Secured Client Server Communication in Cloud Environment

C.Nithya[#1], A.Parvathy[#2], Pethuru Raj[##3], K.Thenmozhi[#4], J.B.B. Rayappan[#5] and Rengarajan Amirtharajan[#6]

[#]School of Electrical & Electronics Engineering, SASTRA University, Tamil Nadu, India – 613401
[##] Infrastructure Architect, Global Cloud Center of Excellence, IBM India, Bangalore, 560045
amir@ece.sastra.edu

***Abstract*— It's smarter to rent than to buy such kind of service is provided by cloud computing. It is a model that is used for delivering resources that can be either Software or Hardware. Its means getting resources through network and more over that charges based only on the amount of computing resources used. Cloud service such as infrastructure as a service is caught for a security issue because by nature it is dynamic and multi tenancy. The common threats to the data in cloud are access to the data by any unauthorized user or cloud provider himself may not be trustworthy. In this paper traditional cryptography techniques are adopted by the client to achieve the user's control over the entire data. Security aspects such as integrity, confidentiality and authentication are considered to have secure data storage. Through advanced encryption scheme and hashing for user's data to preserve it from the security breach in data storage where it is stored in a large data centre.**

I. INTRODUCTION

Cloud computing, established in the year 1967 is the interconnection of several computer devices that allow the users to have a virtual access of internet resources, that is, it allows the user to store the data as audio files, images, text files and video. Cloud provides three different services such as Software as a service (SaaS), Platform as a service (Paas) and Infrastructure as a service (Iaas). In SaaS, software can be accessed from cloud by the user and Paas includes Operating System(OS), execution environment for programming language. Database management and web server services are provided by Iaas. In cloud there are various kind exist namely private, public, hybrid and community clouds [1]. Particular group or an organization thereby limiting its use by others devoid of that group is called private [2]. Allocation of resources by the vendors varies dynamically for users based on their applications in web.Even the functionality and services are offered even outside the corporation to clients called public [3]. Hybrid cloud is the mixture of private and public clouds. Commodity cloud is the specification of cloud from National Institute of Standards and Technology (NIST). Even though cloud is a high scale resource pool which has a problem of security and reliability. The obstacle for the cloud growth is security; each layer of cloud has various kinds of issues. The cloud users need to understand the risks before entering to it [4, 5]. Cloud under HDFS architecture is considered by having some mathematical model to resolve the problem of security issues [6]. Security **plan** besides these issues of cloud should be considered Such as Attack Proactive Alerting, Data Leak Prevention, Security Accident Notification, response and Security Incidents Audits. With this background the traditional schemes like Firewalls, policies to maintain security and Virtual Private Networks(VPN) ensures the data security in the cloud must be enhanced so that fruitful service from the cloud.

Data in the cloud is not only meant to the owner, even the third party cloud can also acess, so to permit the access only to the authorized users security must be ensured [7-9]. In this paper, the client side security is concentrated in addition with the cloud security schemes like authentication.

II. PROPOSED METHOD

The Fig 1 shows the general architecture of cloud, there are so many web services provided by cloud. Mail servers and file servers are also available as a large data centre to give various services. The virtual machines will be allotted according to the availability to the end users.

