Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

# SecureData Storage and Control Access Allowance in Cloud with Authority

Shalini P M ,
M. Tech Scholar,
Deptartment of Computer Science & Engineering,SSIT,
Tumakuru,Karnataka

Rekha H
Assistant Professor,
Deptartment of Computer Science & Engineering,SSIT,
Tumakuru,Karnataka

***Abstract* - Cloud computing is a progressive figuring worldview, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Different plans taking into account the Ciphertext Policy attribute based encryption have been proposed to secure the storage in cloud. Nonetheless, most work spotlights on the information substance security and the access control, while less consideration is paid to the benefit control and the identity security. In this paper focused on better access control permissions for each file based on the attribute of user. Attributes are efficiently utilized for encrypting the valuable data.**

***Keywords* - *Cloud Computing, Encryption Policy, CP-ABE***

## I. INTRODUCTION

It enormously draws in consideration and enthusiasm from both the scholarly world what's more, industry because of the productivity, yet it additionally has in any event three difficulties that should be taken care of before going to our genuine to the best of our insight. As a matter of first importance, data confidentiality ought to be ensured. The data security is most certainly not just about the information substance. Subsequent to the most alluring part of the cloud computing is the calculation outsourcing, it is far sufficiently past to simply direct an entrance control [8]. More probable, clients need to control the benefits of data manipulation control over different clients or cloud servers. This is on the grounds that when sensitive data or calculation is outsourced to the cloud servers or another client, which is out of clients' control in most cases, protection dangers would rise significantly in light of the fact that the servers may unlawfully examine clients' information and access sensitive data, or different clients may have the capacity to gather delicate data from the outsourced calculation.

Consequently, not just the access additionally the operation ought to be controlled. Furthermore, individual information (characterized by every client's properties set) is at danger since one's personality is validated taking into account his data with the end goal of access control (or benefit control in this paper). As individuals are turning out to be more worried about their privacy protection nowadays, the personality security additionally should be ensured before the cloud enters our life. Ideally, any power or server alone ought not to know any customer's close to home data. To wrap things up, the cloud processing framework ought to be versatile on account of security rupture in which some part of the framework is traded off by assailants. Different procedures have been proposed to secure the information substance security by means of access control. Personality based encryption (IBE) was initially presented by Shamir [1], in which the sender of a message can indicate a personality such that just a beneficiary with coordinating personality can unscramble it. Couple of years after the fact, Fuzzy Identity-Based Encryption [2] is proposed, which is otherwise called Attribute-Based Encryption (ABE).

In such encryption conspire, a personality is seen as an arrangement of distinct traits, and unscrambling is conceivable if a decrypter's character has a few covers with the one determined in the ciphertext. Before long, more broad tree-based ABE plans, Key-Policy Attribute-Based Encryption (KP-ABE) [3] and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [4], are introduced to express more broad condition than straightforward 'cover'. They are partners to one another in the sense that the choice of encryption approach (who can or can't unscramble the message) is made by various parties. In the KP-ABE [3], a ciphertext is connected with a set of characteristics, and a private key is connected with a monotonic access structure like a tree, which portrays this client's personality. A client can unscramble the ciphertext if and just if the entrance tree in his private key is fulfilled by the traits in the ciphertext. Be that as it may, the encryption strategy is portrayed in the keys, so the encrypter does not have whole control over the encryption arrangement. He needs to trust that [9] the key generators issue keys with right structures to right clients.

Moreover, when a re-encryption happens, the greater part of the clients in the same framework must have their private keys re-issued in order to access the re-scrambled documents, and this procedure causes impressive issues in execution. Then again, those issues and overhead are all explained in the CP-ABE [4]. In the CP-ABE, ciphertexts are made with an entrance structure, which determines the encryption arrangement, and private keys are created by properties. A client can decode the ciphertext if and just if his characteristics in the private key fulfill the entrance tree indicated in the ciphertext. Thusly, the encrypter holds a definitive power about the encryption arrangement. Additionally, the as of now issued private keys will never be changed unless the entire framework reboots.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

## II. RELATED WORK

Allison Lewko and Brent waters propose [2] a Multi-Authority Attribute-Based Encryption (ABE) framework. In our framework, any party can turn into a power and there is no prerequisite for any worldwide coordination other than the production of an introductory arrangement of common reference parameters. A party can just go about as an ABE power by making an open key and issuing private keys to various clients that mirror their properties. A client can encode information regarding any Boolean recipe over properties issued from any picked set of powers. At long last, our framework does not require any focal power.

