INTERNATIONAL JOURNAL · ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 20th Sept2017. Link :http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-8

Title: **ANONYMOUS AUTHENTICATION OF DATA STORED IN CLOUDS FOR DECENTRALIZED ACCESS CONTROL**

Volume 06, Issue 08, Pages: 255– 261.

Paper Authors

SHAIK GUL MUBEENA, M.SIVALAKSHMI

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ANONYMOUS AUTHENTICATION OFDATA STORED IN CLOUDS FORDECENTRALIZED ACCESS CONTROL

[1]SHAIK GUL MUBEENA, [2]M.SIVALAKSHMI

ABSTRACT: Here we are representing the methodlogy and implementation in decentralized access control with anonymous authentication of data stored in clouds were all the drawbacks related to data stored in clouds system are eliminate by the application of various security level in the clouds system .These implementation will help to secured data in clouds system from various Wrapping attacks, Malware - Injection attacks, Flooding attacks, Browser attacks, and also Accountability checking problems .Protection of data over the clouds system must be main goals. We identify the root causes of these attacks and propose specific solutions.

Key Words: Two factor level Authentication, Deletion of right over cloud to creator, Secret key Generation, Access right to admin, Access control, Authentication, Attribute-based signatures, Attribute-based encryption, Cloud storage, Encryption and Decryption data in clouds system.

I.INTRODUCTION Cloud Computing is mostly used for Corporations, usually for webservers. There are a couple of different Cloud Computing strategies that are common. The first is a Content Delivery Network (CDN) such as Amazon's cloud service. A CDN lets you upload a file to one server and then have it distributed across tens, hundreds or even thousands of servers around the world. The file will be available for download from any one of those servers, and if one server fails, the user automatically downloads from the next available server on the cloud. By default, the user downloads from the closest server or the server with the lowest ping time. The advantage is that there is an extraordinary amount of redundancy and the speed at which users can download will likely increase. In addition, the traffic load from the downloads is taken off your main/central webserver where you host your web pages. Another strategy is to form a linked network of tens or hundreds of servers that all work together as one unit to provide a web service for example. If one of the 'nodes' in the cloud fails, it does not affect the rest of the cloud (well no drastic effects), and the node can easily be replaced without having any downtime. The traffic and system resource load is easily distributed across the different server nodes. When a business says it's moving to 'the cloud', it means that instead of hosting their web site or web service in-house with their own server... they are instead outsourcing their web service to a server-farm/cloud where there is less maintenance involved and less chance of failure. The only major disadvantage to moving to the cloud is that you rest your data security in the hands of your cloud provider which may be a problem for companies with very confidential data. Some companies like Yahoo (but namely Google) build their own server clouds to run all their web services for searching, email etc. Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. cloud computing is basically doing everything online, using applications and storing data online. It is for everyone, anyone can use google docs google mail sky drive etc. In fact google brings out a laptop next year which will be a pure cloud computer where everything is done online. Cloud Computing enables cloud workload mobility using continuous replication of your entire cloud application stack. A single click creates an exact replica of the entire workload, including its up-to-the-second consistent state at a target cloud location within minutes, complete with instances, attached volumes containing all the data, network topology, firewalls, and more. While snapshot-based and backup solutions result in high RPO and degrade performance of the replicated machines, some Cloud Companies do it in real-time, truly continuous block-level data protection (CDP) ensures maximum uptime and minimal loss of data without consuming additional resources at the source application. You can then create a fully functioning, up-to-date copy of the application within minutes. The result is 1-click, failsafe replication of your entire application to, across, and between multiple cloud locations. CloudEndure automatically discovers the network topology of your workload (IP addresses, subnets, load balancers, firewalls) and transforms it to the compatible format of the target cloud. This ensures that the functionality of the replica workload is identical to the source. We use CloudEndure in our office (we build SEO technologies) and it is excellent. A computing capability that provides an abstraction between the computing resource and its underlying technical architecture (e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

A. Our Contributions The main contributions of this paper are the following:

1) Access the system when the are authenticated.

2) Access right is provided by admin.

3) Secret key is needed to access system.

4) Addtion to that is owner is also provide with secret key ,which can be use to provide more security to clouds system.

5) Authentication access is also provide to owner ,so genuine owner can access service and attacker owner will not allows to use services so this increases security our clouds.

6) Owner has been provided with the right to delete there data our the clouds with the help of secret key provided to the during the registration.

7) The protocol supports multiple read and write on the data stored in the cloud.

8) Without genuine secret key provided to owner no one can delete data over clouds, so this create more security over data in clouds.

9) The Main architecture is decentralized, meaning that there can be several KDCs for key management.

10) While login process in owner is provided with two factor authentication so this increases more security.

11) Admin has right to activated authenticated genuine owner and user to access service in clouds system.

12) Secret key is established using various string and integer.

13) Hence all drawbacks related to security of data in clouds system is secured by application of AES keys method from various type of attacks.

14) Secret key is also provided to user for reader/writer to accesses data in clouds system.

15) Admin has given right to give access to both user and creator.

