International Journal of Researc
Available at
https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

Cloud Data Storage and Sharing in Medical Field using CP-ABE

PRASAD CHALUMUR[1], DR. N. SUPRIYA[2] & M. PURNACHANDRARAO[3]

[1]M-Tech Dept. of CSE Raghu institute of technology Visakhapatnam AP
Mail Id: - prasadch283@gmail.com
[2]HOD & Associate professor Dept. of CSE Raghu institute of technology Visakhapatnam AP
Mail Id: - Ritv.cse5@gmai.com
[2]Assistant professor Dept. of CSE Raghu institute of technology Visakhapatnam AP
Mail Id: - purnachandrarao.m@gmail.com

Abstract:

With the appearance of business applications which endorse clients to create dynamic gatherings with the goal that they can store information on cloud servers also, distribute the information inside their utilizer bunches through their portable contraptions. A noteworthy concern peregrinates here that portable clients require the security of their gathering information which ought not be open to other gathering clients. To settle the issue, ABE or Characteristic Predicated Encryption systems are utilized as they are immensely apperceived as a substantial and vigorous instrument to give fine get to control over the information to honest to goodness clients. Simultaneously, as there are involute calculations included in key issuing and information encryption by AAs' (Attribute Ascendant substances) and unscrambling by genuine clients, there subsist some productivity issues. Rekeying assumes a noteworthy part in dynamic frameworks where hubs come-in and move-out. As renouncement of utilizer rights requires the framework to secure information from moved out clients, rekeying must be done on whole information set having a place with that quality clients in the gathering. Be that as it may, the cost of re-keying is another worry for framework proficiency which ought not be repaid with a trade off on information security. There are many research works completed before on information security for web applications using ABE, yet there are compelled ponders on CP-ABE in portable processing with multi authority information stockpiling framework. A framework is actualized which sanctions utilizer gatherings to enlist, CAs'(Certificate Ascendant elements) to endorse enlistments of Users and AAs and relegate open Keys, AAs to oversee properties and disavow utilizer access with rekeying what's more, a unified server for information steadiness. Trial comes about demonstrate the adequacy of proposed arrangement and effectiveness of re-keying

system while inspiring utilizer get to rights on framework engineering. Catchphrases Characteristic Predicated Encryption, CP-ABE, Mobile Data Security, Re-Keying, Utilizer Access Control

Key Words—Access control, Certificate Authority ,Attribute Authorities, Information Owners, Cloud Server, Information Consumers.

1. INTRODUCTION

Unified information stockpiling systems are the indispensable component for ecumenical openness of utilizer information at any snapshot of time. Cloud convenience suppliers offer such housing to have the outsourced information of any utilizer through the web or versatile invention [1]. As versatile contraptions have certain limitation because of outlined equipment capacities, a large portion of the calculations are conveyed at facilitating server end. These facilitating housing bring out nascent challenges for information get to control because of the plenty of information stockpiling by various clients. The cloud servers can't be aimlessly trusted by information proprietors for security for their information, there must be sure strategies to find out the information is bulwarked from abuse. CP-ABE or Ciphertext-Policy Attribute-Predicated Encryption [2], [3] is considered as one among the most fitting techniques for get to control of clients' information in brought together capacity servers, as it gives the information proprietor unlimited yet controlled access on information. In CP-ABE instrument, there subsist a substance which is responsible for trait organization and key designations i.e. Trait Domination (AA). The AA can be any element who goes about as an administrator of the framework, for example, HR chief or gathering executive of the system predicated diversion, and so forth. The guests of the frameworks need to enlist with a specific end goal to be an information proprietor; CA designates people in general key and favors the enrollment and AA doles out credit to the utilizer according to the gathering assignment. Information gets encoded through the characteristic relegated by the AA. A utilizer can decode the information just when they have a place with the same characteristic gathering else information will remain encoded and secured on the server. Till late research works, there is confirmation of just two sorts of ABE which are being proposed: CP-ABE (Ciphertext Approach Attribute Predicated Encryption)

