Secure Data Storage of Mobile Phones on Cloud

Nilesh Khonde , Swapnil Bawankar, Lokesh Ashtankar, Anand Dharamthok , Khaire P. A.

Abstract- The *objectives of our paper are to provide more security to our mobile data stored in the cloud. Cloud computing is one of the promising technologies that will guide to the next invention of Internet. The significance of the data stored in the smart phones is enlarged as more applications are deployed and executed. Once the smart phone is broken or lost, the priceless information treasured in the device is lost altogether. Cloud computing is a mode of computing via the Internet, that broadly shares computer resources instead of using software or storage on a local PC. If cloud storage can be incorporated with cloud services for periodical data backup of a mobile client, the danger of data lost can be minimized. However, the important data might be uncovered by a malicious third party during retrieval or transmission of information using wireless cloud storage without proper authentication and protection Cloud computing is a result of the user-friendliness to isolated computing sites provided by the Internet. Cloud computing is rising the most significant branch for providing textbook applications on mobile devices. In this paper we plan a library mechanism that integrates cloud storage, cryptography authentication to provide safety necessities 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.*

Index Terms— **App42 cloud, mobile device, certificate authority, Telecommunication.**

I. Introduction

Clouds [1] are a very new and popular topic in the field of computer science. Though this is old technology, it is a new concept: main purpose of the original cloud is that “this services provided by cloud computing can be used by user at 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.

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

“Clouded computing is defined as the general term for delivering the hosted service rather than product to the user over the internet”

It is a virtualized resource where we want to store all our data with security dimension so that some application and

software can get full benefits using this technology without any local hard disk and server for our data storage.

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 consist of data stored in a server; servers can be accessed to obtain internal information. Hacker attacks many servers to steal information; data stored in the server’s security is a concern. Management dependability refers to cloud security mechanisms to avoid security breaches. Protecting user confidentiality in clouds is the most important concern in the industry. Mobile phones have become an essential 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 maintain 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] [5].

Simply by using clouds, users can store personal data and back up actions. The cloud can also be used simply for personal data management and real-time updates. It can be used anytime and anywhere by users with mobile phones a carrier. The biggest issue with mobile users keeping personal data in the cloud is security of the personal data. In this study, a method was developed by which mobile users register and share in a stage through the certification center to verify the signature of legitimate sources. Mobile users generate a random number that is passed along to telecommunication. The telecommunication returns random values to verify the transmission of the user registration information. The transmission process uses the hash function to prove whether the transmission was tampered with. If any tampering is found, the transmission is not performed. Faith 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. Not a great agreement 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 user trim peace of mind in a cloud environment.

II. Related work

In earlier, mobile users would backing data within a computer; in the occurrence of data loss, they would recover the data from the computer and leave it back into the phone memory.[3] The same method would apply when phones are misrepresented. Thus, the statistics are backed up regardless of actions, but this process is not very handy: there is no way to bring up to date the data in real time. Distant backing is suitable to business owners; by referring to the phone number, they can plan their schedules [7] and save important documents, which a lot of people may find too complicated to back up on a computer. Moreover, if a phone is damaged or suddenly no longer functioning, there is no manner to obtain data from additional places. Clouds have to be easy to get to over the network.

Mobile users produce an accidental number that is passed along to telecommunication. The telecommunication [4] returns random values to validate the transmission of the user registration information. The communication process uses the hash function to make sure whether the transmission was tampered with. If any tampering or unauthorized action 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 [10]. 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 at tacks 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. With respect to functionality, App42 is intentionally built with a minimal aspect set. It has the following features. (1) Write, read, and delete objects containing 1 byte to 5 terabytes of data each; the number of objects that can be stored is unlimited. (2) Each object is stored in a bucket and retrieved via a unique developer assigned key. (3) A bucket can be stored in one of several regions. The user chooses a region to optimize latency, minimize costs, or address regulatory requirements.

