Smart Cloud Storage Service in Public Cloud Using Dropbox

B. Srujana,
M.Tech Scholar
Department of Computer Science &Engineering
Vignan’s Institute of Engineering for Women
Kapujaggarajupet, Visakhapatnam
Email:borrasrujana@gmail.com

P.Vijaya Bharati,
Asst. Professor
Department of Computer Science &Engineering
Vignan’s Institute of Engineering for Women
Kapujaggarajupet, Visakhapatnam
Email:pvijayabharati@gmail.com

Abstract— Cloud computing is a collection of technologies that have come together with the use of internet, it will serve the customer’s or user’s. While user’s store their data in the cloud it is important that the data should be in a secure manner. For maintaining the data securely we have proposed a scheme which consists of three entities those are users, TPA and the cloud server. Here in the place of cloud server we have used Dropbox. By implementing this concept we will be able to provide security for the data which is stored in the cloud server from the un-authorized access. This concept is applicable for accessing data either in distributed environment or can run the application concurrently by number of cloud users. The main objective is to store the data in the public cloud in an encrypted form rather than in a plain text manner for maintaining data security and confidentiality.

Keywords: *Authentication, Security, Confidentiality*

*****

I. Introduction

In these days cloud computing plays a very important role in almost all aspects of real time environment like industries, hospitals, software companies and so on. Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models are completed by an end user layer that encapsulates the end user perspective on cloud services.

In the cloud domain there are mainly three types of services which were developed based on different models. But as the cloud usage is increased, there were many other services evolved. One among the evolved cloud services is: Storage as a Service .Generally in a cloud context, wherever crucial info is placed in infrastructures of untrusted third parties, guaranteeing the knowledge confidentiality is of overriding importance [1], [2].This imposes clear knowledge management choices: original plain knowledge should be accessible solely by trusty parties that don’t embrace cloud suppliers, intermediaters, and internet. In any untrusted context, knowledge should be encrypted. Satisfying these goals has completely different levels of complexity on the sort of cloud service. During this context, we propose a new methodology. In the below figure it is clearly identified that various types of services like application oriented services, infrastructure oriented services and platform oriented services are existing. In these days a lot of educational institutions and large scale industries are showing their valuable interest in cloud computing. In the cloud computing domain all the users will store the data on servers. As this cloud storage was introduced, a lot of maintenance work is reduced for users in maintaining the data on-site. Almost all the data which was stored in cloud is very secure like financial and patient records. Thus we can say that security and privacy parameters, plays a vital role in cloud computing.

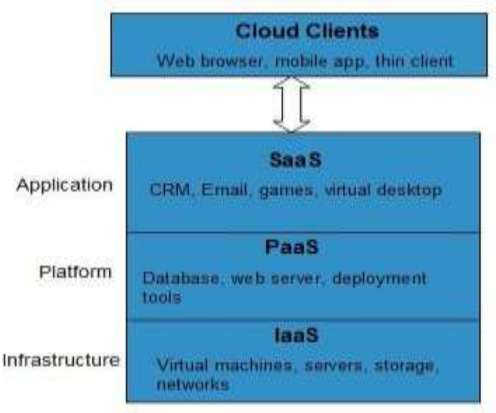

Cloud Clients
Web browser, mobile app, thin client
Application
SaaS
CRM, Email, games, virtual desktop
Platform
PaaS
Database, web server, deployment tools
Infrastructure
IaaS
Virtual machines, servers, storage, networks

Figure 1: Represents the flow of cloud client and various Services

On one side, the user ought to manifest itself before initiating any dealings, and on the other side, it must be ensured that the cloud doesn’t make unauthorized alterations with the information that is outsourced. User privacy is additionally needed so the cloud or alternative users don’t apprehend the identity of the user. The cloud will hold the user in control of the info it outsources, and likewise, the cloud is itself responsible for the services it provides.

II. RELATED WORK

This paper intends a new methodology that is different from previous work in the field of secure cloud database services. Cryptographic file systems and secure storage solutions represent the earliest works to provide confidentiality and integrity of data outsourced to untrusted cloud storage services. There are many solutions guaranteeing confidentiality for the storage as a service paradigm ([3], [4], [5]). There are many existing solutions for the storage of the data such as SPORC [4], SUNDR [9], but we are implementing a new methodology which was better than the previous.

