Provide Privacy and Efficiency of Multi Authority Data Access Control Over Cloud Computing

Bheri Thrinadha[1], Ramesh kumarBehara[2]
Final M.Tech Student[1], Asst.professo[2]
[1,2]*Dept of CSE, Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh, India*

Abstract:

Cloud storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to data access control. So that we can access data before each user will perform the authentication process and also provide data access control policy. In this paper we are proposed mainly on authentication of users, group key generation, data access control policy, data encryption and decryption process. By implementing those concepts we can improve the efficiency of data access and also provide more security of hosting data in cloud.

I. Introduction:

Cloud is a resource area where we can store and retrieve whenever access the data,various roles involved while cloud computing. Data owner is the person who stores and retrieves the data from server, Cloud service provider allows data owner to buy storage space and can manipulate the space whenever required. End users can consume the services provided by data owner. One more specific role involved in cloud computing i.e Auditor, he audits or monitors the data uploaded into the server and gives updates to the respective data owner.

Data authentication and confidentiality are the important factors while transmission of data components over network, because data owner does not know the physical location of the data component which is stored, so data owners needs to handle the authentication and data privacy or confidentiality. Authentication explains about the authorization of the user, only valid or authenticated person can access the data resources which are uploaded. Cryptographic approaches maintain data confidentiality and privacy while transmission of data components. Data component can be encoded with key which is generated from group key protocol securely along with authentication.

Cloud storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to data access control. So that we can access data before each user will perform the authentication process and also provide data access control policy

II. Related work:

Group key protocols can be implemented with two approaches, one in centralized and other is decentralized. In centralized model, key can be generated with group key center or third party center and it can be forwarded to all authenticated users. In decentralized model users or data owners need not depends on third party server.

Cloud computing has been visualize the next generation architecture of IT endeavour due to its large list of advantages in the IT history: on demand service, location independent, resource pooling and rapid resource elasticity. From users side in clouding both individuals storing data distant into the cloud in easier on demand manner brings requesting benefits: relief of the burden of storage management global data access with dependent geo-graphical locations and reducing of large disbursement on hardware / software and personnel maintenances etc.

In multi-authority cloud storage systems, user's attributes can be changed dynamically. A user may be entitled with some new attributes or revoked some current attributes and his permission of data access should be changed accordingly. However, existing attribute revocation methods either rely on a trusted server or lack of efficiency, they are not suitable for

dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems.

In centralized models users registers at centralized server or authentication server and forward the security parameters and generates random key and forwards to respective user in terms of divisor and reminder coefficients and reverse process can be implemented at the receiver end after authentication of hash.

In this paper we proposed multi authority schema for that can support authentication of data consumers and generation of secret key. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. We also proved that our scheme was provable secure for cloud data. In this paper we can also provide data access policy for storing and retrieving data from the cloud. So that by implementing those concepts we provide efficient data access and also provide more security in cloud data.

III. Proposed Work:

We consider a data access control system in multi authority cloud storage contains four types of entities. They are the certification authority, data owner, data consumer and cloud service. in this paper the certification authority will perform the functionalities of acceptance of user registration and generation of group key. The data owner will encrypt the data and stored into by accessing policy of data. The cloud service will provide storing and sending data through data consumers. The final one is data consumer or user is retrieve data from the cloud and decrypts it. The implementation procedure of each and every process is given bellow.

Users Registration:

In this module each user will send request to certification authority. The CA authority will accept request and sent unique id to each user. By using this id we can remain operation performed by users.

Generation of signature and secret key:

The CA set up system by implementing of generation of signature and secret key. Before generating signature the certification authority will choose multiplicative group g with prime order. The CA also chooses one hash function that matches parameter of string as element.
For each user U_{id} ,the CA will choose two random numbers a,b as the global master key of the system and compute public parameter by using following formula.
$Public_{param} = g^{a} * g^{b}$
After generating public parameters the CA will send that parameter to individual users. The users will retrieve parameter and choose two random number p, q. each user will user those random value and calculate shared key by using following formula.

$$Shared\ key_i = public_{param(i)}^{p} * public_{param(i)}^{q}$$

After generating shared keys each user will send keys to certification authority. The CA will retrieve those keys and randomly choose one secret key. After generating secret key the CA
will generate signature for individual user by using following formula.

