DYNAMIC SECURITY OF ROBUST ROLE BASED ACCESS CONTROL FROM MULTIPLE AUTHORIRITES

Shalmali Nighot [1], Tabbsum Patel[2], Shubhangi Tekude[3]

[1-2] Dept. of Computer Engineering Jaihind College of Engineering, Pune, Maharashtra, India
[3]Asst. Professor, Dept. of Computer Engineering Jaihind College of Engineering, Pune, Maharashtra, India

---***---

Abstract – *Data integrity maintenance is the major objective in cloud storage. It includes audition using TTP for unauthorized access.This work implements protecting the data and regeneration of data if someone mishandles it. This job will be assigned to a Proxy server. The data of the users will be stored in public and private area of the cloud. So that only public cloud data will be accessed by user and private cloud will remain more secured. Once any unauthorized modification is made, the original data in the private cloud will be retrieved by the Proxy server and will be returned to the user. Cloud storage generally provides different redundancy configuration to users in order to maintain the desired balance between performance and fault tolerance. Data availability is critical in distributed storage systems, especially when node failures are prevalent in real life. This research work explores secure data storage and sharing using proposed AES 128 encryption algorithm and Role Base Access Control (RBAC) for secure data access scheme for end user. This work also carried out backup server approach it works like proxy storage server for ad hoc data recovery for all distributed data servers. The experiment analysis has proposed in public as well as private cloud environment.*

Key Words: -Crop-recommender, Machine Learning, React, Progressive net App, API.

1. INTRODUCTION

Now a day's cloud storage is used to store and retrieve data that is based on the internet, instead of local storage devices for more reliable, secure, and availability of data. But data is very important and should not be revealed to any unauthorized person, for this purpose encryption method is used to convert this plain data into cipher text and a decryption method is used to convert that cipher text into plain text to get back the original data. So, the encryption algorithm plays the most important role to make data more secure [2]. This research work explores secure data storage and sharing using the proposed AES 256 bit encryption algorithm and SHA-256 algorithm for Role Base Access Control (RBAC) for a secure data access scheme for the end-user. This work also carried out a backup server approach it works like a proxy storage server for ad hoc data recovery for all distributed data blocks. The experimental analysis has been proposed in public as well as private server storage environments. [1] Fig.1 shows the overall system overview

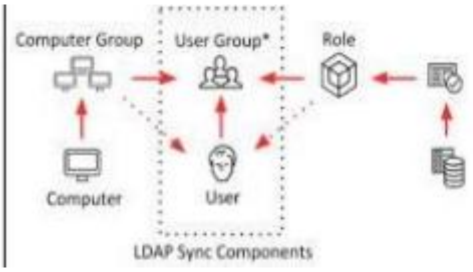

Fig.1: System Overview

The system depicts the principle plan objectives of the proposed plan including key circulation, information secrecy, access control, and effectiveness as takes after: Key Distribution: The prerequisite of key transportation is that clients can competently get their personal / private keys from the gathering director without a Certificate Authorities. In other existing plans, this purpose is skillful by expecting that the communication channel is secure, on the other hand, in our plan, the system can accomplish it without this solid thought. Access control: first, gather individuals can employ the cloud asset for records stockpiling and data sharing. Second, unapproved clients can't get to the cloud asset each time, and disavowed clients can be unfitted for utilizing the cloud asset again as soon as they are renounced [5].

2. MOTIVATION

In existing system, a user can be a Data Owner and a Data Consumer simultaneously. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them. Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree Tp can execute the operation associated with privilege p. The server is delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree Tp.

3. LITERATURE SURVEY

Attribute-Based Access Control with Efficient Revocation in Data Outsourcing System. Authors:-1.Junbeom Hur 2.Dong Kun Noh

Attribute based encryption helpfull to secure the data from unautherized user. Identity based encryption: Introduced by Adi Shamir in 1984 Messages encrypted for an identity. User only need to know identity of recipient Eg " userB@gmail.com "

Fuzzy Identity-Based Encryption:- Introduced by Sahai and water in 2005. View identity as a set of attributes Assign attribute to every user. Encrypt message with attribute set. Example : Suppose owner set the all attributes as universal attribute U and W be an identity having set of attribute, than the user or that identity can decrypt the data if and only if W subset of U. Features:- Provide more security. Encryption and Decryption on user attribute. Disadvantages:- Data owner need to use every authorized user's public key. Less Access policy. Title:- Key Policy Attribute Based Encryption (KP-ABE) Authors:-1. Parmar Vipul Kumar 2.Victor Shoup Description:- Two Flavours of ABE 1.KP-ABE 2.CP-ABE*

Key Policy Attribute Based Encryption (KP-ABE) Authors:-1.Parmar Vipul Kumar 2.Victor Shoup Description:- Two Flavours of ABE 1.KP-ABE 2.CP-ABE Example :- User encrypted a message M and produces ciphertext C with a set of descriptive attributes C1 (3,5,6,7). Every user private key is associated with an access structure. A user with access structure A(1 AND 2) cannot decrypt the message M as this access structure does not satisfy the set of attributes associated with the ciphertext. Another user with access structure A(3 OR 5) can decrypt the ciphertext as this access structure satisfy the attributes of ciphertext . Similar access structures A((1 AND 2) OR (3 OR 7)) and A (3 out of (1,2,3,4,5,6,7)) qualifies the ciphertext to decrypt while the access structure A (2 out of (1,2,5)) does not qualify. Advantage:- Fine-gained access control More flexibility to control user than ABE scheme. Disadvantages:- Encryptor cannot decide who can decrypt the encrypted data. Only one TA which is data user Example :- If the access structure in encrypted data is 1 AND (2 OR 3). If a set of attributes in user's private key is (1 AND 2), then the user can decrypt the data. Advantage:- Encryptor can decide who can decrypt the encrypted data. Less computational overhead than KP-ABE. Disadvantages:- flexibility and efficiency is less for broad cast type system. Only one TA which is data owner. In CP-ABE only static attributes are satisfied there is no dynamic attribute is used.

