SECURED FINE-GRAIN ACCESS CONTROL AND DATA SHARING FOR DYNAMIC GROUPSIN CLOUDS

[1]Srinivasulu M, [2]Aishwarya S Pujar, [3]Ashwini B, [4]Shambhavi R, [5]Patil Rushitha, [6]Madhu M P

[1]Asst.Professor, [2,3,4,5,6]Students
Department of Master of Computer Application
UBDTCE, Davangere

Abstract: **In this study, we present a key update model with a successful key access control scheme for use in a data outsourcing scenario. We combine role-based access control (RBAC) and ciphertext policy-attribute-based encryption (CP-ABE) for access management. The suggested approach aims to improve the initial CP-ABE management attributes and key updates. The attribute certificate (AC) in our scheme, including a user's password, which is used to decrypt the plaintext encrypted using CP-ABE policy. If the qualities listed on the keys are changed (updated or revoked), the key in the AC will be changed in response to the access request. Compared to traditional CP-ABE-based techniques, this significantly reduces the overheads related to key distribution and upgrading for all users at once. We conclude by conducting a test to assess the effectiveness of our suggested strategy.**

***Keywords*: CP-ABE; attribute certificate; access control, password update; performance**

1. INTRODUCTION

Data exporting to a third party, such as a provider of cloud services, is becoming more common as a result of economies of size and effective resource management. However, privacy and security are two of the most significant challenges with adopting data outsourcing services such as cloud computing. Because they are designed to enforce rules in organizations where traditional access control strategies, such as mandatory access control (MAC), discretionary access control (DAC), and role-based access control (RBAC), are ineffective in situations requiring data outsource. The resources are in the hands of data owners. Although cloud services are usually believed to be reliable, the confidentiality of data that has been outsourced remains at risk. Data secrecy in an electronic world must be protected by encryption.

When a great deal of users accesses the same shared data, symmetric encryption incurs key maintenance expenses and key distribution issues; however, public key encryption not only provides robust security but also several copies of the encrypted information since it encodes the data with each user's common key. To ensure data privacy and secure access control, attribute-based encrypting has become common in the data access control methods being used in cloud computing. Most of the time, the ABE technique can be combined with bilateral and public key encryption to give fast encryption and digital signatures. [11, 15].

The attribute-based encryption (ABE) method, first proposed by Be and later refined by Court et al. [1], is also referred to as ciphertext-policy attribute-based encrypting (CP-ABE). Each CP-ABE user has a unique set of attributes that are stored in their private key. The ciphertext is related to the accessibility policy structure, which is defined by the ciphertext's developers or data owners. Ciphertexts can be decoded if a user's features match the encrypted text access pattern. Several CP-ABE-based approaches have been proposed thus far. [2,4,5,7-9] to lower key management costs, boost encrypting and performance, and handle user and attributes revocation. These methods, however, are compliant with the CP-ABE method's extra cryptographic-based upgrading, and policy flexibility in representing user privilege is no longer a concern. Most revocation analyses make a great deal of completely proxy re-encryption (PRE). [10, 12, 13, 16] to minimize the expense of calculation on the part of the data owner.

However, synchronous updates to keys and key distribution are costly overheads generated by feature revocation or policy amendment. The majority of studies have neglected these issues, and current PRE methodologies lack a focus on them.

This paper proposes a novel access control approach termed an Attributes Certificate - Cryptography Policy. The attribute role-based encryption (AC-CP-ARBE) architecture has been proposed to enhance the adaptability and effectiveness of key management in the current CP-ABE-based scheme [1-4, 11]. To do this, we use attribute certificate (AC) from the Power Management Interface (PMI) to set up the CP-ABE scheme's authentication function on remote systems. These certificates specify the attribute profiles of the readable user. According to our approach, the AC can hold an organised attribute-role structure and its associated key for decoding a file protected by the CP-ABE access policy. When the AC is assigned to a specific user, the computation and communication expenses required by an information owner or attribute authority (AA) in updating and sending the encryption keys to all current clients in the case of attribute revocation are significantly reduced. This paper contributed the following contributions, which are summarised below:

1. Our suggested AC-CP-ARBE access management model offers a workable
2. connection between user decryption key management based on the attribute certificate (AC) and CP-ABE-based data encryption.
3. The suggested model is completely compatible with public key infrastructure, which requires an X.509 client password authentication certificate and the ability to confirm the AC's issuer. Consequently, it is possible to establish seamless PKI and

PMI integration to raise access control trust.

