Two Stage Novel Security Approach for the Encrypted Cloud Data

KURELLA S N RAM JAGAN[#1], **PYDIPALA LAXMIKANTH** [#2]

[#1] M.Tech Scholar, Department of CSE,
Chaitanya Engineering Collège, Kommadi, Visakhapatnam., AP, India.

[#2] Head & Associate Professor, Department of CSE,
Chaitanya Engineering Collège, Kommadi, Visakhapatnam., AP, India.

ABSTRACT

Cloud Server has the capability to insert a lot of valuable data on its memory block in a centralized manner in order to provide retrieve, download access and modify the data to and from its centralized location. As we all know that in current days there was no mechanism available to store the data in an encrypted manner in all public clouds and even private clouds. All the data is stored remotely and retrieved from the remote machines not from the local machines, hence the secrecy of data plays a vital role by the cloud service providers. As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption and key access in order to provide data authorization. In this thesis, we proposed and analyzed a secure, easily integrated two cloud data storage in which cloud server is mainly divided into two parts: One part is used for data storage and other part is used for key management.So here the privacy plays a vital role in which valid users can able to access the data and un-authorized users cant able to access the data. Here we launched two roles like Trustee and Attribute Authority for giving security and key access for the data in a secure manner.By conducting various experiments on our proposed model, our result clearly tells that our proposed system is practical and efficient.

Key Words:
Data Authorization, Privacy, Key Management, Cloud Service Provider, Centralized Server.

I. Introduction

As we all know that there are many applications available in the real time cloud computing like data sharing for remote systems to a centralized location [2], big data management systems [1], medical information system etc. Each and every cloud users try to access the applications from their PC through web browser to access, store, retrieve the data to and from the cloud server.There are many principles which really govern the principle of cloud computing, but still a lot if security and privacy issues arise in the cloud computing. All the sensitive data will be reside in the cloud server for sharing and access to and from the remote access, the major issue that arise in the cloud based services is authentication of the cloud server. Initially the cloud user or end user need to register into the cloud server and then once he/she got registered, then the user should substitute his valid credentials for login into the system for various applications and services access[1].

