International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 07, July 2015
www.ijarse.com

IJARSE
ISSN 2319 - 8354

ENSURING CONFIDENTIALITY, AUTHENTICATION & INTEGRITY (CIA) FOR CLOUD COMPUTING

Yogesh Doulatramani[1], Prof. Dilip Motwani[2], Prof. Rinku Shah[3]

[1]PG, Scholar, Dept. of Information Tech., [2,3]Professor, Dept. of Computers Engineering,
Vidyalankar Institute of Technology, Wadala, Mumbai, Maharastra, (India)

ABSTRACT

It has been widely observed that the concept of Cloud Computing has become one of major theory in the world of IT industry. It involves storing the user's data to be able to use the applications and services that the clouds introduce. By sending the data to be processed in the cloud, data owners transfer control of their data to a remote party that may raise security challenges. One of these risks that can attack the cloud computing is the Integrity of the data stored in the cloud and also the Privacy of that stored data on the cloud server.

The proposed model will involve the use of Third Party Broker which will encrypt the client's information for confidentiality of data and also take the hash value of the data to achieve integrity and at the same time will authenticate every cloud user. For encryption an enhanced symmetric key algorithm is designed for storing the data on the cloud and symmetric key is also securely exchanged over the Internet.

Keywords: Cloud Computing, Data Integrity, Data Encryption, Symmetric Key Cryptography, Third Party Broker.

I. INTRODUCTION

Cloud Computing gained attention since 2007. It is the general term for anything that involves providing services on internet. It moves the data and computing from desktop to large data centre's. It is combination of parallel, grid and distributed computing.

Many big companies such as IBM, Google, Amazon, Microsoft, Yahoo and other move themselves to develop Cloud Computing. These companies have launched their own Cloud Computing infrastructures and services and achieved good application results and social impact, such as Amazon's EC2 and S3, Google' Google Apps, Microsoft Azure and so on.[1]

Some of the potential benefits that apply to almost all types of cloud computing includes the following:

1. **Cost Savings:** Companies can reduce their capital expenses and use operational expenses for increasing their computing capabilities.
2. **Flexibility:** The flexibility of cloud computing allows companies to use additional resources in peak times, to enable them to satisfy consumer demands.
3. **Reliability:** Services using multi-redundant sites can support business continuity and disaster recovery.
4. **Reduce Maintenance**: Cloud service providers do the system maintenance that does not require application installations onto PCs.

5. **Mobile Accessible:** Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

1.1 Cloud Computing Service Models

The cloud service provider (CSP) offered its customers with kind of services and tools, which are:

a. **Software as a Service (SaaS):** It involves using their cloud infrastructure and cloud platforms to provide customers with software applications. In this service, the user can take advantage of all applications. The end user applications are accessed by users through a web browser, such as Microsoft SharePoint Online. The need for the user to install or maintain additional software is eliminated.

b. **Platform as a Service (PasS):** It enables customers to use the cloud infrastructure; as a service plus operating systems and server applications such as web servers. The user can control the development of web applications and other software and which use a range of programming languages and tools that are supported by the service provider.

c. **Infrastructure as a Service (IaaS):** The registered user may access to physical computing hardware; including CPU, memory, data storage and network connectivity of the service provider. IaaS enables multiple customers referred to as "multiple tenants" using virtualization software. The user gains greater flexibility in access to basic infrastructure.

1.2 Cloud Computing Components

1. Users: - Users who have data to be stored and interact with the cloud service provider (CSP) to manage their data on the cloud. They are typically, desktop computers, laptops, tablet computers, mobile phones, etc.

2. Cloud Service Provider (CSP):- Cloud service provider (CSP) has major resources and expertise in building and managing distributed cloud storage servers. A CSP offers storage or software services to user's available via the Internet.

3. Third Parity Auditor (TPA):- An optional TPA, who has expertise and capabilities that users may not have, is monitoring the risk of cloud data storage services on behalf of users.