4. Our AC-CP-ARBE scheme offers no key distribution costs and does not require an expensive computation to update keysfor all current users, in contrast to the original CP-ABE scheme.
5. We provide an attribute certificate management system that is extremely scalable and safe in order to make automated enrolments and updating.

2. LITERATURE REVIEW

The majority of current ABE, or encryption based on attributes Encryption with key-policy attributes (KP-ABE) [3, 5] is categorized into two groups. and attribute-based Encryption using ciphertext policy (CP-ABE) [1], is the foundation for cloud computing access control methods data outsourcing. The ciphertext used in KP-ABE is linked to a group of characteristics and the personal secret key is established to go along utilizing the access framework. The coded text may therefore to easily encrypt using group of characteristics that anybody can perform and is independent the access guidelines. The access guidelines is therefore not entirely underthe data owner's control CP-ABE, on the other hand encrypts data using an access policy framework that was created by the data owner. One user's characteristics must be consistent with the ciphertext access structure in request for them to decipher a ciphertext. Several works [2-4, 7, 8, 11] have suggested MA-ABE, or multi-authority attribute-based encryption enable a more complicated cloud computing ecosystem with several owners and authorities.These studies usually concentrate onresolving the revocation problem, decreasing the price of encrypting data and decrypting it,and improving the security of cryptographic processes.

By adding a hierarchical user structure to The authors of [2] HASBE, or hierarchical attribute-set- cryptography that is based on alternative to A set-based approach to encrypting (ASBE) for ciphertext.In this method, a trusted authority generates and disseminates the root master keys, top-level domain authorities, and system parameters.for the purpose of revocation and re-encryption procedure, owner of the data must be reachable throughout the time range agreed upon among users.

The authors of [3] propose to develop a scalable, fine-grained data access management system for individual medical documents (PHRs)utilising encryption based on attributes. The topic of access management in situations with various ownership of authorities is covered in the article. This technique, which allows writing access, grants a time-related signature to the requestors who are allowed to write the data. However, in revocation management, which is reliant on the global The cost of key re-generation and file re-encryption, or CP-ABE is linearly linked to the clients and the size of the policy.

Current CP-ABE-based systems especially rely on the cryptographic activities performed by the data owner or AA re- generating and giving users access to keys when there a policy change or revocation. These pricey overheads will increase rapidlyif there are numerous users.

3. BACKGROUND

3.1Attribute-Based Ciphertext Policy Encryption (Cp-Abe)

As an alternative type Using attribute-based encryption (ABE) for access control, Bethencourt and other. [1] presented encryption based on ciphertext policy attributes.In a sense, the bilinear maps formats the basis of both ABE's cryptographic construction. Following is An explanation of what bilinear maps are officially defined as:

Bilinear Maps

G1 and G2 are two multiplicative cyclic groups with prime order p and e, respectively, and let e be a bilinear map: G1 G1G2. Let g be. the G1 H: 0,1* G1 generator should be a hash function indicating the random oracle nature of the security model.The following characteristics apply to the Map bilinear e:

- **e(ua, bilinearity exists, vb) = e(u, v)ab for all u, v G1 and any a, b Zp**
- **Non-degeneracy: e(g, g) ≠1.**

Defined 1:Access Tree r . Let r represent an entry structure as a tree. each threshold gate of which is identifiable by its offspring With an upper limit, are the non-leaf nodes of the tree. If node x has num_x children and k_x is numx follows its threshold value. = 0 kx. The entrance gate is an AND gate when $k_X = num_X$ and an OR gate when $k_X = 1$. Each leaf node x of the tree is described by an attribute and a threshold value of kx = 1. It is also possible to use the threshold gate in r for k of n; in In this instance, kx equals k, with k the threshold value. selected by the k of n gate.