$sig_i = hash(sharedkey_i \circledR public_{parami})$

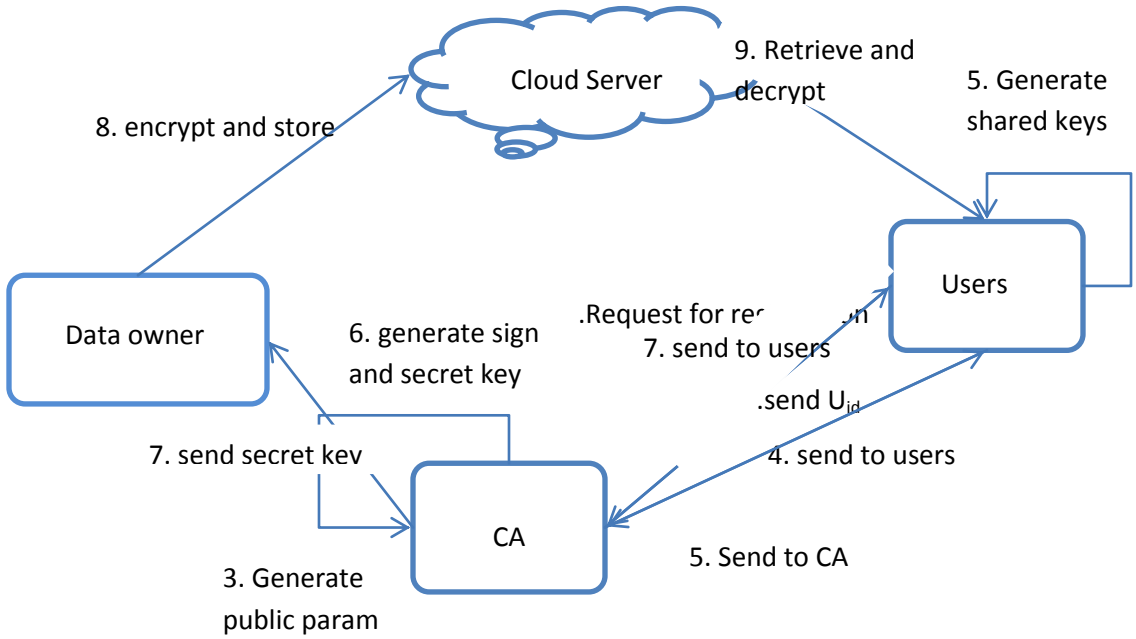
After generating signature the CA will shared points to individual users. The generation of point will be calculate by using following equation.

x_i= secret key/ $sharedkey_i$
y_i = secret key% $sharedkey_i$

So that the CA will calculating share points (x_i,y_i) of individual users and send sig , points to individual users. The CA also Send Secret key to Data owner also.

Signature Verification and get Secret key:

Each user will retrieve the signature and share points (x_i,y_i), perform the verification process and get secret key. The generation of signature will do by using of shared key and public parameter of each user. After generating signature each user will verify that both signatures are equal or not. If both signatures are equal that user is authenticated user or not equal not authenticated user. If the user if authenticated user it will get secret key by using following equation.
$Secret\ key_i = x_i * sharedkey_i + y_i$



Data Encryption and Decryption process:

In this module data encryption process can be done by data owner. Before storing data into cloud the data owner will encrypt data by using IDEA. Before encrypt the data the cloud also provide data storing policy to the data owner. The data owner store data into cloud, the cloud will send verification code to mail of the data owner. The data owner will get verification and perform the verification status. After performing the verification status the data owner will encrypt data and stored into cloud. Before encrypt the data the data owner will get secret key and encrypt the data.

This module contain another process of decryption can be done by data consumers. Before download the content of file the user also perform the verification process. Before performing decryption process the cloud will send the verification code to users mail. The user will get verification code and perform the verification process if both are equal it will decrypt the file and download it. So that if you access data we also perform the verification of each data can be getting and also perform the decryption process. The encryption and decryption process can be done by using IDEA algorithm.

IV. Conclusion

In this paper we proposed multi authority schema for that can support authentication of data consumers and generation of secret key.

Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. We also proved that our scheme was provable secure for cloud data. In this paper we can also provide data access policy for storing and retrieving data from the cloud. So that by implementing those concepts we provide efficient data access and also provide more security in cloud data.

V. References:

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network

[6] M. Chase, ''Multi-Authority Attribute Based Encryption,'' in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC'07), 2007, pp. 515-534.

[7] M. Chase and S.S.M. Chow, ''Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,'' in Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), 2009, pp. 121-130.

[8] A.B. Lewko and B. Waters, ''Decentralizing Attribute-Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11, 2011, pp. 568-588.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in Proc. 5th ACM Symp.

Information, Computer and Comm. Security (ASIACCS'10), 2010, pp. 261-270.
[10] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.
[11] J. Hur and D.K. 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.

BIOGRAPHIES:

Bheri Thrinadha is student in M.Tech (CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.Tech (IT) GMR Institute of Technology, Rajam, Srikakulam. His interesting areas are network security and web technologies.

Ramesh kumarbehara is working as Asst. professor in Sarada Institute of Science, Technology and Management, Srikakulam, Andhra Pradesh. He received his M.Tech (CSE)from Sarada Institute of Science,Technology And Management, Srikakulam, Andhra Pradesh. JNTUKakinada Andhra Pradesh. His research areas includeNetwork Security.