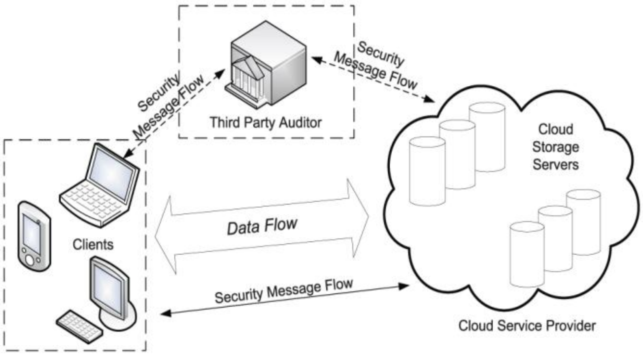


Fig. 1 Cloud Data Storage Architecture

II. RELATED WORK

Cloud Computing is still in high demand where the organizations are either already using or intending to use cloud computing infrastructure services, and the share of cloud service will continue to increase as a percentage of total revenue [2][10].

There are two types of Cryptography – Symmetric & Asymmetric Key Cryptography and out of two types, the symmetric key encryption is the fast and most commonly used compared to asymmetric key encryption. In symmetric key cryptography only one key is used for encryption and decryption and few commonly used algorithms are DES, AES, and IDEA.

Symmetric Key Cryptography technique can work as Stream Cipher or Block Cipher. In stream cipher, data is encrypted either bit by bit or byte by byte and in Block Cipher, data is encrypted block by block where each block should have minimum 64 bits of data.[3]

Syamkumar [4] rely on pre-computation of verification token using sobol sequence for ensuring cloud data security. For a random set of blocks, token is generated and stored locally. Whenever user challenges cloud service provider, it computes a signature which is verified over the tokens stored locally by users. It rely on Reed- Solomon erasure code in file distribution to guarantee the availability and reliability of data and utilize token precomputation using Sobol Sequence to check integrity of erasure coded data in cloud data storage.

Qin Liu [5] gave a scheme for Hierarchical Identity based encryption algorithm which enables higher level users to share the storage data efficiently with lower level users. The file is encrypted only using public keys of intended recipients and stored in server. Number of authorized public keys is also taken as input for encryption algorithm. At the client only store two functions, the bit generator function g, and the function h which is used for encrypting the data. Hence the storage at the client is very much minimal compared to all other schemes. Hence this scheme proves advantageous to thin clients like PDAs and mobile phones.

DalliaAttas[6] suggested in order to overcome the threat of integrity of the data, the user must be able to use the assistance of a Third Party Auditor (TPA). The TPA has an experience that a cloud user does not have and checks over the Integrity that is difficult for the users to check. The user can handout the integrity checking mission to the TPA, in such a way that the TPA will not be able to manipulate with the client data with one way or another.

SaranyaEswaran [7] suggested with the help of TPA it is easy to achieve data integrity and confidentiality goals by using encryption techniques.

Cong Wang [8][9] suggested a flexible distributed storage auditing mechanism, utilizing the homomorphic token & distributed erasure coded data. It allows the users to audit the cloud storage with very lightweight communication & computation cost and its result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization i.e. the identification of misbehaving server.

Caronni proposed another protocol [12], where the server has to send Message Authentication Code (MAC) of data as the response to the message instead of storing the hash of all data. The verifier sends unique random key for the message authentication code to achieve integrity on data from any modification or deletion. Instead of storing the whole data at server specific portions of data is stored; a deterministic verification approach issued.

III. PROPOSED SYSTEM

The Proposed system will consist of three basic components of Cloud Architecture, Cloud Broker, Clients and Cloud Storage Service Providers.

