Secure And Disseminate Cloud Data Over A Mobile

Kirti Dongre
M.E.(Student)
G.H.Raisoni College of Engineering,Nagur

Prof. Jagruti Shah
Asst.Professor
G.H.Raisoni College of Engineering,Nagpur

Abstract

Cloud computing is one of the emerging technologies that will lead to the next generation of Internet. Cloud computing is a way of computing, via the Internet, that broadly shares computer resources instead of using software or storage on a local PC. Cloud computing is an outgrowth of the ease-of access to remote computing sites provided by the Internet. Cloud computing platforms provide easy access to a company's high-performance computing and storage infrastructure through web services. Cloud computing is emerging as one of the most important branch for providing seamless applications on mobile devices. In this paper we design an archive mechanism that integrates cloud storage, hybrid cryptography, and digital signatures to provide security requirements for data storage of mobile phones. Our mechanism not only can avoid malicious attackers from illegal access but also can share desired information with targeted friends by distinct access rights.

1. Introduction

Clouds are a very new and popular topic in the field of IT. [2] Though this is not a new technology, it is a new concept: main purpose of the original cloud is that "users can use the service anytime, anywhere through the Internet, directly through the browser."

Cloud computing is an internet based computing where virtual shared servers [8] provide software, infrastructure, platform, and other resources and hosting them to customers on a pay-as-you-use basis.

It is a virtualized resource where we want to store all our data with security measurement so that some application and software can get full benefits using this technology without any local hard disk and server for our data storage.

There are various definitions for "The Cloud", although cloud computing is generally considered as follows.

"Clouded computing is the delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices as a utility over a network."

Clouds need security too, but they are a new concept, so no safety standard has actually been developed; each company is developing its standards .Data security issues include data stored in a server; servers can be accessed through browsers to obtain internal information. If a hacker attacks many servers to steal information, data stored in the server's security is a concern. Management reliability refers to cloud security mechanisms to prevent security breaches. Protecting user privacy in clouds is the most important issue in the industry.

Mobile phones have become an integral part of life; mobile users store personal data on phones, such as contact lists, text messages, photos, and programs. Smart phones can perform many of the programs detailed above. Business owners keep schedules in the phone; although the information may not be important to other mobile users, it is important to the owner of the phone. If the phone is lost or damaged, or phone numbers are changed, the issue comes up of what to do with the data stored in the phone.

2. Previous Related Work

In previous methods, mobile users would backup data inside a computer; in the event of data loss, they would retrieve the data from the computer and place it back into the phone memory. [1] The same procedure would apply when phones are changed. Thus, the data are backed up despite actions, but this procedure is not very convenient: there is no means to update the data in real time. Remote backup is convenient to business owners; by referring to the phone number, they can plan their schedules [3] and save important documents, which many people may find too complicated to back up on a computer. Moreover, if a phone is damaged or suddenly no longer working, there is no way to get data from other places. Clouds have to be accessible over the network.

Mobile users generate a random number that is passed along to telecommunication. The telecommunication [2] returns random values to verify the transmission of the user registration information. The transmission process uses the hash function to verify whether the transmission was tampered with. If any tampering is found, the transmission is not performed. Trust is important

among mobile users, telecommunication, and clouds, so the method generates a secret value that is only known to the three parties. If any party receives a message with no secret value, then no action is performed [4]. Not a great deal of mobile user information is saved to prevent collusion attacks. In the telecommunication database, storage of personal data is encrypted, which also prevents attacks and internal staff theft. In each phase, encryption is done asymmetrically. The use of encryption methods, digital signature, hash function, random number, and secret value is to let users have peace of mind in a cloud environment.

3. Cloud Storage

Now days, cloud computing is everywhere. But the only problem is that not everyone agrees on what it is. [5] A cloud storage system provides storage as a service to users through a unified interface. Users can easily access the large storage infrastructure.

The storage service can be used at any time on a pay as you on basis. When the service is no longer needed they can be released freely.