III. PROPOSED SYSTEM

In the proposed system there are three entities. They are users, TPA and the cloud server. For data auditing we have used TPA(Third party auditor).Generally user files will be stored in the cloud server but the user can access this application only after TPA will logged in and it will activates the user then the users can proceed to their data storage. Here we are not maintaining the local copy of the data which was stored by the user in the cloud server. The data which was stored by the user is directly uploaded in the cloud server in an encrypted manner it means at anywhere the actual content (plain text) of the user is not stored. For accessing their own data at any time users will get the permission from the dropbox and then the data is decrypted and users can view their data. And TPA will monitor the users access and verifying that whether the users are authorized or not. As the third party auditor TPA also cannot view the actual data, TPA just verify the user's authenticity and their activities. From the below figure we can easily understand how actually the process will work.

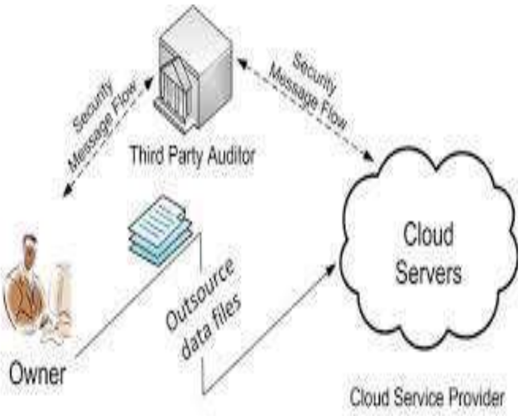


Figure 2: Represents the Architecture of Data Audit in Cloud Server

Generally Storage as a service is the one among the various services that are provided by the cloud. In Storage as a Service the data is stored in the form of plain text, but in this paper we try to store the data in a secure manner by encrypting the data before it is stored in to cloud server in which it provides the valid authentication while retrieving the data from the cloud server. Here for the encryption we have used DES Algorithm.

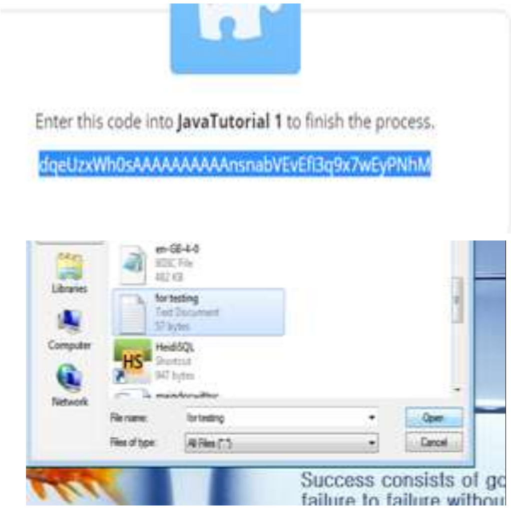
This new methodology will give guarantee for the information which is stored in the cloud server in terms of confidentiality, where the user who has uploaded the data can only access the data directly with his privileges, where others can't access.

IV. RESULTS AND EXPERIMRNTAL ANALYSIS

Procedure for file Processing:

Step1: User wants to process the file but TPA will activate the user first.
Step2: For uploading the file user needs to get permission and key from the dropbox.
Step3: After getting key from dropbox, file is stored in dropbox in an encrypted manner.
Step 4: For file downloading user will enter the dropbox key.
Step 5: Dropbox key is changed for every access.
Step 6: If the user gave incorrect details encrypted file is downloaded.

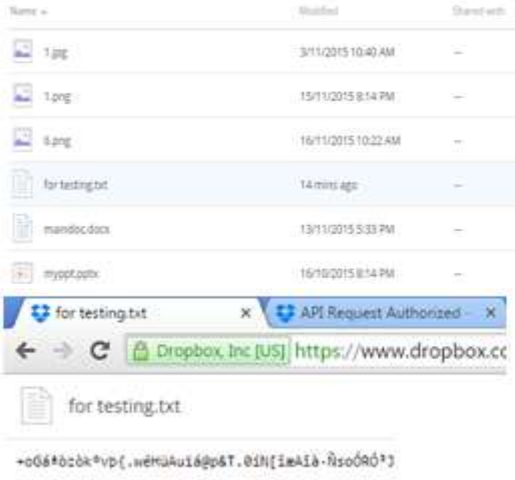
From the proposed system it is observed that the data which was stored in cloud server is in a secure manner. Every time for processing file access the user needs to enter the dropbox secret key, this key is changed for every access. Our experimental result for encrypted data storage in dropbox is shown below.



