IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

A Secure File Store in Cloud Environment using HABE

S. Nandhini[1], R. Sangavi[2], S. Sangavi[3], S. Sowndarya[4]

UG, Department of CSE, MKCE, Karur, India[1, 2, 3, 4]

Abstract: In this project, we propose the HABE (Hierarchy Attribute-Based Encryption) scheme for shared data with large groups in the cloud. We make use of hash signatures to compute verification information on shared data so that the authority is able to audit the correctness of shared data, but cannot reveal the identity of the signer on each block. Hash signature and Keys are generated by Hierarchical Access Tree. We can implement auditing scheme to perform efficient public security to protect both identity and data privacy in cloud environments. Users can also access the data from the data owner through cloud provider in real-time dynamic cloud environment. Data reliability through replication of the original data. Manipulation of data in the replicas, there by maintaining the originality of the data. If hierarcical data are stored in different servers then the unauthorised users cannot access the data.

Keywords: HABE, Data replication, Cloud computing, ABE.

I. INTRODUCTION

Cloud computing is a large pool in which systems are connected in private or public networks, to provide the infrastructure for application, data and file storage. The cloud computing reduces the cost of computation. In which devices provide in on demand. Now a days most of the company's are used the cloud computing for the storage purpose. It is a virtualize one the user who store the information in the cloud. It cannot be find out by user. It will be store in anywhere[1]. Simply say the data store in anywhere and access from anywhere. Example of cloud computing is Yahoo email, Gmail, etc. For example, the personal health record (PHR).

To securely share the Personal Health Record information in cloud, a patient divides his Personal Health Record information (I)into two parts, personal record (i1)contains the patient's name, phone number, address, etc. The medical record (i2) which does not contains personal information, such as medical results, treatment protocols, and operation notes. Then CP-ABE scheme to encrypt the information (i1) and (i2) based on various access policies and actual need. For example, an attending physician wants to access both the patient's name and his medical record in order to make a diagnosis, and medical researcher only wants to access some medical test results for academic purpose, where a doctor must be a medical researcher, and the converse is not necessarily true. The patient sets the access structure of (i1) as: T1 ("Cardiology "AND "Researcher") AND "Attending Physician". Similarly, i2 is termed as: T2 "Cardiology" AND "Researcher". Where Y2= "Cardiology", "Researcher"}.we can find that the two access structures have hierarchical relationships where the access structure T1 is the extension of T2[2]. The two structures could be integrated into one structure T. If the two files could be encrypted with the integrated access structure and produce cipher text .Meanwhile authority person give secret key based on policy of information that will be divided by cloud service provider[12]. The people who access the information of the user, they also have the same type of the secret key then only they can able to access the information of the user. Here the major issue is the entire cloud user may able to access the user information. To avoid this problem mainly use the secret key. It means that all the person able to download all the information, before open the file authority person check the policy of that file. If it is match then only they can access the information. The major problem is that the user may loss the information. The new idea is that replication factor that means the user while store the information in the cloud to take the copy of the information. If the information may loss then the user use the copy of the information. To avoid the large storage space to copy the small amount of patient information.

II. LITERATURE SURVEY

[1] J.K.Liu-"Fine-grained two factor access controls for web-based cloud computing services":Fine-grained two-factor access control protocol for web-based cloud compute services, it is mostly used in web based application. The two factors are Secret key and Light weight security gadget.The user can be granted access only if he uses those two factors. Otherwise, the user cannot use his secret key with another device belong to others for the access. At the same moment, the privacy of the user is preserved[4]. The cloud system only knows that the user possesses some required attribute, but not the original identity of the user. Sensitive data may be stored in the cloud for convenient access and eligible users may also access the cloud system for various applications and services, user authentication is a critical component in

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

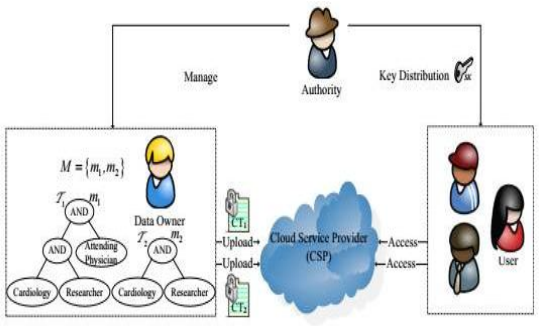
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

cloud system for that user is required to login before using the cloud services or accessing the sensitive data stored in the cloud[5].

[2]X.Xie-"An Efficient Cipher text-Policy Attribute-Based Access Control towards Revocation in Cloud Computing":In this paper the data owner (DO) encrypting the data before publishing in to the cloud, and then distributes the secret keys to all authorized data users (DUs). In this acheive data confidentiality and access control through following ways: (1) DO encrypt a file F with a at random private key k1 and sends the ciphertext C1 to the cloud; (2) If a DU wants to access E (F), he/she first sends the request to DO, thenDO response the k1 and access permit via a secure channel; (3) DU retrieves E (F) from the cloud storage by the permit and then uses k1 to decrypt it.This system can protect the data privacy in a way in which neither unauthorized users nor the untrusted CSP could obtain the plaintext.The access policy revocation is costly, because DO has to retrieve the data, and re-encrypt and re-publish it[13].