Cloud storage is amorphous today, with neither a clearly defined set of capabilities nor any single architecture. [7] Choices abound, with many traditional hosted or managed service providers (MSP) offering block or file storage, usually alongside traditional remote access protocols or virtual or physical server hosting. Other solutions have emerged, typified by the Amazon S3 service, that resembles flat databases designed to store large objects.

At its most basic level, a cloud storage system needs just one data server connected to the Internet. A client (e.g., a computer user subscribing to a cloud storage service) sends copies of files over the Internet to the data server, which then records the information. When the client wishes to retrieve the information, he or she accesses the data server through a Web-based interface. The server then either sends the files back to the client or allows the client to access and manipulate the files on the server itself.

4. Cloud Architecture

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.

In this all outsourced data and data entering into the cloud is measured using reading protocol algorithm. [8] So to keep integrity of overall data we have data reading protocol from user as well as cloud storage level before and after the data adding into the cloud server area and another multi-server data comparison algorithm for every data upload for the purpose of data recovery management.

A cloud storage system provides storages as a service to users through a unified interface. Users can easily access the large storage infrastructure. The storage service can be used at any time on a pay as you go basis. When service is no longer needed they can be released freely.

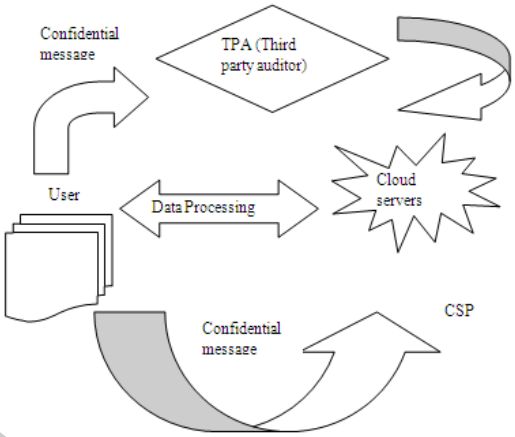

Fig (a) Cloud Architecture and Data Processing Way.

5. Conclusion

In this paper we have study the previous work which is done. Cloud Storage with a great deal of promise, aren't designed to be high performing file systems but rather extremely scalable, easy to manage storage systems.

6. References

[1] Cong Wang, Ning Cao, Kui Ren and Wenjing Lou."Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data." IEEE transactions on parallel and dirtibuted system, 2012.

[2] Sue-Chen Hsueh,Jing-Yan Lin and Ming-Yen Lin "Secure Cloud Storage For Convenient Data Archive of Smart Phones" ,IEEE 15th intenational Symposium on Consumer Electronics, 2011.

[3] Claudio E. Palazzi, Macro Ferrarese FTP4Android: A Local/Remote File Manager for Google Android Platform, 3rd IEEE International Workshop on Digital Entertaintment, networked Virtual Enviroments and Creative Technology, 2011.

[4] Wei Tang, Jun-hyung Lee, Biao Song, Md. Motaharul Islam, Sangho Na and Eui-Nam Huh "Multi-Platform Mobile Thin Client Architecture in Cloud Environment" publish by Elsevier Ltd. Selection and /or peer – rebview under responsibility of the Intelligent Information Technology Application Research Association, 2011.

[5] Rimal, B.P., Eunmi Choi and Lumb, I. "A Taxonomy and Survey of Cloud Computing Systems". International Joint Conference on INC, IMS and IDC, Seoul, pages 44-51. Aug, 2009.

[6] Dinesh C "Data Integrity and dynamic storage way in cloud computing" 2011.

[7] Yanmei Huo, Hongyuan Wang Liang hu, Hongji Yang "A Cloud storage architecture model for data intensive applications" ,2011.

[8] Dinesh C, Prasnna S "Efficient data integrity and reliable storage accesses in cloud using space comparison algorithm" International journal of Computer Applications ,October 201