Secure Cloud Storage of Data

Kirti A. Dongre
Department of Information Technology
Rajiv Gandhi College of Engineering and Research
Nagpur, India.
kadongre30@gmail.com

Roshan Singh Thakur
Department of Computer Science and Engineering
Dr. Babasaheb Ambedkar College of Engineering and Research,
Nagpur,India.

Allan Abraham
Department of Electronics
Tulsiramji Gaikwad-Patil College of Engineering and Technology
Nagpur, India

Abstract— **Cloud computing is one of the upcoming technologies that will upgrade generation of Internet. The data stored in the smart phones is increased as more applications are deployed and executed. If the phone is damaged or lost then the information stored in it gets lost. If the cloud storage can be integrated for regular data backup of a mobile user so that the risk of data lost can be minimized. The user can stored data in the server and retrieve them at anytime and from anywhere. The data might be uncovered by attack during the retrieval or transmission of data using wireless cloud storage without proper authentication and protection. So to avoid this in this paper we design a mechanism that provides a security requirement for data storage of mobile phones.**

Keywords- Cloud storage, encryption,SQL.

I. INTRODUCTION

Mobile devices are essential part of human life as the most important effective and convenient communication tool. The increase progress of mobile computing (MC) [1] becomes a powerful trend in the development of IT technology as well as commerce and industry fields. "Clouded computing is the delivery of computing as a service rather than a product, where they shared resources, software and information provided to computers and other devices as a utility over a network."

Security also needed as the technology grows so cloud need security too. Each company is developing its own standards for data security in the cloud. Data security includes data stored in the server and servers can be accessed the data through browsers to get information from server. Protecting user privacy in clouds is the most important issue in the industry.

Protecting user data in the clouds is the most important issue for the industry. If the cloud industry boasts of its own security mechanism as being safe and it is then broken, clouds will no longer be trusted by users [5]. Clouds have the feature of enabling user access anywhere at any time. Clouds do not need to understand the underlying structure; the user only needs browsers connected to the network for the required data.

Mobile phones most important 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 their important schedules in the phone [2]. If the phone is lost or damaged, the issue comes up of what to do with the data stored in the phone.

Mobile users can keep data backup inside a computer; in the event of data loss and they would retrieve the data from the computer and place it back into the phone memory. 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 [3]. Data backup is convenient to business owners; by referring to the phone number, they can plan their schedules and save important documents, which many people may find too complicated to back up on a computer. If a phone is damaged or suddenly no longer working, there is no way to get data from other places accessible data from the cloud by using network.

II. CLOUD STORAGE

Basically, a cloud storage system can be considered to be a network of distributed data centers which typically uses cloud computing technologies like virtualization, and offers some kind of interface for storing data. To increase the availability of the data, it may be redundantly stored at different locations..

Current condition is that cloud computing is using everywhere. But the only problem is that not everyone agrees on what it is. [4] A cloud storage system provides storage as a service to users through a unified interface. Users can easily access the large storage data from the cloud server.

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

Many cloud storage providers are active on the market, offering various kinds of services to their customers. This study distinguishes between two types of cloud storage services: Basic cloud storage services are generally not designed to be accessed directly by users but rather incorporated into custom software using application programming interfaces" (API). Examples of such basic cloud storage services are AmazonS34, Rackspace5 and Nirvanix6.

Advanced cloud storage services mostly employ basic cloud storage services for the actual storage of data, and provide

[978-1-4799-2352-6/14/$31.00 ©2014 IEEE]

interfaces such as client or web applications which greatly simplify the use of the service for the customer. Many services may also provide an easy to use API to allow integration of the service's capabilities into third-party software.

III. PROPSED METHOD

Data storage in the cloud is designed so that users can use to upload , download, synchronze information through cloud computimg anywhere at any time by using mobile phone. For uploading, downloading and synchronization the identity of mobile users is also protected by authentication. After the legal user authentication the token key is generated. The token key is used for the security purpose. After every login of the individual user a new token key is genereated.

Data in the server is encrypted, but keys are not revealed to the cloud. The keys are stored by the organization that "outsources" its application and user data to the cloud. To get data from the cloud server, the user first contacts to the organization to get the appropriate key(s), and then sends requested the query to the cloud to fetch the data from the server. The input parameters to the query are also sent in encrypted form. The cloud executes the query using this encrypted input and then sends back the results, also in encrypted form. Then, the user's device decrypts the data and displays it.

As shown in Fig 3.1, mobile users use mobile phones to access the Internet and then send registration information to the authentication center, which is subsequently passed on to the signature telecommunication. The telecommunication sends a cloud password back to the mobile user to complete the registration operation. Mobile users then use the password to upload and download the data in the cloud. To share the data from the cloud data storage can also be synchronized with other mobile phones and shared with friends.

