IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

REVOCABLE ATTRIBUTE BASED ENCRYPTION IN CLOUD COMPUTING

Author: Ashwini G

Department of Computer Science and Engineering

University, India

Email: g.ashwini173@gmail.com

***Abstract*-**Cloud computing is one of the emerging technologies. To protect user data and privacy, access control methods ensure that authorized users gain access to data and the system. Cipher Text Policy Attribute-Based Encryption (CP-ABE) is the appropriate method for controlling access to data in cloud storage. However, CP-ABE data access control schemes for cloud storage systems are difficult due to the issue of attribute revocation. Specifically, this article examines a revocable multi-authority CP-ABE system. The attribute revocation method can effectively achieve both front and rear security.

Keywords- Attribute-based encryption (CP-ABE), cloud storage.

I. INTRODUCTION

Cloud systems can be used to enable data sharing capabilities, which can provide several benefits to the user and the organization when data is shared in the cloud. Since many users from various organizations bring their data to the cloud, the time and cost will be less than manual data exchange. Cloud computing is universally accepted as a new IT standard due to its inherent aspects of low resource maintenance. Cloud computing is an emerging technology through which customers can store their document and easily share it with others. Document security is very valuable in maintaining customer trust.

To enhance the security of the cloud, many encryption techniques have been developed to improve the security of the cloud. One of the well-known and popular techniques is the attribute-based encryption technique. Many researchers are researching the ABE technique. In our core article, there are many loop holes in the ABE technique regarding revocation of access permissions. In our core article, the ABE Revocable Technique (RABE) was proposed. According to the author, RABE is effective in managing access permissions. In the RABE technique, the attributes are managed as a master secret key just like the ABE technique and the timestamp (service subscription period) is managed separately.With the help of this secret master key, document is encrypted and stored in the cloud. When decrypting any document, the user must submit their allocated key contains the attribute key. Then the KGC will check the duration of service and update the attribute key to form the master secret key.
Using the master secret key, the document will be decrypted and delivered to the user. The security requirements for data sharing in the cloud computing system are as follows:

Data security: The vendor must be sure that their data outsourced to the cloud is secure and the vendor must take security measures to protect their information in the cloud.

Privacy: The supplier must ensure that all critical data is encrypted and that only authorized users have access to the data in its entirety. User credentials and digital identities should be secure like any data the provider has collected on customer activity from the cloud.

Data confidentiality: In this concept, the user's information must be kept private. It will not be easily disclosed by an illicit or unauthorized person. There shouldn't be easy access to information from the cloud.

Precise access control:unauthorized users to access data redistributed in the cloud. The data owner grants different access rights to a set of users to access the data, while others are not allowed to access it without permissions. Access authorization should be controlled with the help of the owner in an untrusted cloud environment.

User revocation: When a user regains data access rights, they will not allow any other user to access the data at any given time. There is no effect on other authorized users in the group by user revocation.

Scalable and efficient: With the number of cloud users being remarkably high and users joining and leaving the service in unpredictable ways, it is essential that the system maintains its efficiency as well as its scalability. Efficient data sharing in a cloud computing system must meet all security requirements.

Public cloud: Public cloud is called submerged services which are offered by third party vendors who have opted for public internet making them ready for anyone who wants to use or buy them. Technically, there may be similarities in public and private cloud architecture, however, the concepts of the two are different, which are made available by a service provider to a public and when the communication occurs over the non-network. reliable. The management of the public cloud is performed by the cloud provider.

II. EXISTING SYSTEM

The protection and security of clients' information are the essential obstructions that hinder the distributed storage frameworks from wide selection. To keep the unapproved substances from getting to the touchy information,an intuitional solution is to encrypt data and then upload the encrypted data into the cloud. In any case, the customary open key encryption and personality based encryption (IBE) can't be straightforwardly received. The explanation is that they just guarantee the scrambled information can be unscrambled by a solitary known client, with the end goal that it will diminish the adaptability and versatility of information get to control.

III. PROPOSED SYSTEM

In this proposed conspire, any specialist can recoup the redistributed information if and just if this client holds adequate property mystery keys as for the entrance strategy and approval key as to the re-appropriated information. Also, the proposed conspire appreciates the properties of steady size ciphertext and little calculation cost. Other than supporting the quality level repudiation, our proposed conspire permits patients to do the specialist level renouncement.

IV. RELATED WORK

In recent years, to structure the information and get the control plot for multi-authority distributed storage frameworks, the fundamental problem in testing is to create the hidden revocable multi-authority CPABE convention.