3.2 Role-Based Access Control

A user's role, rights, and resources or objects are connected in accordance with the RBAC access control paradigm.

Definition 2: (U, R, P, UA, PA, RH) in a tuple is an RBAC.

- U, R, and P include sets that, respectively, correspond with respect to the group of users, roles, and permissions.
- Many-to-many user- assignment of roles (UA U R) relation;
- A many-to-many system. permission- roles assigned to each called PA, P, and R;
- The role hierarchy is represented by the partial order RH R R on R.

The RBAC paradigm in favor of role progression which a role may be organised in a hierarchy. The hierarchy's top role is situated there, whereas weaker jobs are placed on the lower levels.

3.3 Extension of Access Tree

To increase the expressiveness and scalability with the CP-ABE to include the RBAC paradigm, we describe the The following is the attribute-role-based (A-RBAC) access control model:

Definition 3: The four components of A-RBAC are U, R, P, UA, RH, D, APA, and Attr, where:

- In the RBAC model, U, R, P, and UA, and As, and RH

- The link between D, R, and Attr is a permission-to-role assignment that is many-to-many.
- PA ⊂ Attr × P is a permission-to- attribute attribution.

A user u (∈ U) in a cloud computing environment is an entity that has been given a particular The role ru (R)and asks for permission to reach a resource p (∈ P), such as reading and writing. A group of characteristics referred to as Attr are utilized to describe Role Ru. The attribute authority AA publishes a list of attributes.

In our access management system with cryptography approachan access control policy (ACP) is the term used to describe the expanded access tree. that is utilised for data files' encryption. Figure 1 is an illustration of a policy ring for access controls in a patient treatment system. Data Owner, RoleA, and Role B are the three primary roles in the policy, and each is granted a distinct level of access privileges to the prescription information.

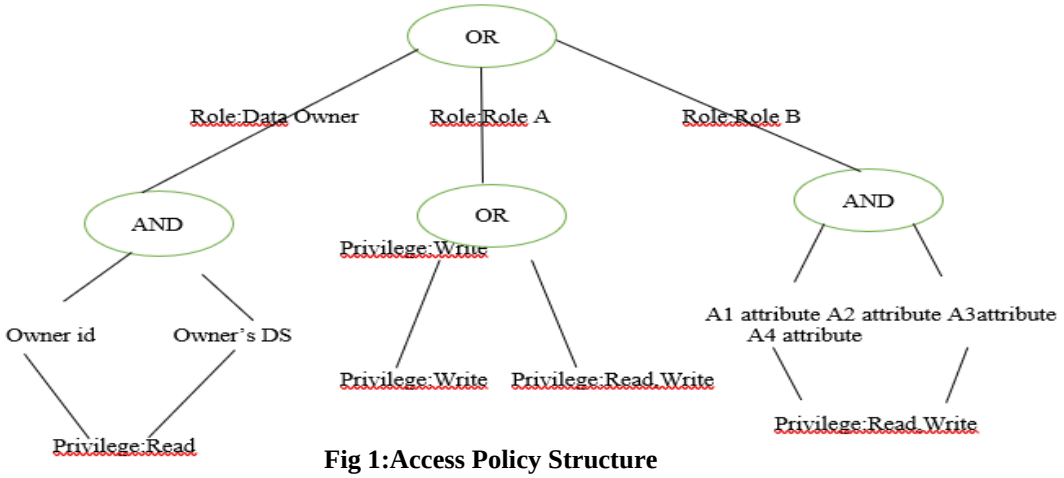


Fig 1:Access Policy Structure

The recommended record is encrypted using the access structure mentioned above. Only Role A and Role B areable to write this file as of Figure 1. After updating the file, users in Role A are expected to reach this and employ it to encode the specified records.