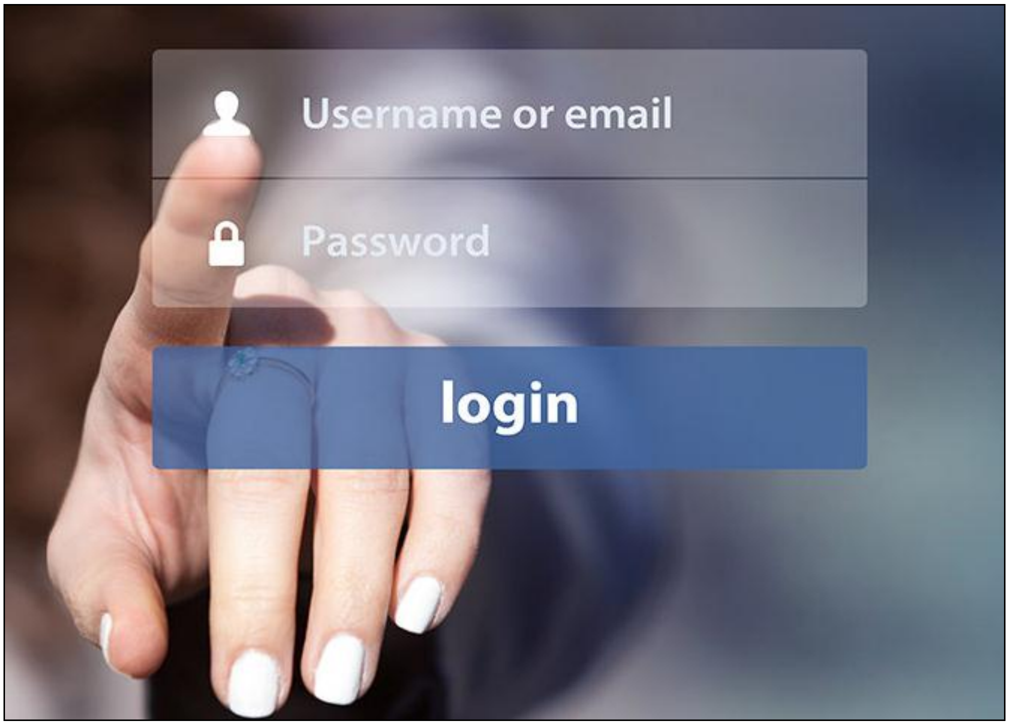

Figure 1.Represents the Traditional Cloud Password Based Authentication

From the above figure 1,we can clearly identify that during the process of login into the cloud, there will be two main problems that arise in the traditional cloud based systems like one is account/password based authentication is not strictly privacy preserving, the second one is the problem that arise in the primitive cloud based services is as we all know that the data from the cloud server will be accessed from different people from different locations and hence it may be very easy for a hacker to install some spyware software to learn the login password in any way from the web browser[2].Hence this traditional password based authentication is no more secure in the current cloud servers to protect their sensitive data inside the cloud storage. Also one more main limitation that takes place in the current cloud server is there are lot of SQL injection attacks that takes place in breaking the cloud firewall and try to gain access illegally for the sensitive data from the cloud server.

Hence in this current thesis , we try to propose a two stage novel security approach for the encrypted cloud data, in which there are two main security primitives that are integrated for the cloud servers in order to protect the sensitive data and give access for the authorized users rather than un-authorized access. The two main security primitives that are used in the current application is :

1) Trustee and
2) Attribute Authority.

The trustee is one who tries to give security token for each and every individual user at the time of login into the system and also it try to verify the identity of user during file download. The security token has some following advantages like

a) It can compute some lightweight algorithms, e.g. hashing and exponentiation; and

b) It is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside [3].

The next security primitive which is used in our proposed application is: Attribute Authority in which the authority tries to upload all the sensitive documents into the cloud server. The authority will encrypt the files and then try to upload all the files into the centralized storage medium in a secure manner, so that if any user who wish to access any file cant able to download the file directly. Each and every individual user try to request the authority for getting file access permission and once if the authority gives access permissions, then the corresponding user will receive a secret key to the registered mail id.This secret key is used for accessing the file in a decrypted manner[4]-[7].

II. Background Work

In this section we mainly discuss about the background work that was carried out inorder to find out the proposed Two stage novel security approach for the encrypted cloud data in order to provide the security for the data which is stored in the cloud server. Now let us discuss about that in detail as follows:

Motivation

We can clearly find out that there are four different services available in the cloud storage and one among them is DaaS which is the main service that what we are using now for providing security for the current application that and prove that this service also gives the best security for the data which is stored inside the cloud memory locations [7]. Now let us discuss about each and every service in detail as follows:

A. IaaS (Infrastructure as a Service)
B. PaaS(Platform as a Service)
C. SaaS(Software as a Service)
D. DaaS (Data /Data Base as a Service)

A. IaaS (Infrastructure as a Service)

This is the first service out of various services that are available in the cloud. This service mainly deals with application level and it is basically used to set the infra-structure for the users[8]. This service is mainly used to create infrastructure for the set of PCs that are linked in an area. The persons who come under this service is IT Professionals, this is clearly shown in the figure 2.

B. PaaS (Platform as a Service)

The second important service in the cloud computing is Platform as a Service, where this is mainly used for customization of cloud server. Here in this service we try to set the platform for the users, where the developer comes under this service. Here the cloud server customizes which type of platforms is needed for their company usage is seen in this service[9].

C. SaaS (Software as a Service)

The third service one among the best services in cloud computing is Software as a Service, where this is mainly used for a consumer to use the cloud service provider’s applications running on a cloud IaaS [10]. Generally business end-users come under this service where all the software’s that are required for running the cloud are processed in this service.