and KP-ABE (Key-Policy Trait Predicated Encryption). In KP-ABE, private keys are used for the get to strategies, while, in CP-ABE, it is given in ciphertext [6]. Ecumenically, there subsist two sorts of CP-ABE systems: single-power CP-ABE [2], [3], [4], [5] in which properties are controlled by a solitary AA and the second one is multi authority CP-ABE [7], [8], [9] in which different properties are managed by different ascendant substances. Multi-authority CP-ABE is more well suited if there should arise an occurrence of distributed storage frameworks as information get to must be given to cosmically huge no. of various clients. If there should be an occurrence of multi-authority predicated information stockpiling, Data Owners (DO) properties can be changed powerfully. A nascent utilizer can be assigned a beginning characteristic by AA or any subsisting bunch utilizer may lose the credit to repudiate their get to rights. However, subsisting trait renouncement plans [10] depends too on a reliable server or are shy of productivity, those were most certainly not fortunate to handle with the property renouncement issues in information get to administration in multi-power predicated information stockpiling frameworks.

2. RELATED WORK:

Existing system:

This incipient paradigm of information hosting and information access accommodations introduces a great challenge to information access control. Because the cloud server cannot be plenarily trusted by information owners, they can no longer rely on servers to do approach control. Cipher text-Policy Attribute-predicated Encryption (CP-ABE) is regarded as one of the most congruous technologies for information access control in cloud storage systems, because it gives the information owner more direct control on access policies. In CP-ABE scheme, there is an ascendancy that is responsible for assign direction plus key distribution.

Disadvantages of existing system:

Chase's multi-ascendancy CP-ABE protocol sanctions the central ascendancy to decrypt all the cipher texts, later it agrees ye master key of ye system. Chase's protocol does not fortify sat encomium revocation.

Proposed system:

Then, we apply our proposed revocable multi-ascendancy CP-ABE system as ye fundamental techniques to construct the

expressive and secure information access control scheme for multi-ascendancy cloud storage systems. In this paper, we first aim a revocable multi authority CP-ABE system, where an efficient and secure revocation method is proposed to solve the attribute revocation quandary in the system. Our assign annulment method is efficient in the sense that it receives less communicating cost and computation cost, plus is assure in ye feel that it can accomplish both rearward security (The revoked utilize cannot decrypt any incipient cipher text that requires the revoked attribute to decrypt) and forward security (The incipiently joined utilize can withal decrypt the aforetime published ciphertexts1, if it has adequate. attributes). Our scheme does not require the server to be planarity trusted, because the key update is enforced by each attribute ascendancy not the server. Even if the server is not semi confided in some scenarios, our scheme can still guarantee the rearward security.

Advantages of proposed system:

We modify the framework of the scheme and cause it more virtual to cloud storage organizations, in which information owners are not involved in the key generation. We greatly amend the efficiency of the attribute revocation method. We withal highly ameliorate the expressiveness of our access control scheme, where we abstract the inhibition that each attribute can exclusively come out at almost once in a cipher text.

3. IMPLEMENTATION

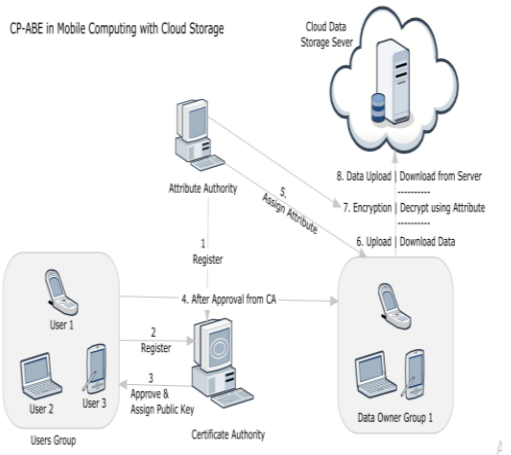

Fig:-1 System architecture

Certificate Ascendancy:

However, the CA is not involved in any attribute management and the engenderment of secret keys that are associated with attributes. For example, the CA can be the Convivial Security Administration, an independent agency of the Amalgamated States regime. For each licit utilized in the system, the CA assigns an ecumenical unique utilized identity to it and withal engenders an ecumenical public key for this utilized. Each utilizer will be issued a Gregarious Security Number (SSN) as its ecumenical identity. The CA is ecumenical trusted certificate ascendancy in the system.