3.4 Privilege Management Infrastructure (PMI)

The authorization process ITU-T Recommendation-based X.509 is referred to as "privilege management infrastructure"(PMI). The Attribute certificates are used by PMI (AC) to store User rights as attributes. As opposed to attribute attestation, which accustomed to store permission Certificates for public keys (PKCs) store Authentication details and information (privileges). While AC must by the issuing attribute authority (AA), be digitally signed, PKCs are typically issued by the certification authority (CA), and the PKC verifies The initials of the AA. Additionally PKC is the, employed to verify the accuracy that of the AC holder identity when claiming rights with this attribute certificate. Therefore, the PKC's existence contributes to the verification of an AC. In AC, a set of attributes may be revised. due to the potential change in attributes.

- AC Issuer AC Holder
- The algorithm that signed this AC.
- Serial No. and the duration of this AC's validity
- The order in which the holders of the attributes are bound, with any further possible elaborations.
- Extensions are utilized to describe further details, such as time, goalsusers, rules, and policies, in addition to privilege revocation, roles, the power source, and delegation of power.

- **4. OUR PROPOSED ACCESS CONTROL MODEL AC-CP-ARBE**
- A Model for Authorization Overview
- The incorporation of attribute certificates in this study improves the user key management of CP-ABE. RBAC is incorporated into CP-ABE at the model's core to increase the CP-ABE policy's expressivity definition handling a number of characteristics is part of the CP-ABE process. The interaction of the AC-CP-ARBE components is seen in Figure 2.

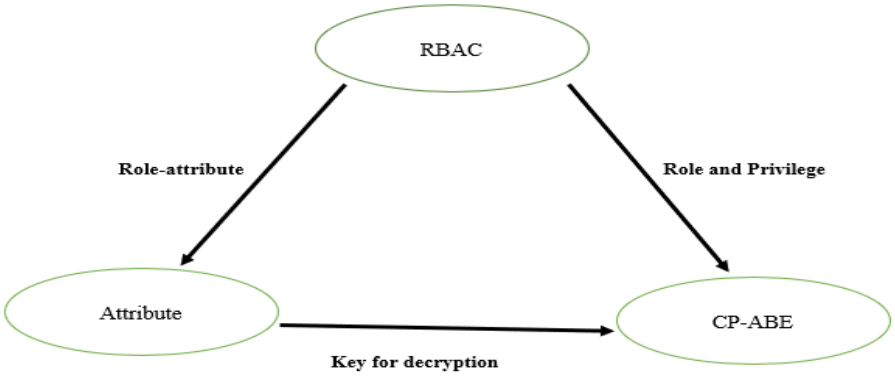


Figure 2. CP-ABE, RBAC, and AC combined into one authorisation mechanism

In essence, as the method of CP-ABE key management, particularly on a grand scale Deployment of CP-ABE, When an attributeis updated or revoked, there is a non-trivial overhead for key modifications. In some applications, it may also be necessary to provide identity verification based on the availability of attribute data. To provide more scalable and useful authorization in a multi-authoritycloud, we suggest as well as put the enhanced model AC-CP-ARBE. In contrast to the current CP-ABE methods, which disseminate encrypted keys to users using, the AC-CP-ARBE technique embeds a key created from AA or the AC's owner of data. The CP-ABE access policy is used to enforce authorization, much as how Data encryption is carried out using the CP-ABE.

4.1 Design of Attribute Certificate for Storing User Decryption Key

The AC model is a built on top of Table 1 of RFC 3281. displays the AC features especially designed to facilitate role-based authorisation and the CP-ABE architecture. The attribute field displays a group of qualities that are assigned to a certain part in AC structure. Every time the value of an attribute changes, the user decryption key (UDK) field for that attribute can be modified.