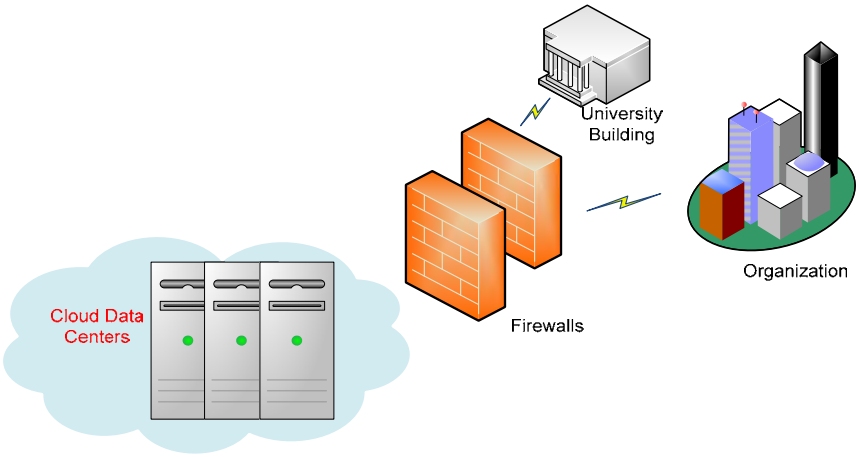

Fig. 1 General Architecture of Cloud Service Providers

A. Phase 1: Request for access

Since cloud is a multitenant architecture many users can request for service. Upon the request by the client for accessing the cloud, the CSP acknowledges the client by providing a user login and authentication code which is randomly generated one. The flow is explained in the following steps as in Fig 2.

Step 1: Request to the CSP for accessing the cloud.

Step 2: Acceptance of request by providing a unique authentication code which is also encrypted & given to the client.

Step 3: Client receives the authentication code.

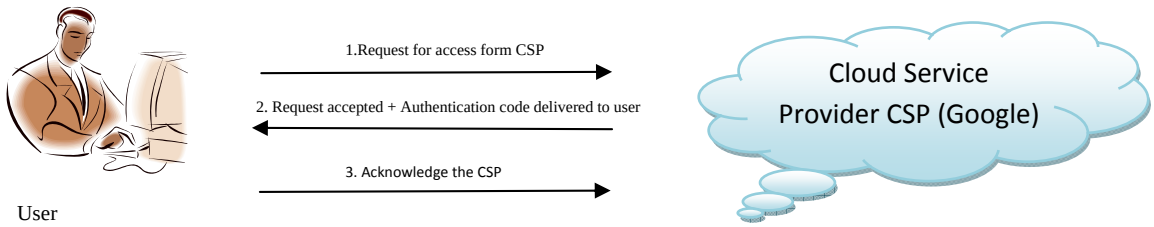

Fig 2: Mode of registration in Cloud Service Provider (CSP)

For sending request: (From client side)
for each message {
open socket
send MAIL FROM
send RCPT TO
send REQUEST
close socket
}
For sending acknowledgement (From server side)
for each message {
open socket
Poll for inbox message
send MAIL FROM
send RCPT TO
generate authentication code randomly
encrypt the code
send authentication code

close socket

}

B. Phase 2: File uploading

High level of security is required for the data stored in the cloud although the CSP is trustworthy. So a method of symmetric key encryption is adopted for securing the data that is stored in the private area of cloud as in Fig 3. Block ciphers are generated from the file where the scrambling of a data is takes place successfully. Although, this is only from the client side, the CSP ensures the confidentiality by providing an authentication code without which access to the cloud is denied. Since existing policy schemes of CSP will take care about the access control in a secure manner. But with this proposed approach still the security aspects are achieved.

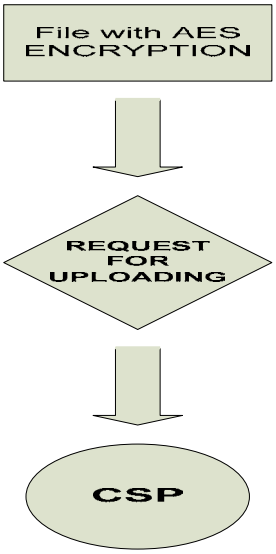

Fig.3 File Uploading

For Uploading a file: (From client side)

for each message {

open socket

send MAIL FROM

send RCPT TO

send encrypted file FILE

close socket

}

C. Phase 3: File download

Cloud is a large data centre the file uploading along with retrieval is very important and there is a need to have guarantee for no intrusion. Whenever user wants to download the file they will be asked for the authentication code for ensuring intrusion free access as in Fig 4. The authentication code is provided by the CSP by the time of access request when the user accepted as a client for CSP.

