposed system is a bit secure in the way of encryption of the data to another level where the data cannot be accessed by the private key and that is also provided by the admin only if the user is an authorized user. This infers the proposed system about the security of the data being uploaded to be encrypted in a way that the data is not to be stolen and only with the specific permission and the access key, the data is to be decrypted.

3. Proposed Methodology
Here we display a Dual or Double-Authority ABE with user security no need of the particular specialist. These requirements are in-significant to fulfill, due in both cases to the collusion resistance prerequisite of ABE. We furthermore present a mysterious key supply protocol which permits multi-authority ABE with upgraded client privacy

1) We permit the clients to communicate with AAs by means of pseudonyms rather than having to supply their GIDs within the clear, and
2) We anticipate the AAs from pooling their information and connecting numerous attribute sets belonging to the same client

A. User Module
The information consumer (client) has to register first. After the registration is done the client has given with particular unique user identification (user identity) by Central Authority. So then the consumer incorporates a given particular number of attributes such that they are related to a anonymous key connected with client quality number of attributes. Then the client will simply have disorganised information from the supplier who provides the cloud service. In any case, the client will unscramble the disorganised data only when client set of attributes fulfils the policy that which is defined within the data that which is encrypted.

B. Owner module
Data provider (Owner) characterizes the login policy about who has to get permission to view each record, later scrambles the data given in the file under the particular systematic approach. Let begin of all, particular single owner scrambles particular person data can be change by the symmetric encryption calculation. At that time, the owner defines get to approach over a property set the next scrambles the particular key by the approach concurring by the open key gotten passed by CA. The next to that the person who provides the service passes the total scrambled information along with the scrambled symmetric key (indicated according cipher text CT) from the server where the information is kept within a cloud server.

C. Admin module
Admin may be super consumer. They will check all the consumer and owner details. Admin will see the chart based on the most range of word look, they will include the specific connected word, so the consumer will effectively mapping connected words for case Uncertainty level two alludes to occasions that almost all people assume as equivocal. These occurrences contain few or more not connected senses, like “apple” (apple maybe a fruit and conjointly apple may be a Smartphone company) and “jaguar” (jaguar maybe a animal and conjointly a automobile company). This work, we mainly consider the clarification of occurrence.

D. Attribute Authority module
These are the main reason for doing the client authenticity confirmation and producing middle keys for authenticity confirmed clients. Our one is not at all like previous existed plans where unique AA
oversees which is not a combine property on individual basis, our planned theme includes varied specialists client authenticity confirmation so that every AA will perform this prepare can autonomously. So that the particular AA chosen, such that make sure client’s genuine attributes done by normally either confirmation conventions, then produce a halfway key that which is related to traits that which has been genuinely checked. The middle key can be a modern construct that assist CA to create more keys.

E. Central Authority module
Main specialist (central authority) is the one who actually controls the whole framework. That is the main reason to framework development by keeping system limits and producing open verification text for every public attribute set. Within framework data formatting stage, it allots every client a one of a form user identification every authority has given a special Attribute identity. In order to ask a verification text from the client, the main authority is capable so that it can produce anonymous keys to the client so that they can get the intermediate key related to client’s real attributes that which is verified through the attribute authority. So the one who actually runs the whole framework, so that the central authority has enough potential that follow attribute authority perniciously confirmed that a client will allow ill-conceived sets. The cloud server offers a public platform for owners to store and share their disorganized info. So that the server of the cloud won’t have the info gets to regulate for the one who provides service. So that the disorganized info is kept inside the cloud server and it can be downloading without access by any client.

Fig. 1. Architecture diagram and proposed methodology

Fig. 2. Framework and system implementation
4. Implementation

A. System Implementation
The system is implemented in Net beans using Java programming language. The information is sent to the cloud server only when the user details authentication is successful. The details provided by any client or user at the time of the registration are asked to be entered for the purpose of authentication and the particular user can be logged in to the provided space to view, upload or delete their own files. when the user or client after login into his/her account they can edit the file content. They can also view the files belonging to other data owners and if the files of other owners are needed then the user places a request to the owner and if the owner is interested to share the files then he will be sending a particular key

B. Encryption of Data
The file that which contains the information is particularly specified by the system and then the information is placed in the cloud space and retrieved in the same format when the request is placed to the particular data owner. This key generation CP-ABE schema is having greater strength than comparing to the other algorithms.

The encryption and decryption strategy in the case of CP-ABE algorithm is faster than the DES and RSA algorithms. The accuracy is also high in the case of this approach. If any of the tests is to be conducted for knowing the accuracy of the algorithm then the precision is found for different algorithms towards the cipher technique and the one having the highest accuracy can be confirmed to be the algorithm being used in the approach.

C. Delay Calculation
The encryption time is noted for the calculation of the delay. And, the difference is stated using the files of different size such as 8MB, 24MB, 50MB, 83MB. And the time is calculated in seconds where the below depicted graph shows the difference between the time taken by different size files to be uploaded into the cloud space.