D. DaaS (Data/Database as a Service)

This is the last one among the set of cloud services that was launched and included in various cloud client services is DaaS, which is clearly seen in below figure 2.This DaaS service is used mainly for storing the data in the form of encrypted manner [11]. As this is having various advantages compared with other cloud client services, it has a small limitation like the data which is stored in this DaaS is not stored in the encrypted manner which is stored in the plain manner. So in this proposed thesis we try to encrypt the data before it is uploaded into the cloud using DaaS service.

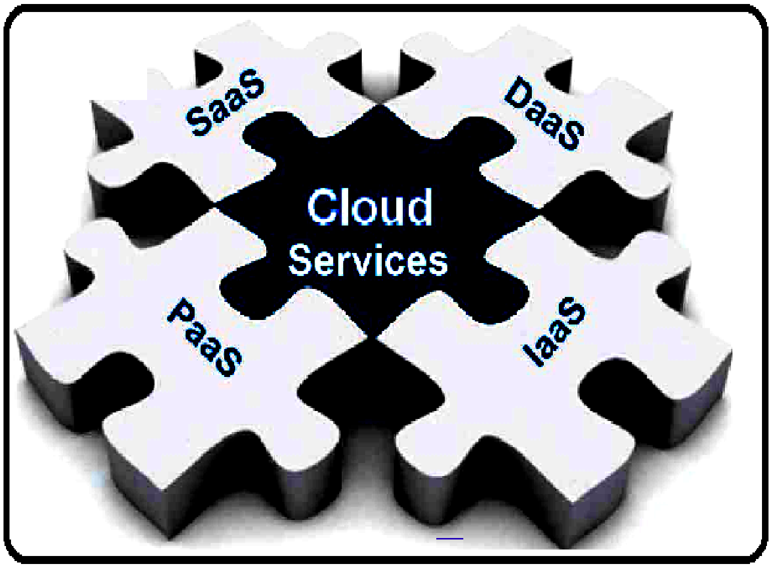

Figure.2. Represents the Various Cloud Services In Real Time Environment

Also we enabled this DaaS service by providing extended security by using two stage novel security approach for the encrypted cloud data in which the cloud user need to get the access privileges from these two individual departments for accessing the file from the cloud server. If any user try to access the files from the cloud server, he/she need to get two access permissions like Token as well as secret key from two individual departments for downloading the data in a plain text manner from the cloud server, if he/she fail to enter valid keys during authentication, the data can't be downloaded in a plain text manner[10]-[12].

III. Two Stage Novel Security Approach for the Encrypted Cloud Data

In this section we will mainly discuss about proposed approach for secure data storage inside a cloud server. Now let us discuss about this proposed model in detail as follows:

Motivation

A Two stage novel security approach for the encrypted cloud data mechanism mainly consists of following entities like

1. **Trustee:** It is responsible for generating all system parameters and initialise the Security device (I.e. OTP).

2. **Attribute-issuing Authority:** It is responsible to generate user secret key for each user according to their attributes.

3. **User:** It is the player that makes authentication with the cloud server. Each user has a secret key issued by the attribute-issuing authority and a security device initialized by the trustee.

4. **Cloud Service Provider:** It provides services to anonymous authorised users. It interacts with the user during the authentication process.

In this proposed thesis, we consider the following threats:

1) **Authentication:** The adversary tries to access the system beyond its privileges. For example, a user with attributes
   {Student, Physics} may try to access the system with policy
   “Staff” AND “Physics”. To do so, he may collude with other users.

2) **Access without Security Device:** The adversary tries to access the system (within its privileges) without the security device, or using another security device belonging to others.

3) **Access without Secret Key:** The adversary tries to access the system (within its privileges) without any secret key.Here device is nothing but OTP [10].

4) **Privacy:** The adversary acts as the role of the cloud server and tries to find out the identity of the user it is interacting with.