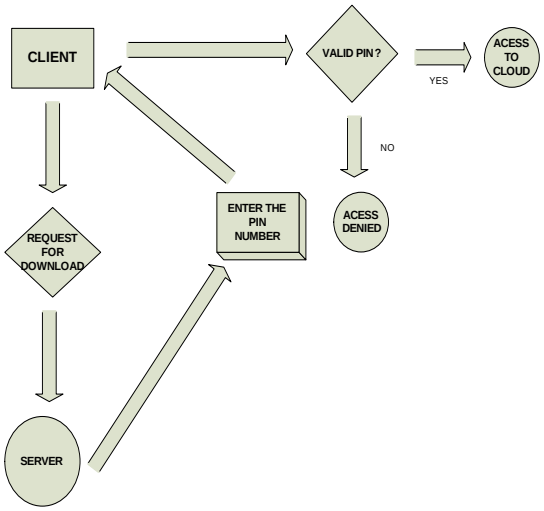

Fig.4 File Downloading

For Downloading file
for each message {
open socket
send MAIL FROM
send RCPT TO
receive FILE
close socket
}

III. RESULTS AND DISCUSSIONS

In cloud infrastructure the security becomes an issue, but through the proposed approach the user can enjoy in secure platform even it is trustworthy since it is from client side security. The Fig 5 shows how the request from the client reaches cloud service providers. CSP always poll message to know whether it is for request, upload or download. If it is for request then the authentication code generated by the server randomly and sent to the client as acknowledgement which is shown in Fig 6.