In building our framework, our biggest specialized collision is to make it arrangement safe. Earlier Attribute-Based Encryption frameworks accomplished plot resistance when the ABE framework power "tied" together diverse segments (speaking to various characteristics) of a client's private key by randomizing the key. Be that as it may, in our framework every segment will originate from a conceivably diverse power, where we expect no coordination between such powers. We make new strategies to tie key segments together and avert arrangement assaults between clients with various worldwide identifiers.

Decentralized property based encryption (ABE) [3] is a variation of a multi-authority ABE plan where every power can issue secret keys to the client autonomously with no participation and a focal power. This is rather than the past developments, where numerous powers must be online and setup the framework intelligently, which is unrealistic. Subsequently, it is clear that a decentralized ABE plan disposes of the overwhelming correspondence cost and the requirement for community oriented calculation in the setup stage. Besides, every power can join or leave the framework openly without the need of reinitializing the framework. In contemporary multi-authority ABE plans, a client's mystery keys from various powers must be attached to his worldwide identifier (GID) to oppose the arrangement assault. Nonetheless, this will trade off the client's protection. Different powers can work together to follow the client by his GID, gather his properties, then imitate him. In this way, building a decentralized ABE plan with security safeguarding remains a testing research issue. In this paper, we propose a protection saving decentralized key-arrangement ABE plan where every power can issue mystery keys to a client freely without knowing anything about his GID. In this way, regardless of the possibility that numerous powers are defiled, they can't gather the client's characteristics by following his GID. Outstandingly, our plan just requires standard many-sided quality suppositions (e.g., decisional bilinear Diffie-Hellman) and does not require any collaboration between the numerous powers, rather [10] than the past equivalent plan that requires nonstandard unpredictability presumptions (e.g., q-decisional Diffie-Hellman reversal) and associations among different powers. To the best of our insight, it is the initially decentralized ABE plan with protection saving in light of standard unpredictability presumptions.

In this paper we characterize and illuminate the compelling yet secure ranked keyword search over scrambled cloud information. We utilized request safeguarding symmetric encryption to ensure the cloud information. Despite the fact that there are bunches of seeking strategies accessible, they are not giving productive list items. For instance the indexed lists returned 40 records and in those 30 records are applicable and the remaining 10 records result contains unessential information. This paper for the most part spotlights on looking systems which will enhance the productivity of seeking. We utilized both key word search [3] and concept based pursuit routines keeping in mind the end goal to recover the significance seeks criteria. This system will recover the archives taking into account broader conceptual, which will enhance the productivity of ranked keyword search. Customary searchable encryption plans permit a client to safely seek over scrambled information through ranked keyword without first decoding it, these systems bolster just traditional Boolean keyword look, without catching any pertinence of the documents in the query item. At the point when specifically connected in huge shared information outsourcing cloud environment, they might experience the ill effects of the accompanying two primary disadvantages. From one viewpoint, for every hunt demand, clients without pre-information of the encoded cloud information need to experience each recovered record keeping in mind the end goal to discover ones most coordinating their advantage, which requests potentially vast measure of post preparing overhead On the other hand, perpetually sending back all documents exclusively taking into account vicinity/absence of the keyword further acquires expansive pointless system activity, which is totally undesirable in today's pay-as-you-utilize cloud worldview.

Individual health record is a rising patient-driven model of wellbeing data trade, which is regularly outsourced to be put away at an outsider [4], for example, cloud suppliers. In any case, there have been wide security worries as individual wellbeing data could be presented to those outsider servers and to unapproved parties.