(4)Objects stored in a region never leave the region unless transferred out by the user.(5) Authentication mechanisms are provided to ensure that data are kept secure from unauthorized access. Objects can be made private or public, and rights can be granted to specific users. (6) It has flexibility so that a protocol or functional layers can be added easily. The default download protocol is HTTP. A Bit Torrent™ protocol interface is provided to lower costs for high-scale distribution. (7) app42 is reliable and is backed with the cloud Service.

III. Proposed plan

Data storage in the cloud is considered so that users can use mobile phones as a platform to upload, download, share, and synchronize information through cloud computing anywhere at any time. Security uses a Combination of TPM chips in the mobile phones to defend the uniqueness of mobile users as well as security skill to keep data transmissions from malicious attacks and tampering for data integrity.

For registration, synchronization, and sharing, the characteristic of mobile users is also protected through third-party certification. A certification center confirms the source of a signature; the user must confirm the legitimacy of the source operation. After legal user authentication, the center allows data transmission to the destination.

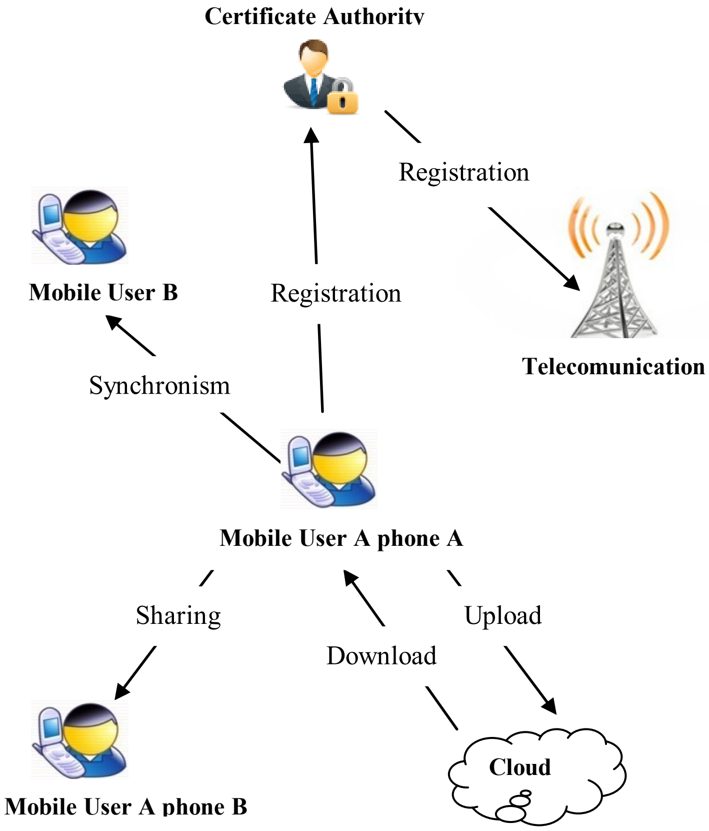

Figure1. Framework

Method

For mobile users to use the cloud, the procedure can be separated into five steps: registration, upload, download, sync, and sharing.

Table

User Type	Accessibility
Mobile User	Upload, download, sharing and synchronization
Certificate Authority	Authentication Source
Telecommunication	Generated cloud password,Store user information action
Cloud	Storage mobile user personal data

Registration

Step 1: Mobile users send information to the authentication center.

Step 2: Certification center receives information that is passed to telecommunication.

Step 3: Telecommunication receives registration information to generate a Cloud Service Password.

Step 4: Authentication center switches to pass on to the mobile user:

Step 5: Action to complete the registration the user receives the message including Mobile User, Phone Number and Cloud Service Password.

Step 6: Stored in phone memory.

Upload

Step 1: Mobile user uploads data.

Download

Step 1: Mobile users send download information including Cloud Service Password, Mobile users and Hash function.

Step 2: Return the user's personal data, hash to the cloud.