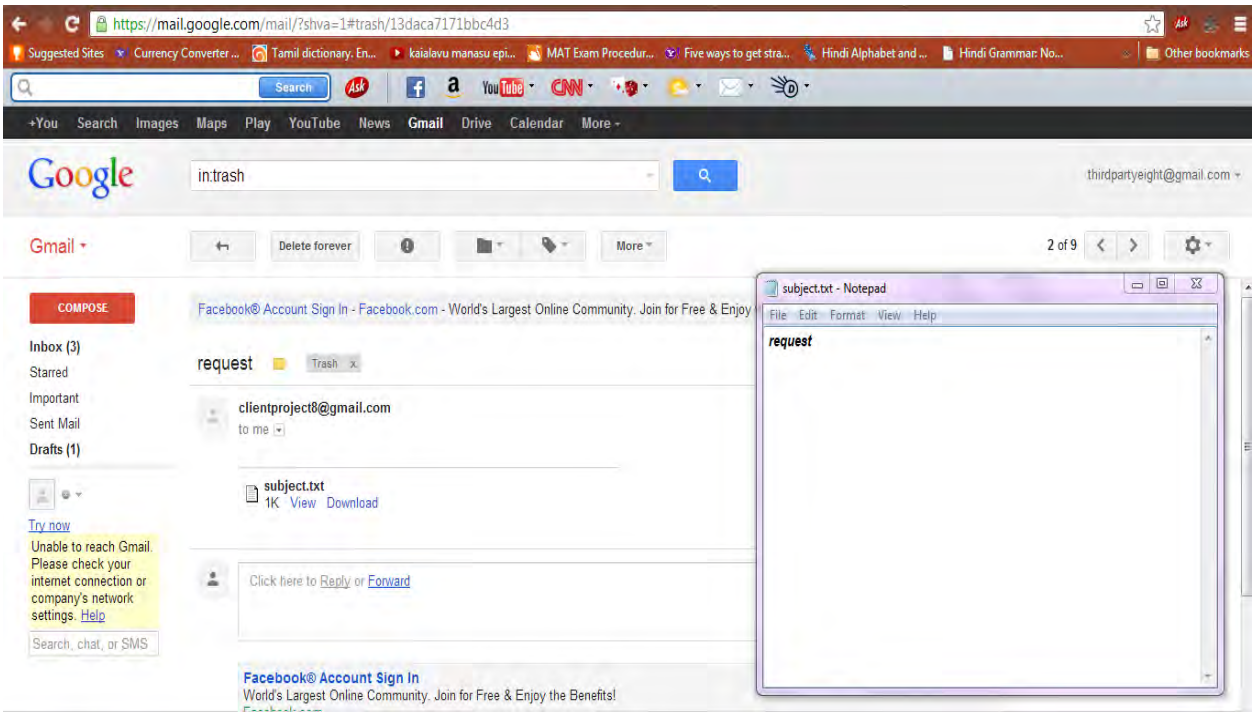

Fig.5 Request to CSP

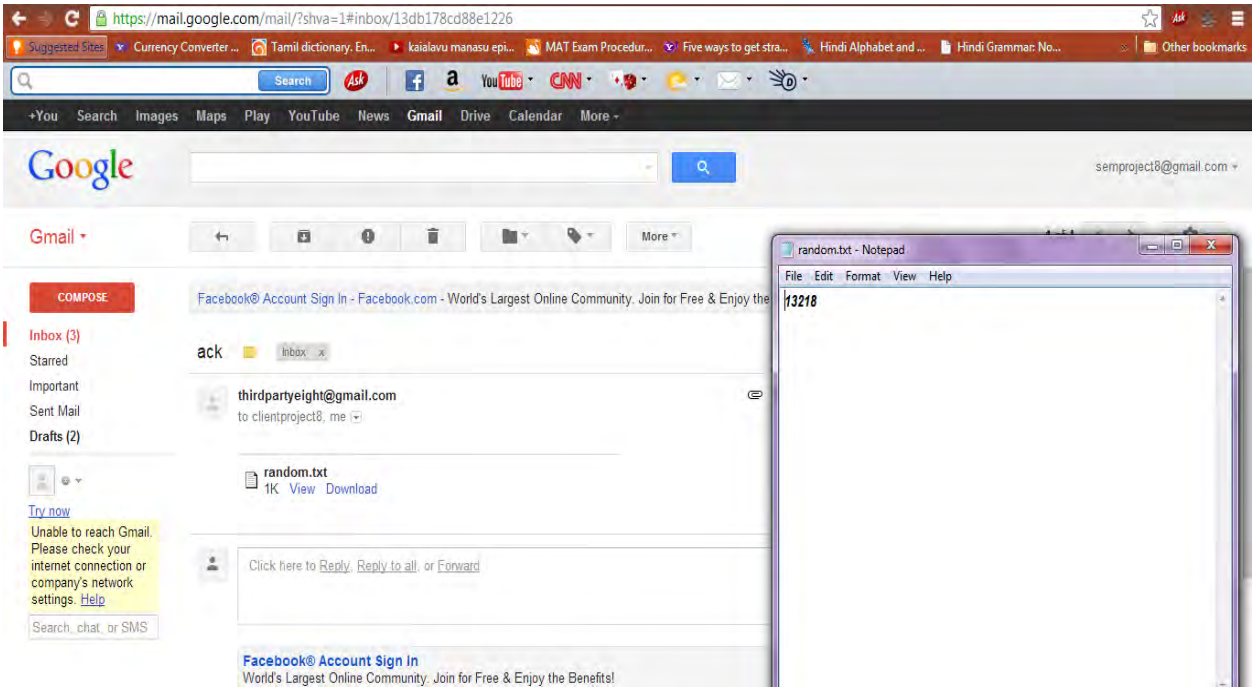

Fig.6 Acknowledgement from CSP

After getting the access permission from the CSP the user can upload the file. By using AES encryption scheme the file is being encrypted then will be uploaded. Because of user intervention server won't be overloaded even client becomes responsible for everything irrespective of CSP. If the subject of the mail service is upload then the server will be accept the file from the client and the data is stored in the virtual server of cloud. The below Fig 7 illustrates the above described details.