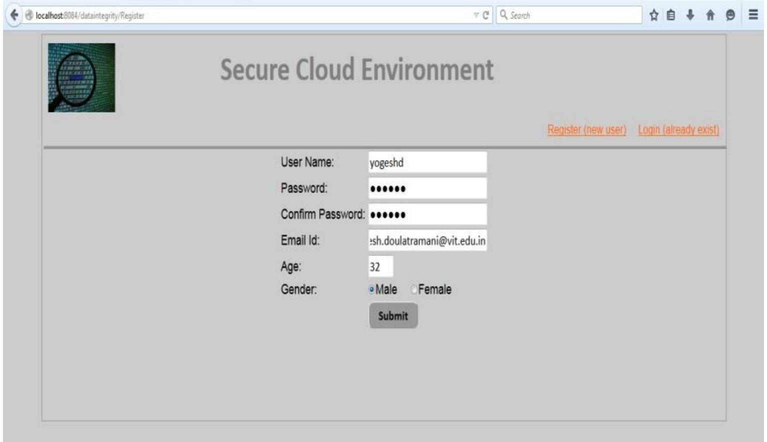
1. The Clients: Clients of the cloud may be individual customers and any organization that have data to be stored in the cloud. Clients rely on the cloud for data computation and its security maintenance. Clients mainly store encrypted data on the remote servers and to ensure security it queries the data through the TPA for Integrity Checks.

2. The Storage Servers : Servers provide significant resources and expertise in managing cloud storage servers. Servers store the client's sensitive data in encrypted form and is considered to be un-trusted entities.

3. The Cloud Broker: It acts as an interface between client and cloud storage server. Request Handling, Encryption, and Integrity Check is done at this side. Broker is considered the most important component.

3.1 Modules Used

1. Registration Module: This module will register a new user by asking the user's details like username, password, email id, age and gender and store all the details in the database.



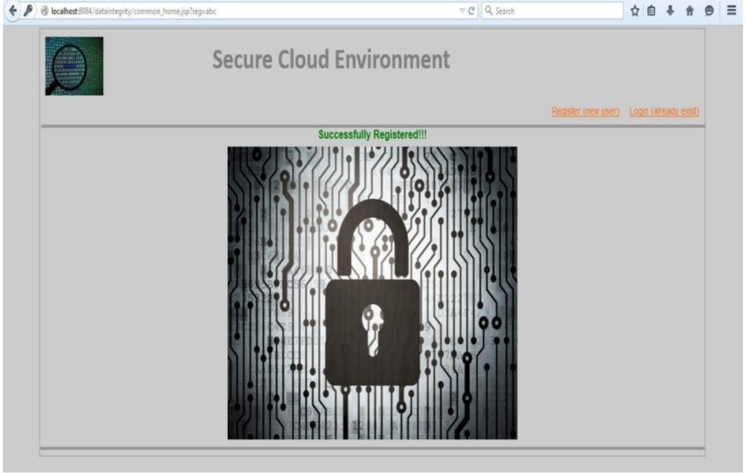
localhost:8084/dataintegrity/Register

Secure Cloud Environment

Register (new user) Login (already exist)

User Name: yogeshd
Password: ••••••
Confirm Password: ••••••
Email Id: :sh.doulatramani@vit.edu.in
Age: 32
Gender: ● Male ○ Female

Fig. 2 Registration of New User



localhost:8084/dataintegrity/common_home.jsp?reg=abc

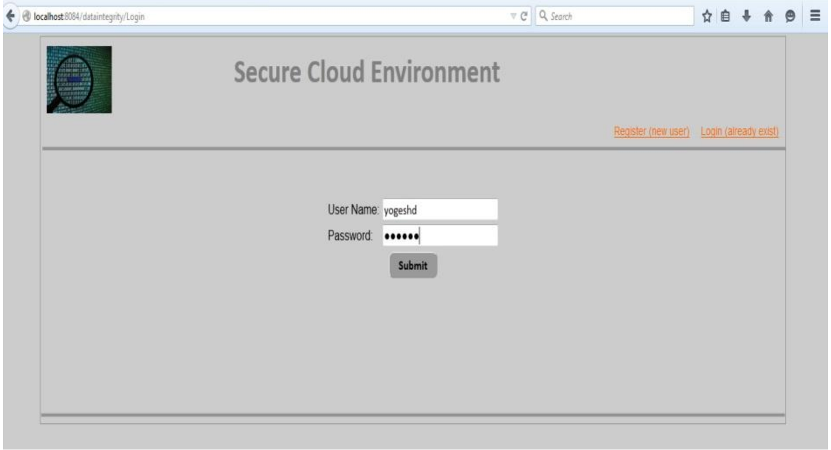
Secure Cloud Environment

Register (new user) Login (already exist)