S. Yu et al. [5] Attribute-based data sharing offered with attribute revocation. The creators mostly used semi-reliable online intermediary servers. This server allows the position to disavow the characteristics of the client with little effort. This plan coordinated in particular the intermediate re-encryption strategy with CP-ABE, and furthermore gives the power to designate the majority of relentless companies to the intermediate servers. The benefits of this blueprint are more secure against content attacks from selected models. Give meaning to the characteristic repudiation which is difficult for CP-ABE plans. The downside is that the capacity overload could be high if the intermediate servers kept all intermediate keys.

S J. Hur and DK Noh, [6] took a hit with attribute-based access control with efficient revocation in data outsourcing systems. They presented a cipher-dependent entry control instrument based on the figure content approach credit to actualize control arrangements with a productive trait and customer denial strategy. Fine control can be accomplished through a double encryption conspiracy. The double encryption instrument obtains a favorable position of the property-based encryption and a particular collection key dispersion in each characteristic collection. This strategy securely treats reappropriated information and accomplished efficiently and securely within information re-appropriation frameworks.

M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, [7] presented scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. They considered the use of a two-frame encryption procedure. Multi-authority ABE and Key Policy ABE encryption methods are combined in a solitary module. The proposed MA-ABE procedure is useful for key administration and adaptive access supported by KP-ABE. The proposed system has endeavored to ensure information security by MA-ABE and information protection by KP-ABE conspires. The general security of the frame has been improved.

S. Jahid, P. Mittal and N. Borisov, [8] have taken a shot at encryption-based access control in social networks with effective revocation. The proposed engineering underlies two methodologies: a fine-grained approach to control arrangements and dynamic collection registration. The two plans accomplished by using feature-based encryption, in any case, is that it is conceivable to evict a client's access without giving new keys to different clients or re-scrambling figure writes. existing. They have demonstrated this by making an intermediary who is interested in the descrambling procedure and implements waiver limitations. The advantage of this plan is that it gives an evaluation of the execution and a model of

In [9], the attribute-based encryption strategy with verifiable externalized decryption changes the first ABE model with reappropriate descrambling to take into account the undeniable nature of the changes in the existing framework. This new model builds a current ABE conspiracy with unmistakable redistributed descrambling that also doesn't depend on irregular prophets. The multi-authority CP-ABE convention allows the focal position to decipher all figure writing, because it contains the ace key of the frame.

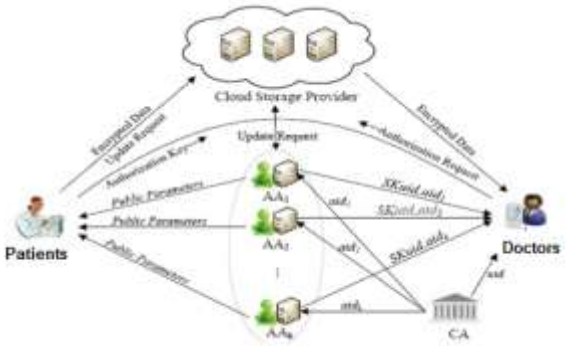
In [10], Chase proposed a multi-authority CP-ABE convention; however, it cannot be applied directly as basic methods for two main reasons: 1) Security issue: Chase's multi-authority CP-ABE convention allows the focal position to decode all ciphertext , because it holds the ace key of the frame; 2) Revocation issue: the Chase convention does not strengthen trait denial.

The procedure used in [11] by S. Ruj, A Nayak and I. Stejmenovic expects the owners to re-scramble the cipertext. K. Yang and X. Jia also recommended that the technique in [2] requires the owner to produce the update data during denial, where the owner should also keep the encryption mystery for
the message in the figure in the frame. This results in substantial storage overhead for the owner, especially when the amount of ciphertext is huge in distributed storage. In the Zhongma Zhu conspiracy (Zhongma Zhu & Rui Jiang, 2013), clients can recruit will specialists from the group leader as well as secure means of correspondence.

In (Nuttapong Attrapadung and Hideki Imai, 2009), Nuttapong Attrapadung allows senders to choose whether or not they want to use either leader in direct repudiation mode while scrambling a message. In direct mode, the sender directly indicates the summary of customers refused in the encryption calculation. With reverse mode, the sender only determines the encoding time. In this context, the content of the figure / the size of the key is not stable.

V. SYSTEM ARCHITECTURE

The System-architecture is shown below.



The CA sets up the framework, and reactions the enrollment demands from all the AAs and clients. In any case, the CA isn't required into any quality related administration.

Every AA regulates an unmistakable property area and produces a couple of open/mystery key for each quality in this characteristic space. Most assuredly, each trait is just overseen by a solitary AA. Once accepting the solicitation of characteristic enrollment from a specialist, the AA creates the relating quality mystery keys for this specialist. Furthermore, every AA is mindful to execute the characteristic disavowal of specialists.