[3]T.H.Yuen-"K times attribute-based anonymous access control for cloud computing": In this paper, a user can validate itself in the cloud. The server just knows the user acquire some essential attribute, yet it does not be common with the individuality of this user. In k-times is mainly focal point in the member of staff serving at table may limit a meticulous set of user to access the system for a maximum k-times within a period or an event.Users can not access if login count exceeds given k limits[6]. We also prove the confidentiality of our instantiation. It can be used to provide unlimited times unspecified authentication. However, in the cloud computing environment, unlimited times access control is sometimes unattractive[7]. Let us take Netflix hosts its service in the cloud by enables its user to access the movies online[8].

III. SYSTEM MODEL



IV. EXISTING SYSTEM

Every data stored in the cloud is not fully secure. To improve the security of the data stored in the cloud in our existing system used the Hierarchy Attribute-Based Encryption[9]. Using this we can store the data in hierarchical structure and the third party user play a major role in this. They only generate the secret key for each and every node of the data in hierarchical tree structure[10]. Find the location of the data by using the hash signature. The unauthorized users can be easily access the data but they could not open it. If they want to open the file, they must satisfy the access policy.

DISADVANTAGES

The main problem of the existing system is that authority person generate the secret key for each and every node in the hierarchical structure for this its needs more number of keys are generated. The authority person is difficult to handle that data[11]. Another one is the authority person may possible to access the data owners.

V. PROPOSED SYSTEM

The data stored in the hierarchical structure it may possible loss the information for that we proposed the new idea is that while the data store in the different kind of server means the unauthorized users difficult to find the location of the data and also to reduce the storage space of the data we have to take the copy of the data in limited ways.

VI. EXPERIMENTAL RESULT

1. Data owner new registrations/login
2. CSP verification
3. Data owner upload file and in encrypting file
4. Data user download shared file and in decrypting shared file

VII. CONCLUSION

Here we proposed the Hierarchical Attribute-based Encryption algorithm in an efficient manner to achieve the more security in cloud environment. Existing system a chance to loss the information for that we proposed the replication concept to protect the data and save the storage space in cloud environment.

REFERENCES

[1] C. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou, "Securityconcerns in popular cloud storage services,"vol. 12, no. 4, pp. 50–57, October-December 2013.
[2] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. K. Liu, "TIMER: secureand reliable cloud storage against data re-outsourcing," vol. 8434, pp. 346–358, May 2014.
[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbasedrevocable identity-based proxy re-encryption scheme for public clouds data sharing," vol. 8712,September 2014.
[4] T. H. Yuen, Y. Zhang, S. Yiu, and J. K. Liu, "Identity-based encryptionwith post-challenge auxiliary inputs for secure cloud applications andsensor networks," vol. 8712, pp.130–147, September 2014.
[5] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X.Phuong, and Q. Xie, "A DFA-based functional proxy re-encryptionscheme for secure public cloud data sharing," vol. 9, no. 10, pp. 1667–1680,October 2014.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

[6] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "ktimesattribute-based anonymous access control for cloud computing," vol. 64, no. 9, pp. 2595–2608,September 2015.
[7] S.Saravanan, Arivarasan."An efficient ranked keyword search for effective utilization of outsourced cloud data" Journal of Global Research in Computer Science, Vol4(4), pp:8-12
[8] S Saravanan, V Venkatachalam ," Improving map reduce task scheduling and micro-partitioning mechanism for mobile cloud multimedia services" International Journal of Advanced Intelligence Paradigms ,Vol 8(2),pp157- 167,2016.
[9] S Saravanan, V Venkatachalam ," Advance Map Reduce Task Scheduling algorithm using mobile cloud multimedia services architecture" IEEE Digital Explore,pp21-25,2014.
[10] S.Swathi "Preemptive Virtual Machine Scheduling Using CLOUDSIM Tool", International Journal of Advances in Engineering, 2015, 1(3), 323 -327 ISSN: 2394-9260, pp:323-327.
[11] S Saravanan, V Venkatachalam, S Then Malligai "Optimization of SLA violation in cloud computing using artificial bee colony"2015, 1(3), 323 -327 ISSN: 2394-9260, pp:410-414.
[12] S. Saravanan, Vikram R ,"Improved Performance Analysis Image Segmentation Based on Cluster Image", Journal of Chemical and Pharmaceutical Sciences,issue 1,2017,pp92-95
[13] S. Saravanan, Vikram R ," Evolutionary Calculations on Gravitational Interactions Method of Global Leader Organize ", Journal of Chemical and Pharmaceutical Sciences,issue 1,2017,pp115-118

DOI 10.17148/IJARCCE.2017.6345