Synchronism

Step 1: Mobile user uses phone A to upload data.

Step 2: Mobile user uses phone B to access the cloud.

Step 3: Cloud passes a message to telecommunication.

Step 4: Telecommunication passes Cloud Server Password to mobile user.

Step 5: Mobile user receives the Cloud Server Password and stores the Cloud Server Password, Mobile users and Hash Function in the phone B memory, and accesses the cloud again.

Step 6: Allow access to cloud and the cloud checks the Cloud Server Password.

Sharing

Step 1: Requirements of mobile user B to share data.

Step 2: Certificate Authority (CA) verifies the signature.

Step 3: Mobile user A authenticates mobile user B.

Step 4: Transmission of intact certification center.

Step 5: Mobile user B to access cloud.

IV. Security Analysis

In this section, three aspects to the narrative are discussed: conspiracy, not credible, and attacks.

Conspiracy: A conspiracy between enterprises in order to earn more interest would violate the moral conscience. A member of the database may sell information to other companies to earn fees. Collusion between two companies may occur: the members leak information and jointly deceive users, who are unaware of what is happening. To prevent this, in the proposed method, the authentication center, telecommunication, and cloud do not store too much personal information. Instead, the information is stored in the enterprise and encryption technology is used for cipher text, which lets businesses transmit information only to real members, as all cipher text is protected.

Not credible: Irrespective of the circumstances, when a message or mail is received, the credibility of the source will be doubted with a security breach. In the method, acetified center is used to confirm the identity of the source in addition to multi-layer protection as well as achieve non-repudiation. Digital signature technology can confirm the identity. This way, only digital signatures from the sender using the receiver's public key can be used to open a message. Without the sender's private key, the message cannot be opened.

Attack: In the Internet, users can be attacked everywhere. As long as the Internet is accessed to send a message, the message transmission is subject to attack. In the method, the existence of personal data in the cloud must be through the Internet. An attacker may be present, but in this method, the transmission is encrypted asymmetrically. The transfer also includes one-way hash functions that are encrypted and cannot be decrypted by only an action without verification.

V. Conclusion

In the study, we used some very simple security technology. During transmission, each character is acknowledged by using the hash function to determine whether the transfer was deliberately tampered with during the process. Communication between mobile users uses a random number, so that parties can be recognized. A message for mobile users is verified by a trusted third party certificate authority. Messages can be transmitted with more layers of protection. If a user does not admit to sending or receiving messages, the recovery of information can be checked at the certification center. The digital signature can also be used to recognize legal status. In each role, data are not stored to the database, as internal staff may take it for illegal purposes. Not storing the data also reduces the opportunities for internal attackers. To handle external attackers, the encryption method is asymmetric. Personal data are stored into the clouds so that the text is stored in secret with the hash function used for validation. A disposable lost session key is encrypted into the cloud. This is different for every upload, so it is difficult for an attacker to break.

VI. REFERENCES

[1] www.priv.gc.ca,“Introduction to Cloud Computing”.

[2] K.Dongre , J.Shah “Secure And Disseminate Cloud Data Over A Mobile”, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 10, December- 2012.

[3] C. Y. 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.

[4] Nuno Santos, Krishna P. Gummadi, Rodrigo Rodrigues, “Towards Trusted Cloud Computing”, International Conference on Hot topics in cloud computing, pages 3-3, 2009.

[5] D.G.Devi, P.Subha “Formal Secure Outsourcing of Linear Programming in Cloud Computing” International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[6] Preeti Garg, V.Sharma, “Secure Data Storage in Mobile Cloud Computing” International Journal of scientific & Engineering Research ,volume4,issue 4,april 2013.

[7] Grossman, R.L., “The Case for Cloud Computing”, International Conference on IT Professional, page 23-27, March-April, 2009.

[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

[9] Simple Storage Service: http://api.shephertz.com/

[10] App42 for Developers: http://api.shephertz.com/app42-dev.php