Before transferring a mutual information to the distributed storage workers, the patient characterizes an entrance strategy and scrambles the information under this entrance strategy. From that point onward, the patient sends the Ciphertext and its relating access strategy to the CSP. Then, the patient is liable for giving and repudiating the specialist's approval.

Every client is marked with a lot of properties, other than a worldwide novel identifier. So as to get the common information, each specialist needs to demand the quality mystery keys and approval from AAs and patient, individually. Any specialist can download the ciphertext from the CSP. Just the approved specialist who has the particular properties can effectively recuperate the re-appropriated information. It becomes clear that the CSP gives information stockpiling administration and authorizes the procedure of ciphertext update.

VI. IMPLEMENTATION

Public Key Generation

Step 1: Select p, q p and q are both prime, $p \neq q$

Step 2: Calculate n=p*q

Step 3: $\phi(n) = (p-1)(q-1)$

Step 4: Select an integer e, such that gcd $(\phi(n), e) = 1$; $1 < e < \phi(n)$

Step 5: Calculate d, such that de mod $\phi(n) = 1$

Step 6: Public Key: KU = {e, n}

Step 7: Secret Key: KS = {d, n}

CPABE ALGORITHM

• **Setup.** A randomized algorithm Setup(k) takes in as input a security parameter and provides a set of public parameters (PK) and the master key values (MK).

• **Encryption**. The algorithm Enc(M, T , PK) is a randomized algorithm that takes as input the message to be encrypted (M), the access structure T which needs to be satisfied and the public parameters (PK) to output the ciphertext CT. We can say, that the encryption algorithm embeds the access structure in the ciphertext such that only those users with attributes satisfying T will be able to decrypt and retrieve the message M.

• **Key-Generation.** The KeyGen(MK, PK, A) algorithm takes as input the master key values (MK), the public parameters (PK) and the attribute set of the user (A), and outputs for the user a set of decryption keys SK which confirms the users possession of all the attributes in A and no other external attribute.

• **Decryption.** The decryption algorithm Dec(CT, SK, PK) takes as input the ciphertext CT, the user secret keys SK and the public parameters PK, and it outputs the encrypted message (M) as long as the attributes A embedded in SK satisfy the access structure T which was used while encrypting the ciphertext CT. i.e message M is output if T(A)=1 else, it outputs ⊥.

V1I. RESULTS

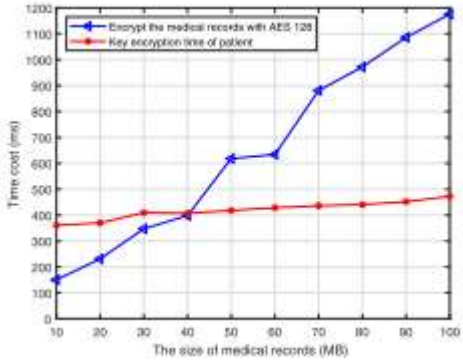


Fig: The computation cost for upload phase

Above Figure depicts the computation cost of the upload phase. In this phase, the patient needs to execute the encryption operation of medical records as well as the key encapsulation operation. The AES 128 encryption algorithm is used to test the encryption time of different medical records ranging from 10 M to 100 M. The computation cost of encryption increases linearly with the medical record size grows. When the file size is 30 M and 60M, the computation cost of encrypting the medical records is 347 ms and 634 ms, respectively. Due to data sharing, the patient needs to generate the key ciphertext. We can see that the computation cost of key encapsulation rows linearly with the file size when fixing the attribute number to 10. When the file size is 30 M and 60 M, generating the key ciphertext consumes 409.311 ms and 428.619 ms, respectively.

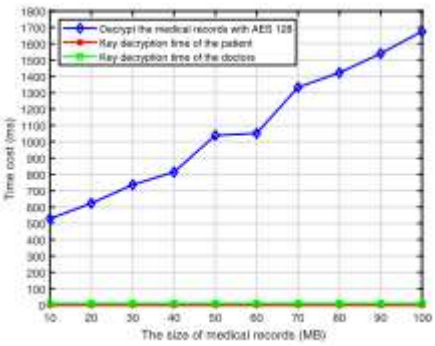


Fig: The computation cost for download phase

Above figure describes the computation cost of the download phase. In this phase, the patient and the doctors need to obtain the key and then execute the decryption operation of medical records. Specifically, the computation cost for a patient to obtain the random key is negligible since the symmetric key is stored in the local. Due to the outsourcing decryption, the doctors obtain the random key only executing one exponential operation. Besides, the AES 128 decryption algorithm is used to test the decryption time of different medical records ranging from 10 M to 100M. Similarly, the computation cost of decryption grows linearly with the medical record's size increases. When the file size is 50 M and 80 M, generating the ciphertext consumes 367 ms and 862 ms, respectively.