Successfully Registered!!!

Fig. 3 New User Successfully Registered

2. Login Module: A user can click on Login link from the Home Page if already registered and then enter the username & password and if login details are verified by this module then user has successfully logged in and can see its profile page.



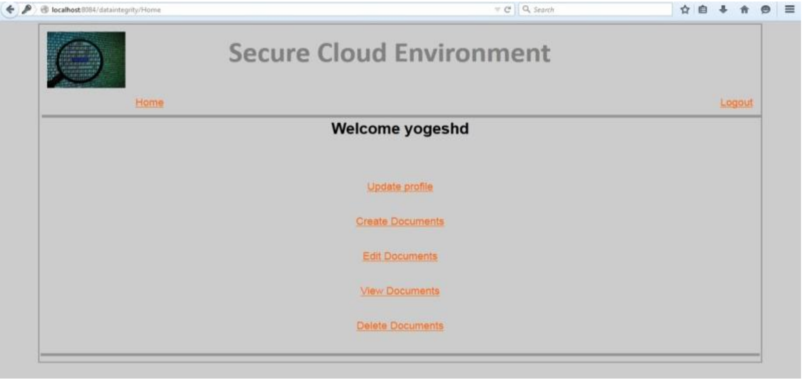
localhost:8084/dataintegrity/Login

Secure Cloud Environment

User Name: yogeshd

Password: ••••••

Fig.4 Login Page



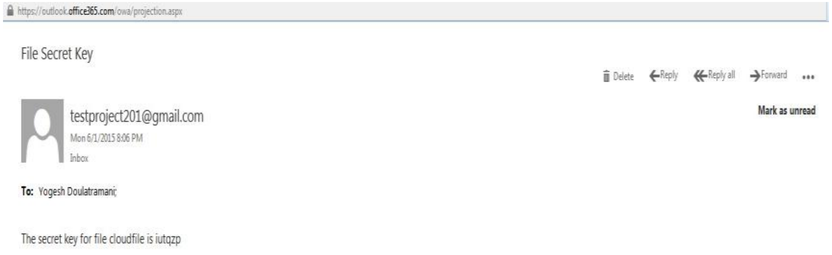
localhost:8084/dataintegrity/Home

Secure Cloud Environment

Welcome yogeshd

Fig.5 Home Page

3. Key Distribution Module: When the user will create a new file then for that created file a key will be mailed to the user by this module hence every time user will access that file has to enter the key and then access that file.



https://outlook.office365.com/owa/projection.aspx

File Secret Key

testproject201@gmail.com
Mon 6/1/2015 8:06 PM
Inbox

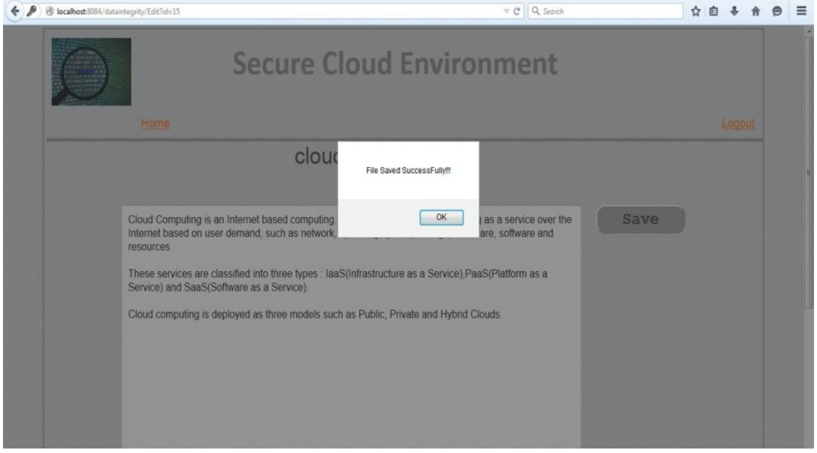
To: Yogesh Doulatramani;