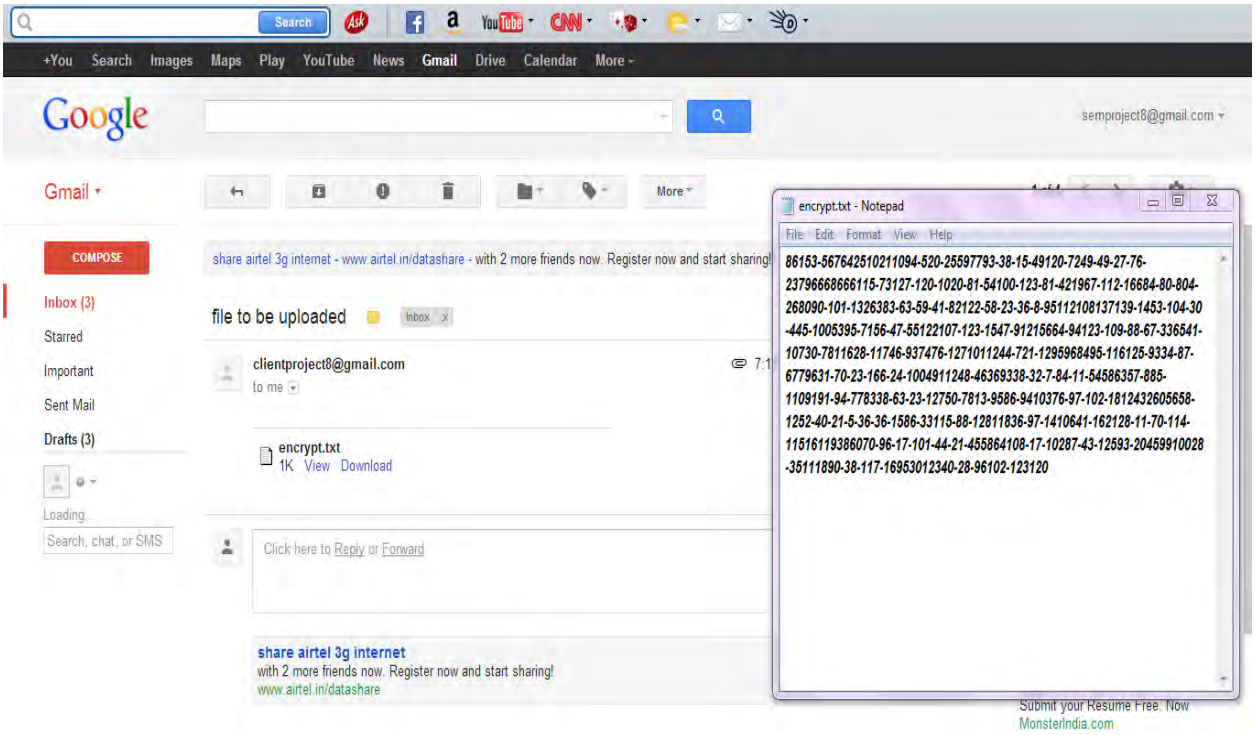

Fig.7 Uploading a file from CSP

When the client is asking for download then CSP give them an encrypted file after getting the correct authentication code. The code is verified by CSP so that security aspects are achieved with fully controlled access. If the code is correct then the client can log on else access denied. The following Fig 8 shows the described one.

```
run:
download
Enter the aunthentication code:
13218
YOU HAVE SUCCESSFULLY LOGGED IN
BUILD SUCCESSFUL (total time: 2 minutes 45 seconds)

   run:
   download
   Enter the aunthentication code:
   13228
   ACCESS DENIED
   BUILD SUCCESSFUL (total time: 6 seconds)
```

Fig.8 Authentication Code Verification

Then the encrypted file is getting downloaded from CSP. Then the received file is decrypted by the client with proper key shown in the following Fig 9.