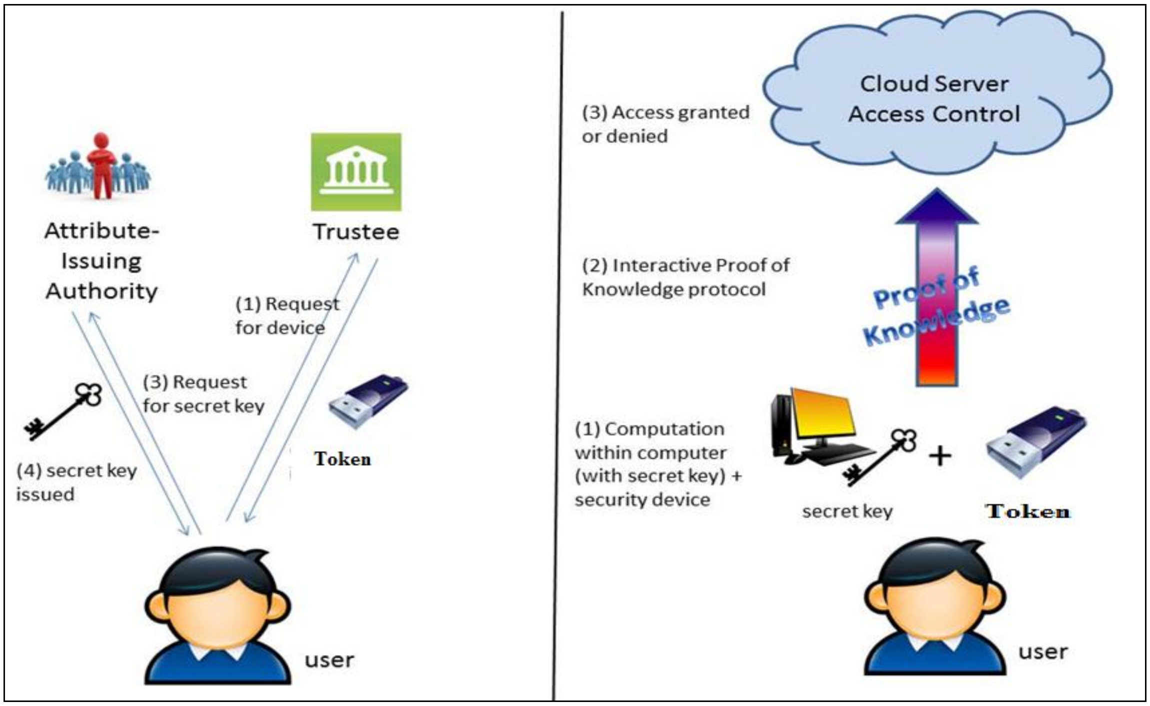

Figure.3. Represents the Proposed Architecture of Two Stage Novel Security Approach for the Encrypted Cloud Data

From the above figure 3, we can clearly represent the proposed architecture in which the user enters two main phases :

a) One is Key Generation Phase
b) Second is Key Verification Phase

If we look clearly from the figure 3,left side part indicates the generation phase and right side part indicates the verification phase.The following are the step by step procedure for the Two Stage Framework Algorithm.

a) User Key Generation Process

STEP 1:

Initially the user needs to register into the application with all his basic details

STEP 2:

After registering the user need to request the Trustee for token generation and this token is used for getting login into the account.

STEP 3:

User receives the token from the trustee and in turn use that token for getting login into the account.

STEP 4:

The User once login into the account with his authorized token, try to request the Attribute Authority for getting secret key to download the file.

STEP 5:

The User receives the secret key from the attribute authority for the requested file

b) User Key Verification Process

STEP 6

The user try to verify the Secret key and Token with the cloud server, so that cloud server validates both the user inputs.

STEP 7

The system will validate the user inputs and then try to give access for that corresponding file.

STEP 8

The system will try to give conformation like access granted or denied based on the user inputs.

IV. Implementation Phase

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed application. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My-SQL Server. Here we used a live cloud server like DRIVEHQ for showing the performance of our proposed application. The application is divided mainly into following 5 modules. They are as follows:

1. Data User Module
2. Two Stage Access Control Module
3. Trustee Module
4. Attribute Authority Module
5. Cloud Server Module

Now let us discuss about each and every module in detail as follows:

1. DATA USER MODULE

In the first module, every user needs to register while accessing to cloud. After user registered, at the time of user login then user need to provide one time key to access user home.One time key will be provided by cloud. key will be corresponding user mail id.After user access the user home, User can view the all files upload in cloud.User need to send the file request for both trustee and authority.After user have the two factor access control, user can download the corresponding file.