Zheng and Lou propose a novel patient-driven system and a suite of components for information access control to PHRs put away in semi trusted servers. To accomplish fine-grained and adaptable information access control for PHRs (personal health record), we influence property based encryption (ABE) strategies to encode every patient's PHR document. Not the same as past works [4] in secure information outsourcing, we concentrate on the different information proprietor situation and separation the clients in the PHR framework into various security areas that extraordinarily lessens the key.

Taeho jung and xiang –yang Li think about how as an outside aggregator [5] or multiple parties can realize some arithmetical measurements (e.g., sum, product) over members' exclusive information while saving the information security. We accept all channels are liable to listening in assaults, and every one of the correspondences all through the collection are interested in others. We first propose a few conventions that effectively ensure data security under semi-honest model and after that present propelled convention which endure up to k passive adversaries who don't attempt to alter the calculation. Under this frail supposition, we confine both the correspondence and calculation unpredictability of every member to a little consistent.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

Toward the end, we display applications which take care of a few fascinating issues through our conventions.

*Proposed System:*

Below figure 1 shows the proposed system, various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. Various techniques have been proposed to protect the data contents privacy via access control. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information.

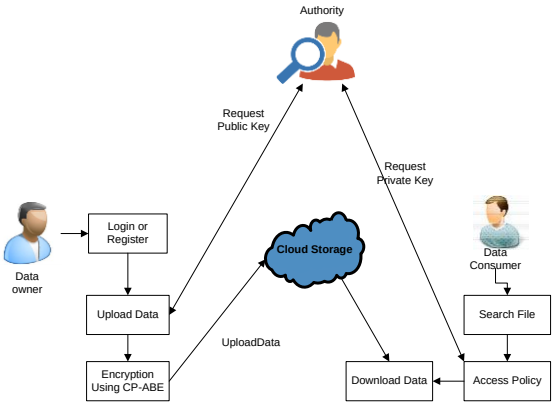


Figure 1: Architecture of Proposed System

When data owner (user) wants to upload the data to cloud he needs to request cloud authority (CA). CA provides the public key to the user and then user will encrypt the data and upload to the cloud. Public key will be generated using attributes of data owner which are given in registration time. if data consumer wants to download the data from the cloud the request will passed to CA. CA will authenticate the data consumer whether the user is valid or not if the user is valid MA provides the private key to the data consumer and key has to match with attributes of user. If attributes are matched then data consumer can able to download. Otherwise he cannot download the data.

### *A. User Regestration and User Login Module*

In this module, the fields are username, password, email id and mobile number. User must register with the cloud then perform the remaining operation without registration can't perform the other operations so initially user register then go for the login. After entering all fields, user details will be stored in the Cloud.

In user module, the fields are username and password. And before login he should be registered as a user then only he can login and use the secured system in cloud computing.

### *B. File Upload and Security*

In this module is used to upload the files present in user system and CP-ABE algorithm is used for file encryption. In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the one specified in the ciphertext.

The file is present in the cloud is downloaded and use the CP-ABE algorithm for file decryption. In the CP-ABE, ciphertexts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users attributes. A user [7] can decrypt the ciphertext if and only if his attributes in the private key satisfy the access tree specified in the ciphertext. By doing so, the encrypter holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots.

We let each authority be in charge of all attributes belonging to the same category. . For each attribute category, suppose there are k possible attribute values then one requester has at most one attribute value in one category. Upon the key request, the attribute authority can pick a random number ru for the requester and generates H(att (i ))ru for all i $\in \{1, \ldots, k\}$.

After the attribute keys are prepared, the trait power and the key requester are occupied with a 1-out-of-k OT where the key requester needs to get one attribute key among k. By presenting the 1-out-of-k OT in our Key Generate calculation, the key requester accomplishes the right attribute key that he needs, however the attribute authority does not have any valuable data about authority is accomplished by the requester.