It establishes the system and accepts the registration of all the users and AAs in the system.

Attribute Ascendant entities:

Every AA is an independent attribute ascendancy that is responsible for ennobling plus annulling user's attributes according to their role or identity in its domain. In our scheme, every attribute is linked with one AA, but each AA can manage an arbitrary number of attributes.. Each AA is responsible for engendering a public assign key for to each one assign it deals and a secret key for each utilized reflecting his/her attributes.

Information Consumers:

Each utilizer has an ecumenical identity in the system. A utilizer may be entitled a set of attributes which may emanate from multiple attribute ascendant entities. The utilizer will receive a secret key linked with its attributes ennobled by the representing attribute ascendant entities.

Information Owners:

The owner defines the access policies over attributes from multiple attribute as cendant entities and encrypts the content keys under the policies. Each owner first divides the information into several components according to the logic granularities and encrypts each information component with different content keys by utilising symmetric encryption techniques.

Cloud Server:

Then, the owner sends the encrypted information to the cloud server together with the cipher texts. They do not rely on the server to do information approach assure. But, the access control transpires inside the cryptography. That is only when the user's attributes gratify the access policy defined in the cipher text; the utilizer is able to decrypt the cipher text

4. EXPERIMENTAL RESULT

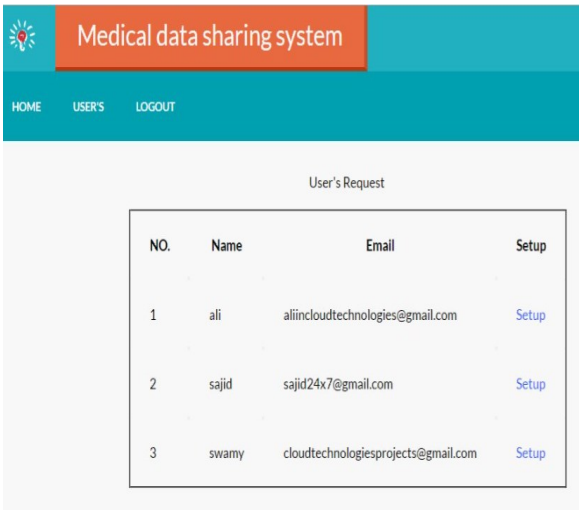

Fig:-2 Setup users

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

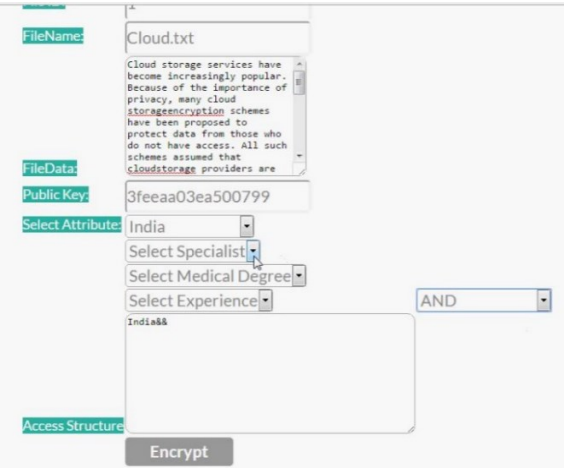

Fig:-3 Encrypt and Upload File

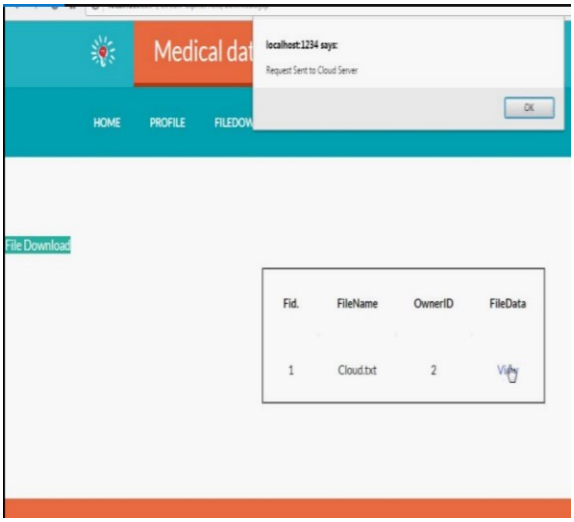

Fig:-4 User sent request to cloud

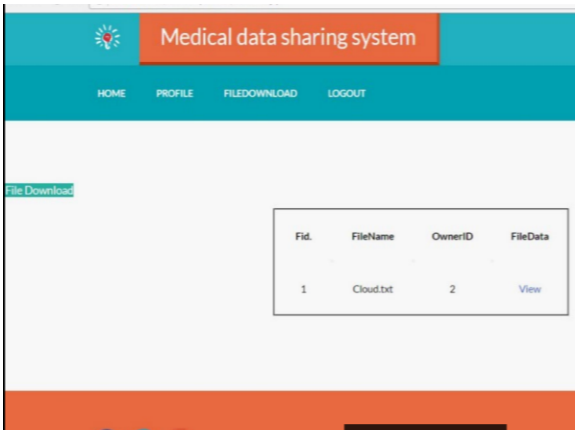

Fig:-5 View and Download file

5. CONCLUSION

This examination basically focuses on giving adaptable and efficient application arrangement which takes after CP-ABE conspire on portable distributed computing. The proposed instrument Gives a safe and productive answer for trait renouncement predicament and offers fine-grained access to true blue clients. Our framework sustains multi-domination CPABE plot where various trait ascendant substances may subsist to give clients greater openness and adaptability