Risk Involved in Cloud Data Storage and its Safety Measures

K. Mythili
Research Scholar
SCSVMV University

S. Rajalakshmi
Professor
SCSVMV University

ABSTRACT
Cloud computing is a technology which will facilitate companies or organisation to host their services without worrying about IT infrastructure and other supporting services. Usually cloud computing services are delivered by a third party – Cloud Service Provider(CSP) provider who owns the infrastructure. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. In this paper we focus on risks involved in data storage in cloud computing and solutions to minimize the risks.

Keywords
Security; Cloud Service Provider; access control; data Server; Software License Agreement

1. INTRODUCTION
Maintaining and managing a corporate network is a difficult task when the network grows. The increasing growth increases the need for extra resources. Storage is one such resource which grows high and increases the security issues and challenges associated with it. Most of the owners prefer to invest on larger hard drives while others on external storage devices (Compact Discs, Thump drive etc.). The cloud data storage is the alternate for these storage resources and facilitates with major needs of customer.

1.1 Cloud Data Storage
Cloud Data storage is an off-site storage technique in which the data will be stored in a server. Cloud data is managed and maintained by third parties. The drawback of using external storage devices and large hard drives which are inside a private network is that, they cannot be accessed from outside the network. Cloud storage overcome these drawbacks. The data stored in cloud can be accessed anywhere in the internet irrespective of our geo-location. One of the highlighting features of cloud storage is easy expandability. Depending upon the users need it can be expanded.

1.2 Cloud Data Storage Service
A cloud storage system needs just one data server connected to the internet. The client uploads the copies of his files to server (data server) through internet. When he/she needs to access his file he can access it via a web-based interface. Depending upon the user's request, the server allows user to manipulate his file from server itself or sends it back to user.

1.3 Data Centres
The facilities that house cloud storage systems are called as data centres. The data centres are too big that it has many storage servers in it. The data on cloud is stored in data centres. The cloud storage systems focus on some specific tasks such as storing e-mail messages or digital pictures and some other files. Eg : Google Docs, Gmail, Hotmail, Youtube.

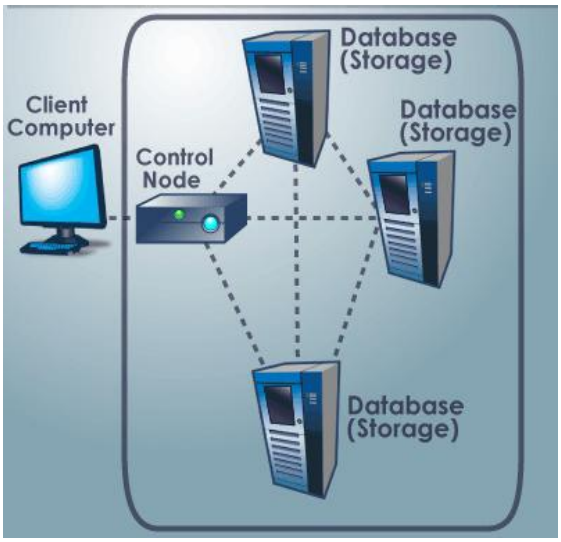

Fig.1 Cloud Storage

1.4 Concerns about Cloud Storage

1.4.1 Reliability and Security
Like all other communications cloud also provides the 3 security features.

1. Encryption
2. Authentication
3. Authorization

1.4.1.1 Encryption
The information stored is encoded using a complex algorithm. An encryption key is required to decrypt the files.

1.4.1.2 Authentication
A username and password is provided to cloud users to access his accounts/services etc. The user credentials are validated and allow the user to access the permissible services.

1.4.1.3 Authorization

Cloud maintains a list of people who are authorized to access the services. The protective measures mentioned here doesn't make a feel that data is secure in a remote storage system because it is still vulnerable to some electronic backdoors or a disgruntled employee.

1.4.1.4 Reliability

An unstable cloud storage system is always a liability. The chances are high that data may get lost any time. An unstable internet connection also questions the reliability of cloud.

2. OTHER CONCERNS ABOUT CLOUD

2.1 Loss of Governance

Customers give the control to cloud service providers on a number of issues that may impact their security, mission and goals. Cloud security suggests that business are vulnerable when they go entrust their data to a third party and many things can go wrong. The customer will not have complete control on his/her data on cloud.

2.2 Lock In

There are some situations in which the user may not be able to access any of his data or services on cloud. This makes the customer helpless if he is depending on cloud completely. Such situations are referred as Lock-In.

A Vendor lock-in is a situation in which the customer using a product or service cannot easily transit or migrate to another cloud service provider. This usually arises because of incompatibility with the competitors (Service Providers).

2.3 Contract Termination

Cloud Services are payable on usage basis. The user has to pay only for his usage. This is made using some contracts or agreements which user has to agree. All these contracts specifies a period or validity. The cloud services can be accessed through out the period where user's account is active. Once the contract gets terminated the data stored will be deleted instantly from data centers. The user has no recovery option for the deleted files. Data once lost is lost forever.