2. TWO STAGE ACCESS CONTROL MODULE

If user need to access file in cloud. They need to get the two stage access control.

1. **Trustee:** Need to get security response from trustee for corresponding file.
2. **Authority:** Need to get secret key from authority for corresponding file.

3. TRUSTEE MODULE

It acts as admin for cloud server. Trustee will give request for all files security response when user request for any file.Initailly this trustee will give token access for entering into the application and it also provides access permission during file download for the valid users.

4. AUTHORITY MODULE

Authority will upload the file in cloud. And uploaded file will store in drive HQ in encrypted format. Authority will give secret key for all files when user request for any file and the secret key will be send to corresponding user mail Id.

5. CLOUD SERVER MODULE

In this module the cloud server can view uploaded files in cloud. It can also view the details and log information of downloaded files by user in cloud. This cloud server is mainly used for monitoring the log information of file upload and file download details. As a part of data storage we try to integrate real time cloud service provider in this proposed application like DRIVEHQ public cloud account to show the performance of our proposed application in a real time manner.

V. Conclusion

In this thesis, we for the first time have proposed Novel TWO STAGE APPROACH (including both user secret key and a lightweight security device like token) access control system for accessing the sensitive information from the cloud server in a secure manner. Based on the attribute-based access control mechanism, the proposed two stage access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. By conducting various experiments on our proposed protocol, our comparison results clearly tell that our proposed approach is best in providing security for the sensitive data which is stored inside the server space.

VI. References

[1] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in *Proc. ACM SIGMOD Int. Conf. Manage.Data*, 2004, pp. 563–574.

[2] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,”in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006,pp. 79–88.

[3] C. Cocks, “An identity based encryption scheme based on quadratic residues,” in *Cryptography and Coding*. Cirencester, U.K.: Springer,2001, pp. 360–363.

[4] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, “An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing,” in *Proc. 19th ESORICS*, 2014,pp. 257–272.

[5] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, “Security concerns in popular cloud storage services,” *IEEE Pervasive Comput.*,vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[6] Ilzins, O., Isea, R. and Hoebeke, J. Can Bioinformatics Be Considered as an Experimental Biological Science 2015

[7] Raul Isea The Present-Day Meaning Of The Word Bioinformatics, Global Journal of Advanced Research, 2015.

[8] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, “Secure sharing and searching for real-time video data in mobile cloud,” *IEEE Netw.*, vol. 29, no. 2, pp. 46–50, Mar./Apr. 2015.

[9] *Ehrlich, M; Wang, R. (19 June 1981). "5-Methylcytosine in eukaryotic DNA". Science.**212** (4501): 1350–1357*

[10] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, “TIMER: Secure and reliable cloud storage against data re-outsourcing,” in *Proc. 10th Int.Conf. ISPEC*, 2014, pp. 346–358.

[11] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, “Secure sharing and searching for real-time video data in mobile cloud,” *IEEE Netw.*, vol. 29, no. 2, pp. 46–50, Mar./Apr. 2015.

[12] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, “Security concerns in popular cloud storage services,” *IEEE Pervasive Comput.*,vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

VII. About the Authors

KURELLA S N RAM JAGAN is currently pursuing his 2 Years M.Tech in the Department of Computer Science and Engineering at Chaitanya Engineering College, Kommadi, Visakhapatnam., AP, India. His area of interest includes the Cloud Computing and IOT.

PYDIPALA LAXMIKANTH is currently working as an Head & Associate Professor in the Department of Computer Science and Engineering at Chaitanya Engineering College, Kommadi, Visakhapatnam., AP, India. He has more than 14 years of teaching experience in various engineering colleges. His research areas include the Data Mining, Web Mining,Bio Informatics.