to use the framework. The preferred standpoint here is, the calculation cost is hardly decremented because of the conveyance of workload among various elements. It is sheltered to outsource information on doubtful servers also because of better get to control and security. This proposed instrument can be connected on sundry online jovial gatherings or business applications which authorize clients to frame gatherings and allocate the transferred information inside the gathering.

6. REFERENCES

[1] M. Chase and S.S.M. Chow, ‘‘Improving Privacy and Securityin Multi-Authority Attribute-Based Encryption,’’ in Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09), 2009,

pp. 121-130.

[2] A.B. Lewko and B. Waters, ‘‘Decentralizing Attribute-BasedEncryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’11,2011, pp. 568-588.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Attribute Based InformationSharing with Attribute Revocation,’’ in Proc. 5th ACM Symp.Information, Computer and Comm. Security (ASIACCS’10), 2010,pp. 261-270.

[4] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ‘‘Scalable and SecureSharing of Personal Health Records in Cloud Computing UsingAttribute-Based Encryption,’’ IEEE Trans. Parallel DistributedSystems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[5] J. Hur and D.K. Noh, ‘‘Attribute-Based Access Control withEfficient Revocation in Information Outsourcing Systems,’’ IEEETrans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221,
July 2011.

[6] S. Jahid, P. Mittal, and N. Borisov, ‘‘Easier: Encryption-BasedAccess Control in Social Networks with Efficient Revocation,’’ inProc. 6th ACM Symp. Information, Computer and Comm. Security(ASIACCS’11), 2011, pp. 411-415.

[7] S. Ruj, A. Nayak, and I. Stojmenovic, ‘‘DACC: Distributed AccessControl in Clouds,’’ in Proc. 10th IEEE Int’l Conf. TrustCom, 2011,pp. 91-98.

[8] K. Yang and X. Jia, ‘‘Attribute-Based Access Control forMulti-Authority Systems in Cloud Storage,’’ in Proc. 32th IEEEInt’l Conf. Distributed Computing Systems (ICDCS’12), 2012,pp. 1-10.

[9] D. Boneh and M.K. Franklin, ‘‘Identity-Based Encryption fromthe Weil Pairing,’’ in Proc. 21st Ann. Int’l Cryptology Conf.:Advances in Cryptology - CRYPTO’01, 2001, pp. 213-229.

[10] A.B. Lewko and B. Waters, ‘‘New Proof Methods for Attribute-Based Encryption: Achieving Full Security through SelectiveTechniques,’’ in Proc. 32st Ann. Int’l Cryptology Conf.: Advances inCryptology - CRYPTO’12, 2012, pp. 180-198