The secret key for file cloudfile is iutqzp

Fig.6 Secret Key is Emailed

4. Data Encryption Module: This module will encrypt the contents of the entire file by using the symmetric key cryptography technique hence confidentiality goal can be easily achieved.

5. Document Creation Module: This module will help the user to create a new file and then while creating a new file with the help of key distribution module a key will be mailed to the user for that newly created file.



File Saved SuccessFully!!!

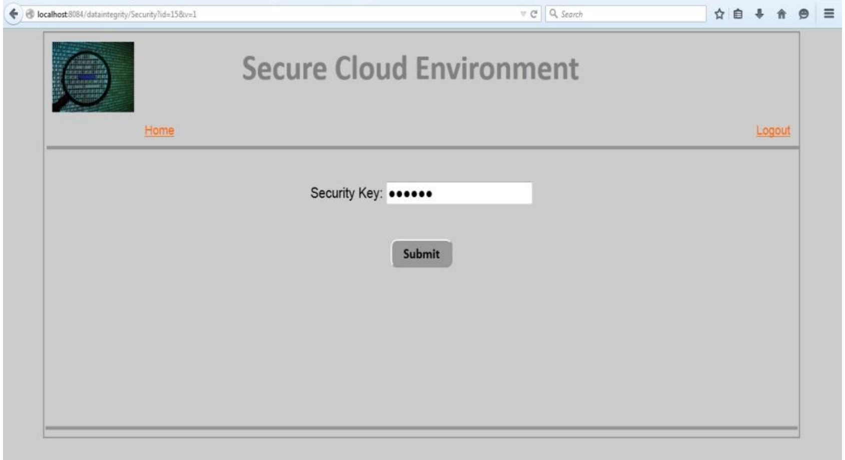
Cloud Computing is an Internet based computing. … as a service over the Internet based on user demand, such as network, … are, software and resources.

These services are classified into three types : IaaS(Infrastructure as a Service),PaaS(Platform as a Service) and SaaS(Software as a Service).

Cloud computing is deployed as three models such as Public, Private and Hybrid Clouds.

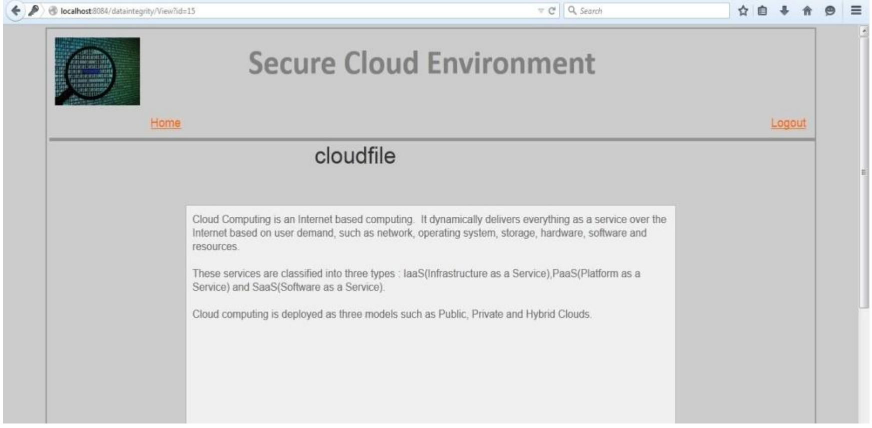
Fig.7 New File is Saved

6. Document View Module: This module will allow the user to view the contents of the file after entering the key correctly.