VIII. CONCLUSION

In this article, we investigated the effective data access control scheme designed for multi-authority cloud storage systems. Nowadays, there is an emerging trend that more and more customers are starting to use public cloud storage for online data storage and sharing; security in the cloud is a major issue. Multi-Authority CP-ABE reduces decryption overhead for users based on attributes. This cryptographic technique based on secure attributes for robust data security that is shared in the cloud. This multi-authority CP-ABE scheme has proven to be secure and verifiable. The revocable multi-authority CPABE is an effective technique.

IX. FUTURE WORK

In the future, we will try to research other effective and improved techniques to keep the ciphertext constant until the end, even if a new user adds or revokes.

REFERENCES

[1] SJ Hur and DK 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.

[2] Mr. SanthoshkumarB.J, M.Tech, Amrita VishwaVidyapeetham, Mysore Campus, India "Attribute-based encryption with verifiable externalized decryption." In International Journal of Advanced Research in Computer Science and Software Engineering »Volume 4, Number 6, June 2014, ISSN: 2277 128X.

[3] M. Chase, "Multi-Authority Attribute Based Encryption," in Proc. 4th theory of cryptography Conf. Cryptography Theory (TCC'07), 2007.

[4] Aiello, W., Lodha, S., Ostrovsky, R. Rapid digital identity revocation (extended summary). In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 137-152 Spring, Heidelberg (1998).

[5] Amit Sahai and Brent Waters, 2005. "Fuzzy Identity-Based Encryption", R. Cramer (Ed.): EUROCRYPT 2005, LNCS 3494, pp. 457–473, 2005. International Association for Cryptological Research.

[6] Ankita Nandgaonkar, Prof. Pallavi Kulkarni, 2016. "Encryption algorithm for cloud computing", *International Journal of Computing and Information Technology*,Flight. 7 (2), 983-989.

[7] Attrapadung N., B. Libert, E. De Panfieu, 2011. Expressive encryption based on key policy attributes with cipher texts of constant size, in: PKC'11, in: LNCS, vol. 6571, Springer, pp. 90–108.

[8] Attrapadung N., H. Imai, Double-policy attribute basedencryption, in: ACNS'09, in: LNCS, vol. 5536, 2009, pp. 168-185.

[9] Bethencourt, J., Sahai, A., Waters, B. 2007. Encryption based on the attributes of the ciphertext policy. In: IEEE Symposium onSecurity and Privacy 2007, pp. 321–334.

[10] Bindu K. Madhavi, C. Sudarsana Reddy, 2014. Sharing Data for Dynamic Groups in the Cloud ", International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835 Volume-1, Issue-2

[11] Boldyreva A., V. Goyal and V. Kumar, 2008. "Identity-based encryption with effective revocation", in ACM CCS, pp. 417–426

[12] Boneh D. and MK Franklin, 2001. Identity-based encryption from Weil's matching. In CRYPTO, pages 213–229.

[13] Boneh D., X. Boyen, EJ Goh, 2005. Hierarchical identity-based encryption with constant-size ciphertext, in: Eurocrypt'05, in: LNCS, vol. 3494, 440–456.

[14] Canetti R., S. Halevi, J. Katz, 2003. A forward-secure publickey encryption scheme, in: Eurocrypt'03, in: LNCS, vol. 2656, pp. 254-271.

[15] Cheung L., C. Newport, 2007. Provably secure ciphertextpolicy ABE, in: ACM-CCS'07, pp. 456–465.

[16] Craig Gentry, 2003. Certificate-based encryption and the problem of certificate revocation. In EUROCRYPT, pages 272–293.

[17] Emura K., A. Miyaji, A. Nomura, K. Omote, M. Soshi, 2009. An encryption scheme based on ciphertext policy attributes with constant ciphertext length, in: ISPEC ' 09, in: LNCS, vol. 5451, pp. 13–23.

[18] Hanaoka Y., G. Hanaoka, J. Shikata and H. Imai, 2005. Highly isolated hierarchical key encryption and its application. In ASIACRYPT, pages 495–514.

[19] Libert B. and JJ Quisquater, 2003. Cryptosystems based on efficient revocation and threshold matching. In PODC, pages 163–171.

[20] Naor M. and K. Nissim, 1998. Revocation of the certificate and updating of the certificate. In USENIX Security Symposium, Naor, D., Naor, M., Lotspiech, J. 2001. Revocation and tracing schemes for stateless receptors. In: Kilian, J. (ed.), CRYPTO 2001. LNCS, vol. 2139, 41–62. Heidelberg, Springer