2.4 Data Migration

One of the biggest issues faced by cloud users is data migration. Most of the cloud service provider does not support the feature of data migration. The user who's willing to change the service provider will not be able to do that directly from one service provider to another service provider. The user will have to download all his data to a local storage to migrate it to a different service provider.

2.5 Interoperability

Most of the service providers doesn't have this feature. The data generated in by a particular server may or may not be working in another server.

2.6 Management Interface Vulnerability

Management interface vulnerabilities can also lead to hijacking of account.

2.6.1 Malicious Insider

A malicious insider is as harmful as a hacker outside the network.

3. MITIGATION PLANS

1. Looking at risk factor
2. Managing Resource Centrally
3. Patching & Updating
4. Negotiating SLA

3.1 Looking For Risk Factor

This can help to identify the risk which are faced by user while using clouds.

3.2 Managing Resource Centrally

This will help the user as well as a corporate employee in accessing the resources anywhere from the world.

3.3 Patching and Updating

Once a vulnerability is identified a patch for the same is made and issued as an update for the cloud servers.

3.4 Negotiating SLA

Negotiating Software License Agreement can help a user to have extra features and other benefits. A user can use SLA to compare the companies. By this comparison either he can negotiate with his current service provider or can migrate to other.

4. PROPOSED SCHEME

we propose three schemes for Data availability, correctness and also for reliability.

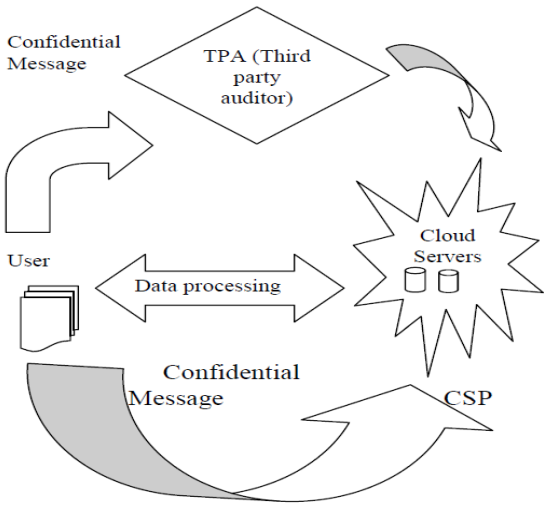

Fig.2 Cloud Architecture and Data Processing Way

To reduce the work load of the user, TPA has the delegation for the data checking with a few limitation so that he can't modify content of the data in his auditing. And TPA pays due care on storage correctness verification.TPA auditing is in the manner of privacy preserving concept so that verification can be done in separate manner alone from any interaction by others.

4.1 Server Access Point

To keep the data away from server failure in every data inclusion by unauthorized person or any internal and external attack coming within CSP address domain, one access point or restore point in every update is given to the cloud server when client does some delete, modification, and append in his will. It is done in the time of data comparison in every update for the data by user with the help of CSP.

4.2 Data Log

A log file is created and indexed on access time. This log file contains index along with new version of data file. Therefore whenever the data is accessed from the server, this log file has the index for new version of customer file access with its modifications, so that the customer can able to track of information about the data modification along with date and time. Since the cloud data can be accessible to multiuser, this log file keeps track of which user made an attempt of data modification with the respective version.

5. BENEFITS

TPA auditing is in the manner of privacy preserving concept for the verification of data availability. With the access point or restore point the data can be protected from unauthorised users. Data log maintains the data file versions along with time information as index**.**

6. CONCLUSION

"Cloud" computing builds on decades of research in virtualization, distributed computing, utility computing, and, more recently, networking, web and software services. It implies a service-oriented architecture, reduced information technology overhead for the end-user, great flexibility, reduced total cost of ownership, on demand services and many other things. This paper identifies the risk involved in cloud data storage and focussed on three methods to handle the risk and hence we obtained the features like of storage like data availability, reliability and correctness.

7. FUTURE ENHANCEMENT

Here we leave more ways as Future enhancement to process for maintaining security and reliability of data using TPA and access point, so that user can identify inserting the attempt of different data having same weight in un-trusted cloud server. In our future study we also have planned to implement the security measure of cloud data storage with the help of CSP for data update.

8. REFERENCES

[1] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE Transactions on services computation vol. 5, no. 2, April-June 2012.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009.

[3] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.

[4] Sun Microsystems, Inc., "Building Customer Trust in Cloud Computing with Transparent Security," https://www.sun.com/offers/details/sun_transparency.xml, Nov. 2009.

[5] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[6] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[9] Cloud_Security_Alliance (2009, April). "Security Guidance forCritical Areas of Focus in Cloud Computing." Retrieved Nov 25, 2009, from http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

[10] Addressing Cloud Computing Security Issues, Future generation computer systems (2011) www.elsevier.com/locate/fgcs.