Security Key: ••••••

Fig.8 User Enters Security Key Received Via Email



cloudfile

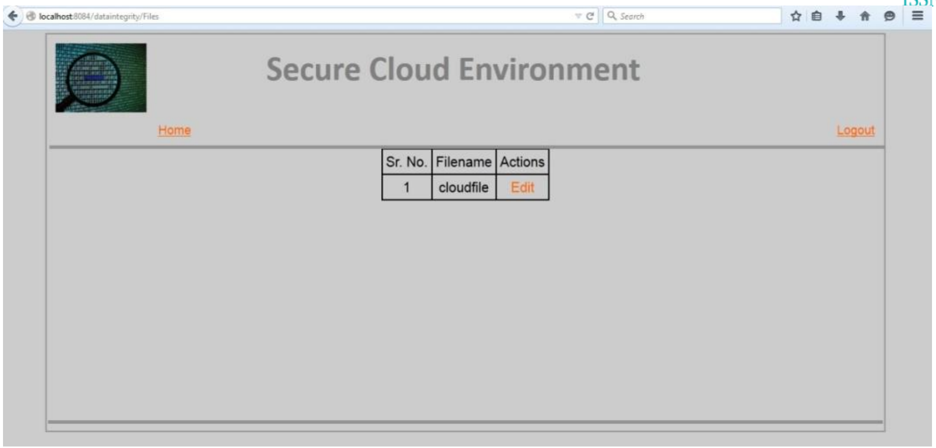
Cloud Computing is an Internet based computing. It dynamically delivers everything as a service over the Internet based on user demand, such as network, operating system, storage, hardware, software and resources.

These services are classified into three types : IaaS(Infrastructure as a Service),PaaS(Platform as a Service) and SaaS(Software as a Service).

Cloud computing is deployed as three models such as Public, Private and Hybrid Clouds.

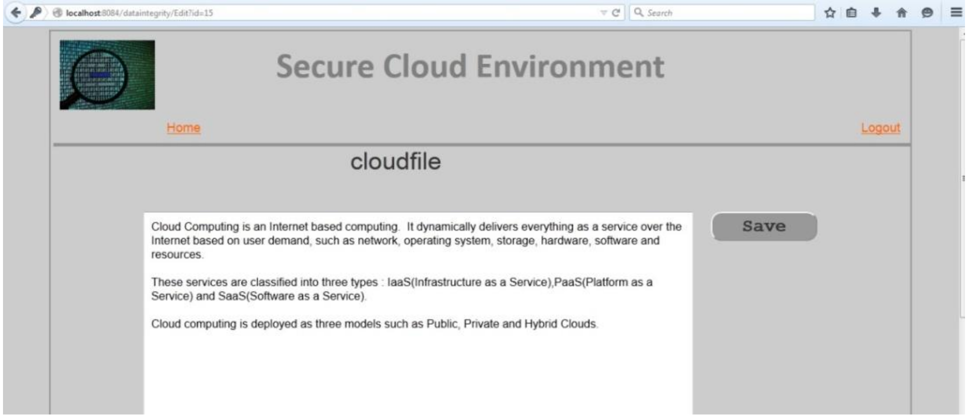
Fig.9 View the File Contents

7. Document Editing Module: This module will allow the user to add new contents, delete existing contents or modify the existing contents of a file and for this user should enter secret key.



Sr. No.	Filename	Actions
1	cloudfile	Edit

Fig.10 Edit the File



cloudfile

Cloud Computing is an Internet based computing. It dynamically delivers everything as a service over the Internet based on user demand, such as network, operating system, storage, hardware, software and resources.

These services are classified into three types : IaaS(Infrastructure as a Service),PaaS(Platform as a Service) and SaaS(Software as a Service).

Cloud computing is deployed as three models such as Public, Private and Hybrid Clouds.