### *C. Cloud Storage*

- Cloud storage stores the encrypted data of data owner. We can categorize [6] the storage parts into several groups.
- Owner module is to upload their files using some access policy. First they get the public key for particular upload file after getting this public key owner request the secret key for particular upload file. Using that secret key owner upload their file.
- User module is used to help the client to search the file using the file id and file name .If the file id and name is incorrect means we do not get the file, otherwise server ask the public key and get the encrypted file. If user wants the decrypted file means user must have the secret key.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

## RESULTS AND DISCUSSIONS:

The algorithm is implemented in java. When user uploading data, access allowance setting is done for each file. User details are made anonymous using k-anonymity as shown in Figure 6. The uploaded file will be encrypted using CP-ABE.

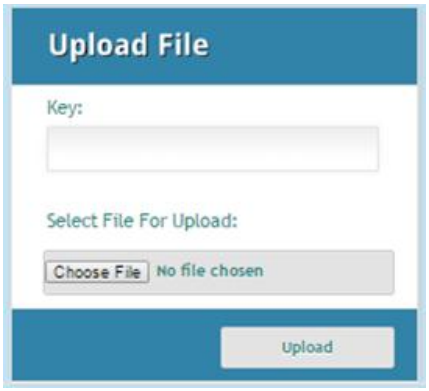


Figure 3: Data Uploading

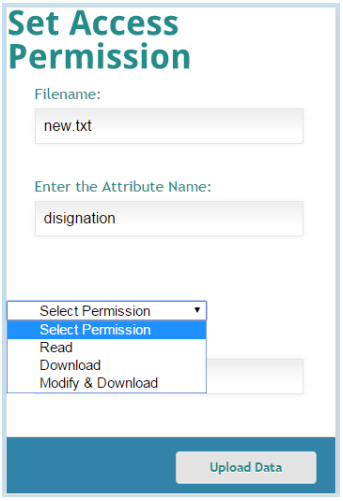


Figure 5: Setting Access Permission before uploading to cloud by data owner based on the attribute of the user for each file

## CONCLUSION

One of the promising future works is to present the productive user revocation component on top of our anonymous CP-ABE. Supporting user revocation is an essential issue in the genuine application, and this is an awesome test in the utilization of ABE plans. Making our plans perfect with existing CP-ABE plans that support effective client revocation is one of our future works.

Future work focuses on introducing multiple authorities system (MA) to track cloud users and protecting private information of users by using anonymity algorithm.

## REFERENCES

[1] Taeho Jung, Xiang-Yang Li.” Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption” IEEE Transactions on Dependable and secure computing, Volume 12 , Issue: 1,February 2015.

[2] Lewko and B. Waters, “Decentralizing attribute-based encryption,”in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[3] S. Müller, S. Katzenbeisser, and C. Eckert, “On multi-authority ciphertext-policy attribute-based encryption,” *Bull. Korean Math. Soc.*, vol. 46, no. 4, pp. 803–819, 2009

[4] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,” *IEEE Trans. Parallel Distrib. Syst.*, Volume 24, Issue 1, pp. 131–143, 2013.

[5] Taeho Jung and Xiang-Yang Li,“Collusion-Tolerable Privacy-Preserving Sum and Product Calculation without Secure Channel”. IEEE Transactions on Dependable and secure computing, Volume12, Issue: 1, 2015.

[6] Wang, K. Ren, and J. Wang, “Secure and practical outsourcing of linear programming in cloud computing,” in *Proc. IEEE INFOCOM*, pp. 820–828, 2011

[7] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in *Proc. IEEE 30th ICDCS*, Jun. 2010, pp. 253–262.

[8] Y. Liu, J. Han, and J. Wang, “Rumor riding: Anonymizing unstructured peer-to-peer systems,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 3, pp. 464–475, Mar. 2011.

[9] *Tor: Anonymized Network*. [Online]. Available: https://www.torproject.org/, accessed 2014.

[10] Shamir, “How to share a secret,” *Commun. ACM*, volume 22, Issue 11,pp. 612–613, 1979.

[11] Raymond Chi-Wing Wong, Jiuyong Li, Ada Wai-Chee Fu and Ke Wang, “(α, k)-Anonymity: An Enhanced k-Anonymity Model for Privacy-Preserving Data Publishing”, ACM, 2006.