Hybrid Attribute Based Encryption. Authors:-1. GD Makkar

2. Vivek Panwar Title:- Fragmentation of Data in Large-Scale System For Ideal Performance and Security. Authors :- 1.Dr. Shubhangi D.C 2. Sonali V .Katke Description:- ▪ Used to incresing the security in cloud computing . ▪ The data file is divided into fragments, and these fragments are placed on the nodes, in order to provide the security to the data in the cloud. ▪ The fragmented file is encrypted and is stored within the network in a distributed fashion. ▪ At decryption time if attributes are matched then all fragmented data is combine in sequence manner and user get data. Hb-ABE:- Combination of both CP-ABE and LBE. Advantages:- Proper Key managment. hierarchy of authorities instead of using single trust authority as in the case of KP-ABE and CPABE. All static and dynamic attributes like location are satisfied . Location based encryption is used for securing mobile communication by limiting area inside which the recipient can decrypt the message. Title:- Fragmentation of Data in Large-Scale System For Ideal Performance and Security. Authors :- 1.Dr.Shubhangi D.C 2. Sonali V .Katke Description:- Used to incresing the security in cloud computing . The data file is divided into fragments, and these fragments are placed on the nodes, in order to provide the security to the data in the cloud. The fragmented file is encrypted and is stored within the network in a distributed fashion. At decryption time if attributes are matched then all fragmented data is combine in sequence manner and user get data.

4. PROBLEM STATEMENT

In the proposed research work to design and implement a system which will provide the data security from collusion attack in trusted as well un-trusted cloud environments. The system will focus long communication scenario between data owner, user, TPA and authorities using different security techniques, it will provide highest security than all existing approaches

5. PLATFORM FUNCTIONALITY

Practicality The platforms functioning is contains 2 varieties of actors(User and Data Owner) .

Data Owner practicality includes:

♣ Update the data within the portal the data should get on the premise of last ten year anlysis.

♣ Provide the data needed by the Users .

User functionality:

♣ Obtaining information/data from portal according to their serch.

6. EXSISTING SYSTEM

System there's several computerised system for the Data storage and retrival .but some drawback are Delegation problem. No guarantee that calculated result returned by cloud is always correct that is some times cloud provides fake result.

7. PROPOSED SYSTEM

In proposed system we are going to upload the data from users onto server so it can available multiple authorized user for 24 hours. To provide a data security we are going to use an standard encryption algorithm and divide data into cunks and store it on multiple servers and give a backup to the data single server.

8. FUTURE WORK

In this work system propose a secure Role Base Access Control (RBAC) data sharing scheme for untrusted environment in the cloud. In our scheme, the users can securely get their private keys from middleware authorities, TPA provide and secure communication between multi users. Also, our scheme is able to to provide the secure revocation for untrusted user. The proxy key generation has also proposed in this work. When data owner revokes any specific end user system automatically expired the existing keys and generates new keys for all shared users. The system can achieve highest level security as well as privacy through such approaches.

9. CONCLUSIONS

In this work system propose a secure Role Base Access Control (RBAC) data sharing scheme for untrusted environment in the cloud. In our scheme, the users can securely get their private keys from middleware authorities, TPA provide and secure communication between multi users.

Also, our scheme is able to provide the secure revocation for untrusted user. The proxy key generation has also proposed in this work. When data owner revokes any specific end user system automatically expired the existing keys and generates new keys for all shared users.

The system can achieve highest level security as well as privacy through such approaches.

10. ACKNOWLEDGEMENT

We would like to take this opportunity to thank our project guide Prof. Bhosale D.S. for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful. We are also grateful to thank, our other faculty members from the Computer Engineering Department, Jaihind college Of engineering, Kuran for allowing us to perform our project.

11. REFERENCES

[1] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2017.

[2] Jianan Hong, Kaiping Xue and Wei Li, "Comments on "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi-Authority Data Access Control for Cloud Storage Systems", IEEE transactions on information forensics and security, VOL. 10, NO. 06, June 2017.

[3] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", IEEE transactions on information forensics and security, VOL. 10, NO. 01, January 2017.

[4] Kan Yang and Xiao huaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.

[5] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th Financial Cryptography and Data Security. Springer, 2010, pp. 136-149.

[6] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no.1, pp. 69-73, 2012.

[7] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing, vol. 8, no. 1,pp. 92-106, 2015.

[8] J. Yuan and S. Yu, "Public Integrity Auditing for Dynamic Data Sharing with Multiuser Modification," IEEE Transactions on Information Forensics and Security, vol. 10,no. 8, pp. 1717-1726, Aug. 2015.

[9] Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J.Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Transactions on Services Computing, vol.6, no. 2, pp. 409-428, 2013.

[10] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers, vol. 62, No.2, pp. 362-375, 2013