II. LITERATURE REVIEW

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud Computing offers the users an opportunity to purchase already deployed Computing Infrastructure (by the providers, such as Google, Microsoft, Amazon) to run ones' applications.One can dynamically acquire as many computing resources as one wants on demand. Cloud providers already have large data centers (simply saying a repository of servers), having hundreds of thousands of servers. Means they already have the hardware. If you require 10 servers to run your application, you can acquire 10 servers and you have to pay as per your use. “Cloud Computing is the delivery of computing as a service rather than a product where by shared resources, software and information are provided to computers and other devices as a metered service over a network (typically internet)”. Though its quite clear but I understand that it needs more explanations. Cloud Computing is a methodology of providing services in every tier (ie. App, Process and data) For example, if you are working in tier 3 i.e Data then you might need a huge amount of storage. From where would you get it? an option would be to simply ask your organization to get you a huge storage by starting a data server which surely would cost a hefty amount to your organization. Also, when your database needs expansion so will you require more space and hence more data servers adding up the woes of your organisation. The second way is to go for a cloud service like google+ etc get your certificate and start the data server. With very low initial cost you can start your data storage and later on if you need to expand it will not add much to your bills. This data server which you got is a virtualized storage and the physical place would be somewhere in the Google data center. Now, why would google do this for you? Yes, They will charge you by your usage and i think that's the best way. You didn't have to own a storage before storing. Similarily, you dont require a OS before running an application, you dont require a physical server to run your own website, You might own a big firm spread across the world but you dont need to purchase s/w or infrastructure at every place. Just need to get it from a cloud service provider. So, cost efficiency is the major benefit of cloud computing. Inside this we have more benefits like, easy and efficient expansion or scaling. So how do we achieve this? Large Scale Distributed Systems that's all. What are the issues in cloud? there are many as of now, but with time they will be dealt. Major are like compliance issues, Migration issues, Security in some areas etc. Hope this explanation helps you.

III. EXS IS TING S YSTEM Existing work on access control in clouds are centralized in nature. All schemes use ABE or symmetric key approach and does not support authentication. Earlier work provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where a single Key Distribution Center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. Although a decentralized approach is proposed in some of the existing papers, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, a distributed access control mechanis m in clouds was proposed. However, the scheme did not provide user authentication. The other draw back was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. Cloud servers are prone to Byzantine failure, where a storage server can fail in arbitrary ways. The cloud is also prone to data modification and server colluding attacks. In server colluding attack, the adversary can compromise storage servers, so that it can modify data files as long as they are internally consistent. To provide secure data storage, the data needs to be encrypted. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques. Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption. The keywords are sent to the cloud encrypted, and the cloud returns the result without knowing the actual keyword for the search. The problem here is that the data records should have keywords associated with them to enable the search. The correct records are returned only when searched with the exact keywords. Security and privacy protection in clouds are being explored by many researchers. Many homomorphic encryption techniques have been suggested to ensure that the cloud is not able to read the data while performing computations on them. Using homomorphic encryption, the cloud receives cipher text of the data and performs computations on the cipher text and returns the encoded value of the result. The user is able to decode the result, but the cloud does not know what data is has operated on. In such circumstances, it must be possible for the user to verify that the cloud returns correct results.

Disadvantages of Existing system

The identity of the user is not protected from the cloud during authentication.

- There can be only one KDC for key management.
- Access control of data stored in cloud is centralized.
- Two users can collude and access data or authenticate themselves, if they are individually not authorized This is called collusion attack.
- Revoked users can also access data even after they have been revoked.
- Prone to replay attacks
- Single read and writes on the data stored in the cloud.

IV.PROPOS ED S YSTEM Here we have implemented various methodlogy releted to the security of data or files in clouds system. Basically the data store in clouds my be vulnerable to many kinds of attacks over the clouds system ,securing the data in clouds system must be import tasks for developer to develop a system were all the possible type of attacks can be nullified. Various security level has be implemented over the clouds system which make the clouds system more secured over various types of attacks.

- Validate user only access data to read & write.
- Validate owner can upload data to the clouds system.
- The uniqueness of the user and owner is protected from the cloud during validation process with their identification.
- Validate owner can delete data over the clouds by using secret keys.
- The system also has the feature of access control in which only legal users are able to decrypt and encrypt the stored information in clouds system.
- All access right are provided to admin only for both user and owner.
- The system prevents replay attacks and supports development, variation, and evaluation data stored in the cloud for both user and owner.
- Secret keys the important part or roles in clouds system.

V. S YS TEM ARCHITECTURE

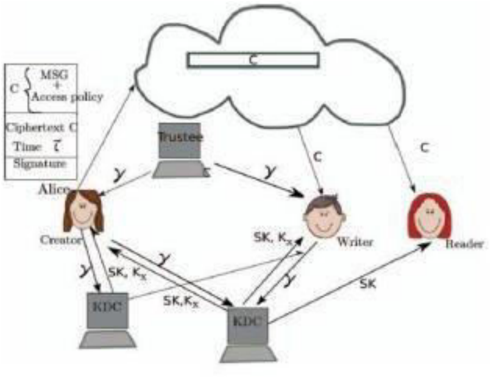


Fig-1 Decentralized Access Control With Anonymous Authentication of Data Stored in Clouds

A. Access Control Module: This 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 it do not get the file, otherwise server ask the public key and get the encryption file .If u want the decryption file means user have the secret key.