Fig.11 New Contents Added

8. DataPartitioner Module: This module will partition the entire file and then the partitions of that file will be stored on the virtual machines.

9. Hashing Module: This module will help to achieve Integrity goal where the hash values of the file contents will be stored and then that hash value is always checked while retrieving the files and if its hash value is same means contents of the file is accurately stored.

10. Data Storage Module: This module will store the contents of the file on the virtual machines.

11. Data Retrieval Module: This module will help the user to retrieve the contents of the file which are stored on the virtual machines.

IV. IMPLEMENTATION

VMware Workstation transforms the way technical professionals develop, test, demonstrate and deploy software by running multiple x86-based operating systems simultaneously on the same PC. VMware Workstation takes advantage of the latest hardware to replicate server, desktop and tablet environments in a virtual machine.. No other desktop virtualization software offers the performance, reliability and cutting edge features of Workstation.

With the ability to allocate multiple processor cores, gigabytes of main memory, and graphics memory to each virtual machine, Workstation maximizes your computer’s resources to run the most demanding applications in a virtual environment. Workstation also lets you build complex virtual machines on your laptop running Cloud

Foundry, Big Data applications like a single-node Apache Hadoop cluster or 64 bit virtual machines within vSphere.

Hence this paper idea is implemented using VM Workstation where multiple Red hat Operating Systems are installed and using these operating systems the data is stored on these machines as such machines are called Virtual Machines with the help of MySql Database.

MySQL is a database system used on the web that runs on the server and it is ideal for both small and large organizations. It is very fast and easy to use.

IV. CONCLUSION

This system provides a better integrity checking with the help of the Cloud Broker with the encryption & hashing algorithms. Storage security is highly enhanced since only the encrypted data is stored at cloud sites and the client even doesn't get the whole file without the knowledge of the Database manager which is at broker side.The performances measures such as encryption time and time taken to detect corruption are reduced and shown with encryption algorithm for a cloud environment.

REFERENCES

[1] RenukaGoyal, NavjotSidhu "Third Party Auditor: An Integrity Checking Technique for Client Data Security in Cloud Computing" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4526-4530

[2] Nedhal A AL-Saiyd,Nada Sail "Data Integrity in Cloud Computing Security" Journal of Theoretical and Applied Information Technology 31st December 2013. Vol. 58 No.3

[3] Singh, S Preet and Maini, Raman. "Comparison of Data Encryption Algorithms", International Journal of computer Science and Communication, vol. 2, No. 1, January-June 2011,pp. 125-127.

[4] P.Syam Kumar, R.Subramanian and D. ThamizhSelvam, "Ensuring Data Storage Security in Cloud Computing using Sobol Sequence", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[5] Qin Liu, Guojun Wang, Jie Wu, "Efficient Sharing of Cloud Storage Services", 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010).

[6] DaliaAttas& Omar Batrafi," Efficient Integrity Checking technique for securing client data in Cloud Computing", IJECS-IJENS VOL: 11 No:05 Oct 2011.

[7] SaranyaEswaran "Identifying Data Integrity in the Cloud Storage",IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012.

[8] QiangWang,CongWang,KuiRen"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,1045-9219/11/$26.00IEEE2011

[9] CongWang,QianWang,KuiRen"Toward Secure & Dependable Storage Services in Cloud Computing,1939-1374/12/$31.00IEEE2012

[10] Cloud Computing Evolution in the Cloud Available at: http://www.pwc.de/de_DE/de/prozessoptimierung/assets/cloud_computing_2013.pdf.

[11] Velte T. A., Velte J. T. and ElsenperterR.,Cloud Computing A Practical Approach,Chapter 1: Cloud Computing Basics,McGrawHill, USA, 2010. http://www.south.cattelecom.com/Technologies/CloudComputing/0071626948_chap01.pdf.

[12] Sriram L., Khajeh-Hosseini A., Research Agenda in Cloud Technologies, 2010.