Enter this code into **JavaTutorial 1** to finish the process.

dqeUzxWh0sAAAAAAAAAnsnabVEvEfi3q9x7wEyPNhM

Figure 3: File uploading Process

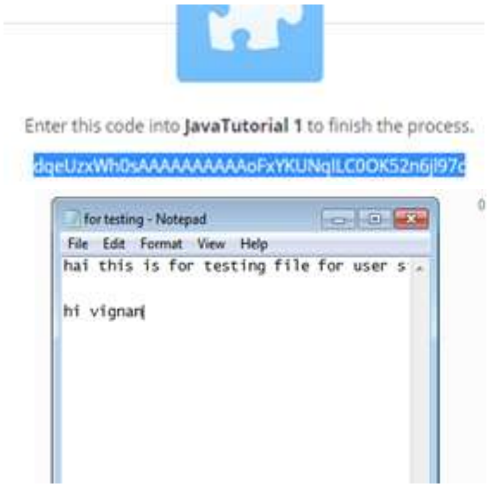


Name	Modified	Shared with
1.jpg	3/11/2015 10:40 AM	--
1.png	15/11/2015 8:14 PM	--
6.png	16/11/2015 10:22 AM	--
for testing.txt	14 mins ago	--
maindoc.docx	13/11/2015 5:33 PM	--
myppt.pptx	16/10/2015 8:14 PM	--

for testing.txt

```
+oGá*bzòk*vp{.wéHüAuiá@p&T.0iN[iæAìà·ÑsoÓRÓ³}
```

Figure 4: File stored in cloud server in Encrypted Form



Enter this code into **JavaTutorial 1** to finish the process.

dqeUzxWh0sAAAAAAAAAoFxYKUNqILC0OK52n6jl97c

```
hai this is for testing file for user s

hi vignan
```

Figure 5: Different code for File Downloading and Actual data after Decryption

V. CONCLUSION

In this paper we clearly proved that the proposed methodology guarantees security and confidentiality of data stored in public cloud server. It does not require any alterations to the cloud server, and it is immediately applicable to existing cloud server. As in this proposed model the data is stored in an encrypted form in the cloud and it also clearly provided an accurate result in maintaining audit for the cloud data storage. In this we have used Dropbox as live cloud storage for storing the data in an encrypted manner and accessing the data at a same time by different users from the distributed systems.

REFERENCES

[1] T.Grance and W.Jansen, Guidelines on Security and Privacy in Public Cloud Computing. Technical Report Special Publication800-144, NIST, 2011.

[2] M. Armbrust et al., A read of Cloud Computing, Comm. of the ACM, vol. 53, no. 4, pp.50-58, 2010.

[3] H. Hacigumu s¸, B. Iyer, C. Li, and S. Mehrotra, Executing SQL over Encrypted Data in the Database-Service-ProviderModel, Proc. ACM SIGMOD Int’l Conf. Management Data,June2002.

[4] A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten, SPORC: cluster Collaboration Using Untrusted Cloud Resources, Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, Oct. 2010.

[5] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan, CryptDB: Protecting Confidentiality with Encrypted QueryProcessing, Proc.23rd ACM Symp.Operating Systems Principles,Oct. 2011.

[6] P.Mahajan, S.Setty S.Lee, A.Clement, L.Alvisi, M.Dahlin, and M.Walfish, Depot: Cloud Storage with stripped-down Trust, ACMTrans,laptop Systems,vol,29,no.4,article 12,2011.

[7] H.Hacigu”mu” s,B.Iyer, and S.Mehrotra, Providing information as a Service, proc. eighteenth IEEE Int’l conf,Data Eng.,Feb 2002.

[8] C. Gentry, Fully Homomorphic Encryption Using Ideal Lattices, Proc. 41st Ann. ACM Symp. Theory of Computing, May 2009.

[9] J.Li, M.Krohn, D.Shasha and D.Mazie’res, SecureUntrustedDataRepository(SUNDR), Proc, Sixth USENIX Conf. Operating Systems style and Implementation, oct,2004.