B. Distributed Key Policy Attribute Based Encryption : KP-ABE is a public key cryptography primitive for oneto-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized. The encryptor associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access structure. Encryption: It takes a message as input &.outputs a cipher text.

Key Generation: Generate a key use to validate the user identity. It outputs user secret key. Decryption: It takes as input cipher text, user get the message in the original format.

C. File Assured Deletion: The policy of a file may be denied access to user if the key is wrong or any malious activity is done while entering the secrete key. Only valid user will access the file this will give the authentication more security in cloud. .The user put the wrong key multip le time the user consider as attacker. This will give assured that file is deletated by the valid person.

D. Two factor level Authentication: This is provided by using secret key and password to access to upload data over clouds.

E. Deletion of right over cloud to creator: This is done with the help of secrert key provide to owner to delete data over clouds.

VI. DETAIL DES IGN

System Initialization:

The System Initialization is the initial process for the system. The system get initialized for the user. The user can register within the system.

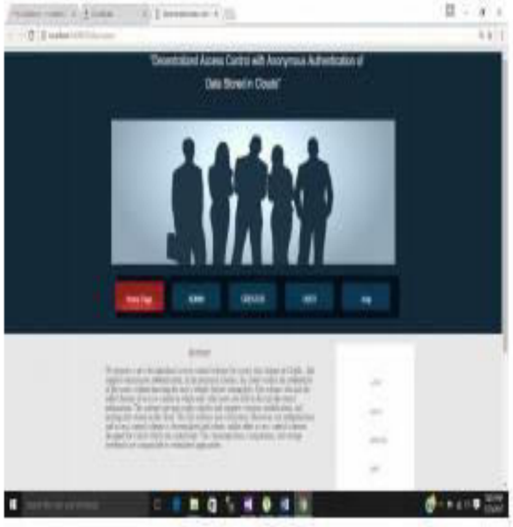
Admin Module: Admin check the request from the user to access the system. Admin activate only the valid user, Admin have right to remove the attacker from system. Admin can see the login history & file created by creator.

Creator Module:Creator create the file and upload in the cloud to access or see to user & Creator can see the file history

User Module:The User have to register themselves under the registration module. According to the user credentials, which will be provided by the users, the user will get the secrete key. User with the authentication can read & write in the file. Reader can only read the file & Writer can able to write. but Writer cannot able to create file.

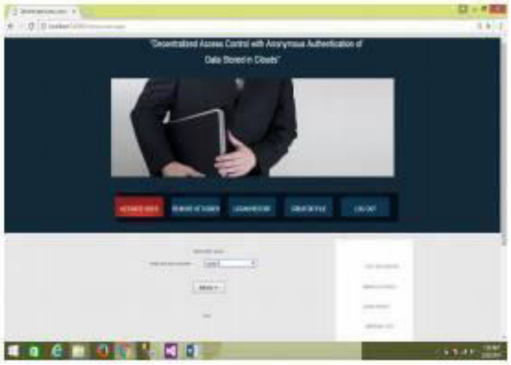
VII. SCREENS HOT

•HOME PAGE



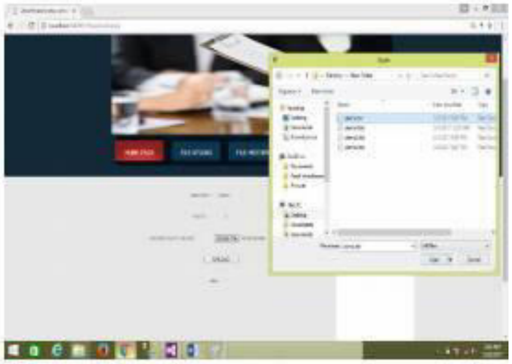
"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds"

- Admin page



"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds"

- Creator page:



- User page(writer):

VIII CONCLUSIONS

Hence we have implemented an decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user/owner that stores information, but only verifies the user's/owner's credentials or records store in database system. Key distribution is done in a decentralized way. All drawbacks related to pervious paper has been overcomes related to security reasons over clouds system.

REFERENCES

1. Sushmita Ruj, Milos Stojmenovic, Amiya Nayak CSE,Indian Institute of Technology, IIT, Indore, India, –sush@iiti.ac.in Singidunum University, Belgrade,Serbia mstojmenovic@singidunum.ac.rs SEECS, University of Ottawa, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014

2. S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp.556–563, 2012.

3. C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE T. Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

4. Kan Yang, Xiaohua Jia and Kui Ren, " DAC-MACS:Effective Data Access Control for Multi-Authority Cloud Storage Systems", IACR Cryptology ePrint Archive, 419, 2012.