TABLE 1. CERTIFICATE OF ATTRIBUTION

Holder of the Certificate: John Smith
AuthorityHos1 CA(AA1) is the issuer.
System: SHA2RSA
Identifier: 25ACB56
2016/01/20 through 2017/01/19
Characteristics Information Role: Doctor Attribute: Name: John SmithOffice: Tokyo Hospital: ALevel: 8Position: Full MD General MD Type Specialty: CardiologistHire Date: 01/10/2008   Extension: [xs4445475fdsefsd4f24] for EDK. (E[r€ R ZP, D, gr], Random Key Component: Exp.Time)

A key value that is determined by a certain role and the traits that go with it,which are provided by AA, is used to decrypt the data using the CP-ABE policy to encrypt. The benefit of the authorised ACP's role will be activated Then the user can use the to access the file allocated privilege if a certain set of trait included in AC fulfils an ACP.Our model states that since the user may Sign up when AC and receive the key. encoded in the AC, there are no costs associated with key distribution. Two elements are presentin the extension field: (1) the UDK is an encrypted value used as the key value for a collection of characteristics visible (2) The components of the encrypted key in the AC. assembled to create a UDK. The bilinear map's random r € Zp, a Key generator g and key component D make up the random key component.

5.SNAPSHOTS

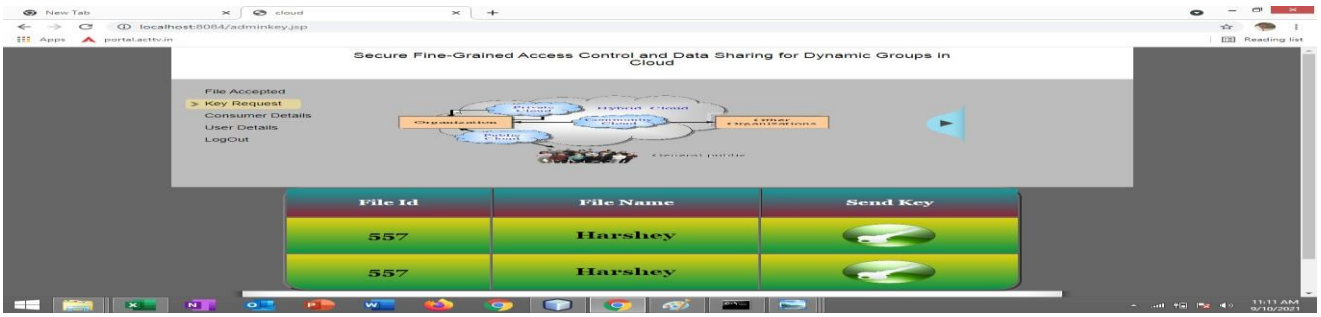
Fig 3.1 Main Page

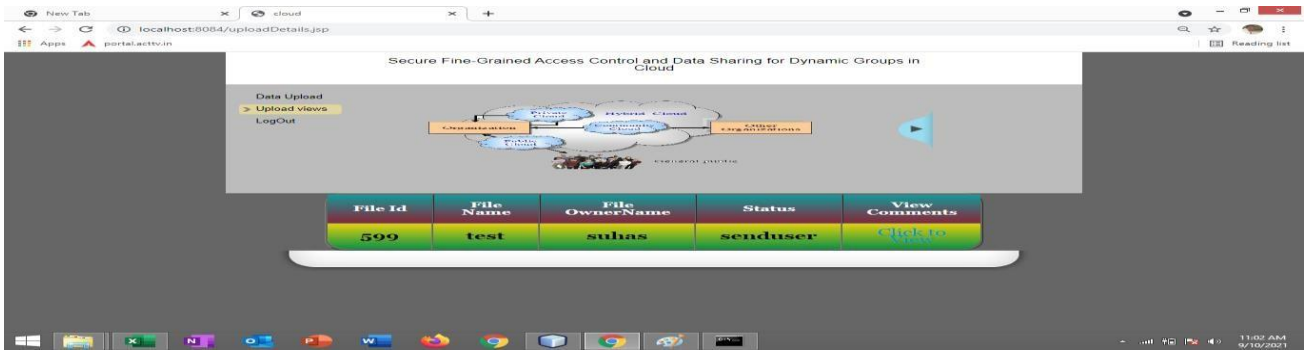
Fig 3.2 Login Page of Data Owner

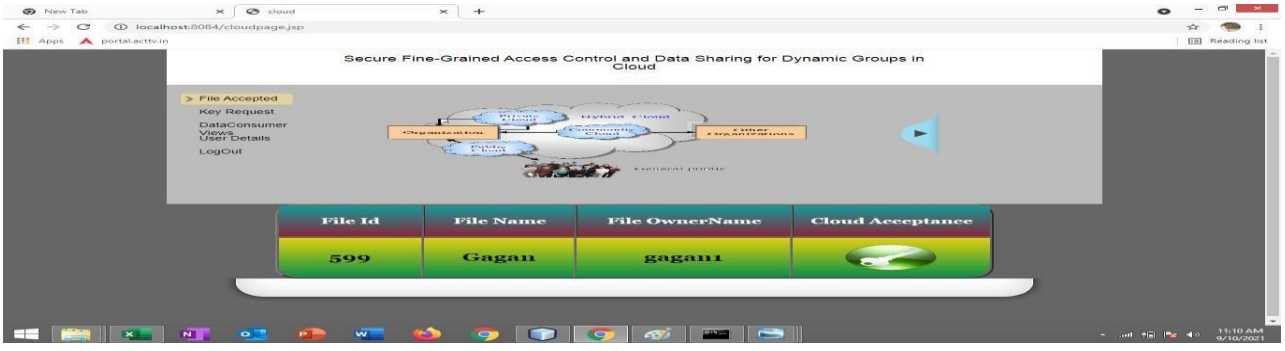
Fig 3.3 Login Page of Data User

Fig 3.4 Login Page of Authority

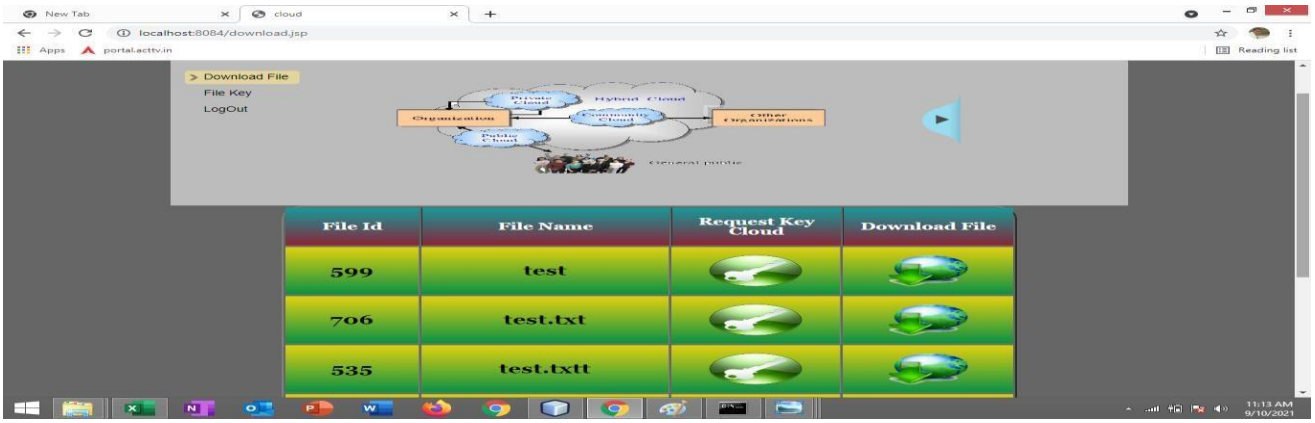

Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud
Cloud Computing
DataOwner
Authority
DataConsumer
Authority
User Name
Password


Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud
File Accepted
Key Request
Consumer Details
User Details
LogOut
File Id
File Name
Send Key
557
Harshey
557
Harshey


Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud
Data Upload
Upload views
LogOut
File Id
File Name
File OwnerName
Status
View Comments
599
test
suhas
senduser


Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud
File Accepted
Key Request
DataConsumer Views
User Details
LogOut
File Id
File Name
File OwnerName
Cloud Acceptance
599
Gagan
gagan1


Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud
Data Upload
Upload views
LogOut
Upload Any Data File/video
File_id
File_Name
Security key
Title
Min Value
Max Value



6. SECURITY ANALYSIS

6.1 SECURITY MODEL

In the context regarding cloud computing, presume information owners may be entirely trusted. These people are ostensibly dishonest, which raises the possibility that they may work together to gain entry to restricted info. The AA might be damaged or The perpetrators made a compromise.Security paradigm permits attacker to request any hidden key, but that key not be utilized to crack the contest the ciphertext's encryption. Since our cryptographic system is founded on the original CP-ABE.

Security Features of AC-CP-ARBE.

6.1.1 Strong Authentication and authorization based on PKI and PMI

Key pairs that the CA has signed are required for all entities in our system. Every type of communication and system access is verified using the public digital signature and key certificate. An attribute certificate demonstrates how the permission ticket and the authentication process are related. The AC verification may be confirmed using the stamp of the issuer.

6.1.2 Secure data access control

The CP-ABE, on which our cryptographic system is based, has been shown in order to prevent cooperation attacks according to the generic security concept, and secure.Update and creation of secure decryption keys

At the data owner or attribute authority, the ACMS service supports user key creation automatically and securely. The request for an updating AC is verified using is PKI authenticity and the authority granting the qualities' signature. The AC signature request, creation of the key, and AC delivery steps are all secured using SSL connection. The RSA key belonging to the relevant user is used to rIn a cryptographic way the produced user decryption key.

7. EVALUATION AND EXPERIMENT

We do the tests in this part to see how well our newly suggested scheme stacks up against the first CP-ABE. In our trials, the ACMS, certification authority (CA), and cryptographic function are all three elements of the access control function. Withthe use of the CP-ABE library and our suggested algorithms, we put our recommended access control methods into practise. The PHP and Java programming languages are used to build the service on top of Apache Server. Using Open SSL, we provide key pairings for system entities and users in the CA service.

Ubuntu Linux is used to run all services on an 2.40 GHz Intel(R) Xeon(R)-CPU E5620. To assess the efficacy of the design we present, we compare the Performance of regenerating keys and key updating of three schemes, including our expanded scheme AC-CP-RBE and the original CP-ABE. One of the five attributes is eliminated in the test scenario. We tested both systems with as many as 800 concurrent non-revoked customers seeking key updates/key regeneration in order to ascertain the worst-case situation.

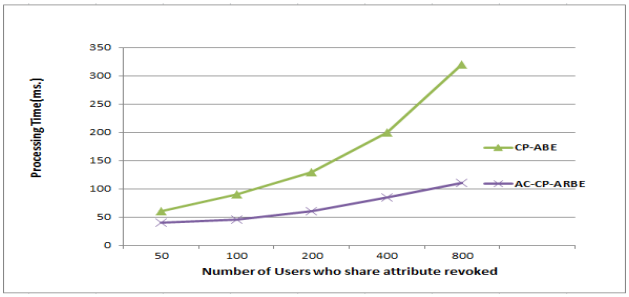


Fig 4. Comparison Of Key Update Cost

The graph in Figure 3 demonstrates that the AC-CP-ARBE proposal we made incurs less expensive key changes than whenever an attribute is revoked, the original CP-ABE. The computation necessary to instantaneously produce fresh CP-ABE keys for all non-revoked users represents the primary cost associated with CP-ABE. Prior to being sent to all impacted individuals, all keys created are also encrypted. Instead of using key regeneration, AC-CP-ARBE uses a key update technique with a single calculation cost. As a consequence, the key is changed to reflect the properties that the AC has selected as active. Additionally, the key distribution process is not necessary. The key update algorithm is executed once the user enters the key update request. Consequently, our recommended plan has a lower computational overhead for this aspect of the attribute revocation effect.