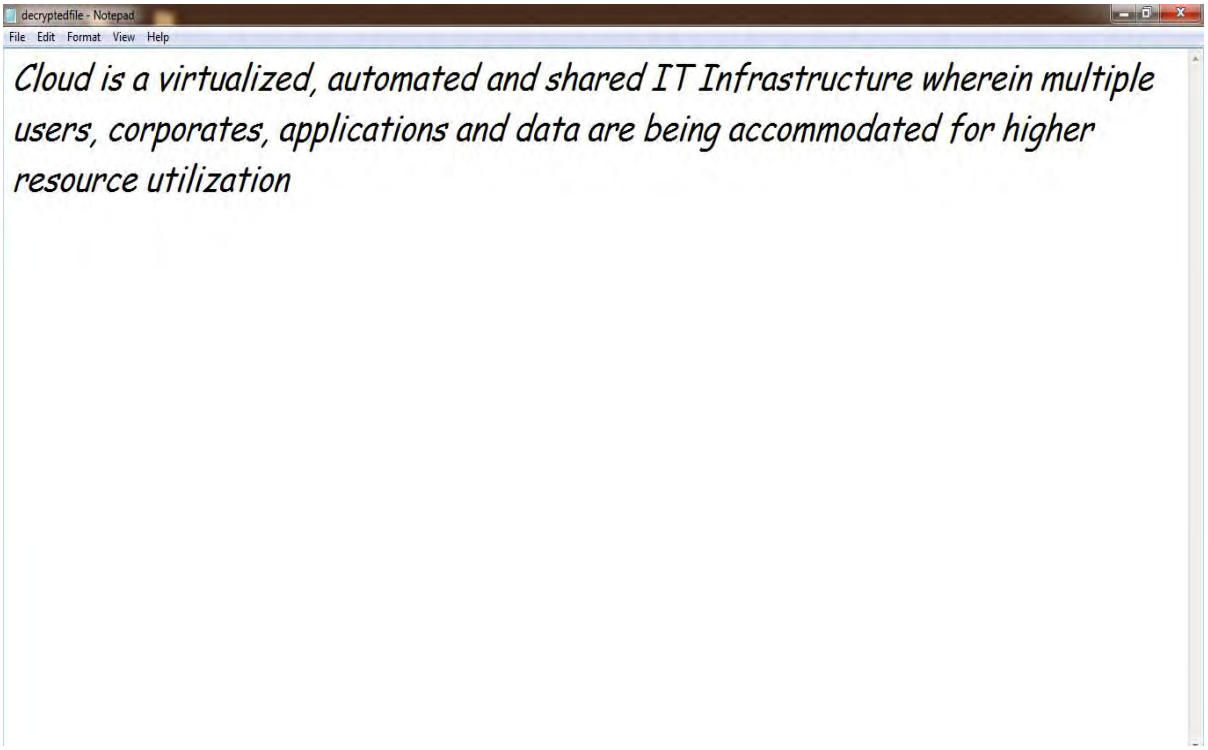

Fig.9 Decrypted File in the Client End.

IV. CONCLUSION

In this paper, the proposed model stating that it would definitely lay a challenge to the attackers and the hackers in specific in cloud environment. The above proposed model is a type of two levels - authentication wherein the access control to cloud is through the" Authentication code" which is also encrypted through public key algorithm. Although this level seems to be preliminary; this forms the strong base for the data security. Also to maintain the integrity, the file to be stored is encrypted and the same is decrypted after the download from the cloud. AES is used in this proposed methodology where side channel attack and brute force attack is also challenging one. To further extend the above proposed model three level authentication can also be included only in case of utmost necessity. This proposed model is experimented in Gmail which is one of the Google's cloud-based service.

REFERENCES

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Network and Computer Applications*, vol. 34, no.1, pp. 1-11, 2011.

[2] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583-592, 2012.

[3] Yingjie Xia, Li Kuang, and Mingzhe Zhu. "A Hirerchical Access Control Scheme in Cloud using HHECC," *Inform. Technol. J.*, vol. 9, no. 8, pp.1598-1606, 2010.

[4] S. K. Sood, "A combined approach to ensure data security in cloud computing," *J. Network and Computer Applications*, vol. 35, no. 6, pp. 1831-1838, 2012.

[5] D. Chandramohan, T. Vengattaraman, M.S.S Basha, and P. Dhavachelvan, *MSRCC - Mitigation of security risks in cloud computing*, 2012.

[6] J. Han, W. Susilo, and Y. Mu, "Identity-based data storage in cloud computing," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 673-681, 2013.

[7] C. Liu, X. Zhang, J. Chen and C. Yang, "An authenticated key exchange scheme for efficient security-aware scheduling of scientific applications in cloud computing," In *Proc. IEEE 9th International Conference on Dependable, Autonomic and Secure Computing, DASC 2011*, pp. 372, 2011.

[8] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," In Jaatun, M.G., Zhao, G., Rong, C. (eds.) Cloud Computing. LNCS, vol. 5931, pp. 157–166, Springer, Heidelberg, 2009.

[9] L. Kang, X. Zhang, "Identity-Based Authentication in Cloud Storage Sharing," In *IEEE International Conference on Multimedia Information Networking and Security*, pp. 851–855, 2010.