![Fig. 3. Encryption Time](image)

![Fig. 4. Algorithms working across different schemes](image)
There are different features which can explain the uniqueness and the strength of the approach. The comparison of the stated algorithms can be depicted using the following:

Fig. 5. Cloud Based Server Incorporating Attribute Based Encryption (Abe) Processes

5. Results and discussions
The information is encrypted by the CP-ABE algorithm in plan to be attacked from third party uses. As there is no scope for third party clients, once the client is verified, at that time the entrance of any malwares is avoided. If the confirmation isn't demonstrated by the client at that time the precise client cannot move further. Presently, after the effective confirmation of any client all the groups from all clients are often seen and hence any client who has any requirement of a selected record, can put a ask at the record and which itself ends up in the owner of the precise file. And at that time the owner gets a ask and on the off chance that the owner is interested to share is/her records at that time the reaction from owner is sent to the precise asked individual. And at that time he are often planning to the records and once the record is gotten to by a selected key the key’s consequently changed and a brand new key's created. And with the identical key any record can not be opened twice. This basically decreases the false sharing of critical information. Usually, achieve

6. Conclusion
In our present paper, we implemented contemporary system, to kill the direct one-point execution of the present CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION plans.Therefore by successfully changing CP-ABE cryptographic strategy into current system, so our new strategy provides a vigorous and productive get to regulate with a single central authority or the multi-authorities for open cloud capacity. Our plot utilizes numerous AAs to provide the stack of the time-taking authenticity confirmation and modern entries of client’s demands. More over we presented a fully secured strategy that follow a property authority’s wrong behaviour check. Therefore a detailed security and execution examination is made so that to check whether the conspire is safe and productive. So that the safety examination results gives that our could method would be effective .Other than, with the new inspecting & following conspire, no Attribute Authority might not accept it’s gotten out of hand key conveyance. Encourage execution analysis

References
[1] Li Wei et al "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage" IEEE Transactions on parallel and distributed systems 275 (2015): 1484-1496
[2] Rahangdale Gangeshkumar C and Archana Raut "An approach for advanced multi-authority access control system for public cloud storage" 2017 International Conference on Innovations in Information Embedded and Communication Systems (ICIIECS) IEEE 2017
[3] Riad Khaled "Multi-authority trust access control for cloud storage" 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS) IEEE 2016
[4] Al-Dahhan Ruqayah R et al "Revocable Decentralized Multi-Authority Access Control System" 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion) IEEE 2018 [5] Li Xiaoyu et al "Two-factor data access control with efficient revocation for multi-authority cloud storage systems" IEEE Access 5 (2016): 393-405

[5] Kurosawa Kaoru and Yasuhiro Ohtaki "How to update documents verifiably in searchable symmetric encryption" International Conference on Cryptology and Network Security Springer Cham 2013

[6] D Cash S Jarecki C Jutla H Krawczyk M-C Ros, u and M Steiner “Highly-scalable searchable symmetric encryption with support for boolean queries” in Advances in Cryptology–CRYPTO 2013 2013 pp 353–373

[7] S R Lenka and B Nayak “Enhancement of the Data Security in Cloud Computing using RSA Encryption and MDS algorithm “ vol 2 no 3 pp 60-64 2014

[8] C Bosch Q Tang P H Hartel and W Jonker “Selective document retrieval from encrypted database” in ISC 2012 pp 224–241

[9] Fu Zhangjie et al "Enabling personalized search over encrypted outsourced data with efficiency improvement" IEEE transactions on parallel and distributed systems 279 (2015): 2546-2559

[10] Masadeh Shadi R et al "A comparison of data encryption algorithms with the proposed algorithm: Wireless security” The 6th International Conference on Networked Computing and Advanced Information Management IEEE 2010

[11] Ramakrishnan B Durdu A Rajagopal K and Akgul A 2020 Infinite attractors in a chaotic circuit with exponential memristor and Josephson junction resonator AEU-International Journal of Electronics and Communications 123 p153319

[12] R “Kaur “Effective Symmetric key Block Ciphers Technique for Data Security :RUNDAEL” vol 3 no 7 pp 2005-2008 2014”

[13] P" Kalpana “ Data Security in cloud computing usingRSA algorithm " vol 1 no 4 pp143-146 2012"

[14] Balamurali R and Chandrasekar A 2019 Multiple parameter algorithm approach for adult image identification Cluster Computing 22(5) pp11909-11917

[15] Fu"Zhangjie et al "Towards efficient content-aware search over encrypted outsourced data in cloud" IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications' IEEE 2016"

[16] Xue Kaiping and Peilin Hong "A dynamic secure group sharing framework in public cloud computing" IEEE Transactions on Cloud Computing 24 (2014): 459-470