8. CONCLUSION

We have introduced the access restriction architecture based on CP-ABE, RBAC, and PMI combined to facilitate In cloud storage systems, collaborative data sharing is flexible and scalable. In our method,not only AC describes the users' authorization profiles,but also improves the usability and efficacy of updating keys in when an attribute is revoked. Our proposed method customer key changes in light of the AC standard permits the effective handling massive scales of attribute-based revocation systems. Users may updatekeys in a variety of ways, and data owners pay substantially less for transmission and processing.

We will implement our recommended strategy on a genuine cloud environment and assess its effectiveness using bigger data sets in terms of users and characteristics in order to verify scalability and efficacy regarding our model, the AC-CP-ARBE.

REFERENCES:

1. Ciphertext-policy Attribute-based Encryption, Proc. of IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 20–23 2007, pp. 321-334. J. Bethencourt, A. Sahai, and B. Waters.
2. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing by Z. Wan, J. Liu, and R. H. Deng. 2012, Volume 7(2), Pages 743–754 of the IEEE Transactions on Information Forensics and Security.
3. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-based Encryption, IEEE Transactions on Parallel and Distributed Systems, January 2013, Vol. 24, pp. 131-143.
4. Effective Data Access Control for Multiauthority Cloud Storage Systems: DAC-MACS, by K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, IEEE Transactions on Information Forensics and Security, Vol. 8(11), 2013, pp. 1790–1801.
5. O. Pandey, A. Sahai, B. Waters, V. Goyal, and V. Goyal. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data, Proceedings of CCS'06, Alexandria, Virginia, USA, November 2006, pp. 89–98.
6. M. Chase and S. S. M. Chow, Improving privacy and security in multi-authority attribute-based encryption, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'09), ACM, November 2009, pp. 121–13.
7. Decentralizing attribute-based encryption: A. B. Lewko and B. Waters, Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology, EUROCRYPT'11, Springer, May 2011, pp. 568-588.
8. An expanded CP-ABE based Access control model for data outsourced on the cloud, Proceedings of IEEE 39th Annual Computer Software and Applications (COMPSAC 2015), Taichung, Taiwan, July 2015, pp. 73-78.
9. Y. Kawai, Outsourcing the Re-encryption Key Generation: Flexible Ciphertext-Policy Attribute-Based Proxy Re-Encryption, Proc. of International Conference on Information Security Practice and Experience (ISPEC 2015), Beijing, China, May 2015, pp.301-315.
10. Adaptable Ciphertext-Policy Attribute-Based Encryption, In Paring 2013, LNCS, Vol. 8365, 2013, pp. 199–214. J. Lai, R. H. Deng, Y. Yangj, and J. Weng.
11. D. Chadwick, "The X.509 Privilege Management Infrastructure," NATO Advanced Networking Workshop on Advanced Security Technologies in Networking Proceedings, Bled, Slovenia, 2003, pp. 15–25.
12. Cloud Docs: Secure Scalable Document Sharing on Public Clouds, Proc. of IEEE International Conference on Cloud Computing (CLOUD'15), New York, USA, June 2015, pp. 532-539.
13. Acsc.cs.U of Texas, Cpabe
14. http://javadoc.iaik.tugraz.at/iaik_jce/current/iaik/x509/attr/AttributeCertificate.html
15. Open PERMIS source code is available at http://www.openpermis.info