Implementing database labeling and key assignments. All the applications that we used for our evaluation use MySQL as their back-end database. We implemented labeling in a MySQL-proxy between the database and the PHP Runtime. For each of these applications, we used the following setup. We 1) create a database with the exact same schema used in the application, 2) insert sample data into the database to create a training database for labeling, 3) identify all SELECT queries in the application that read data from the database, 4) perform database labeling on SELECT queries in the applications, and finally 5) analyze the labels attached to the cells to verify the data classification and key assignment performed by our techniques.

In mobile device, users store and retrieve (encrypted) data that are stored on the cloud, and user can obtain their encrypted keys from the organization. The critical job is to protect decrypted data and user keys. Desktop applications can protect keys locally using standard techniques. For example, by storing and isolating the keys on disk with permissions given only to the user that represents the organization. However, we need an approach to provide similar isolation properties in web applications, where data, code and keys are combined in the same browser [7].

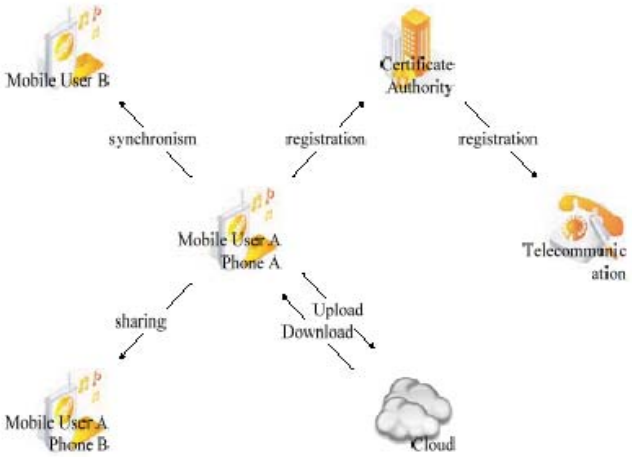


Fig 3.1. The Framework

IV. SYSTEM COMPONENTS AND IMPLEMENTATION

A. Definition

Cloud Computing can be defined as a model for enabling convenient, on-demand network access to a shared pool of dynamically scalable, and often abstracted, computing resources. Though the basic concept of this form of computing may not be groundbreaking, its re-emergence since 2008 has introduced new possibilities to satisfy a nearly insatiable need for computing power and memory [1]. For example, a Cloud deployment model can offer users and developers the option of utilizing multiple servers or storage devices that appear as one logical resource. This dramatically increases the amount of physical drive space and sheer computing power available without the need to invest in a local hardware infrastructure. Solving larger and more complex problems in shorter amounts of time, while spending ultimately less money to do so, is a possibility that has greatly piqued the interest of international corporations and government agencies alike.

B. Service-oriented cloud computing architecture.

A cloud computing is a large-scale distributed network system which is implemented on a number of servers in data centers. The cloud services are classified based on a layer (Fig. 4.1). In the first layers of this paradigm, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are stacked.

- Data centers layer: It provides the hardware facility and infrastructure for clouds. In this layer, a number of servers are linked with high-speed networks which provide services for users. Data centers are built in less populated places, with high power supply stability and a low risk of disaster.

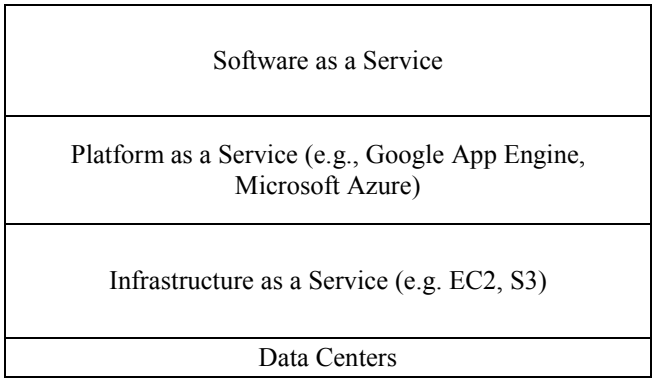


Fig 4.1 Service-oriented cloud computing architecture.

- Infrastructure as a Service (IaaS): IaaS is on top of the data center layer. It gives provision of storage, servers, hardware and networking components. The users pay on a basis they use. Thus, clients can save cost as the payment is only based on how much resource they really use. Infrastructure can be expanded or shrunk dynamically as needed. The examples of IaaS are Amazon EC2 (Elastic Cloud Computing) and S3 (Simple Storage Service).

- Platform as a Service (PaaS): It gives the capability to deploy consumer-created or acquired applications using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and, possibly, application hosting environment configurations.

- Software as a Service (SaaS): It has capability to use applications supplied by the service provider in a cloud infrastructure. The all applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

The cloud computing architecture can be divided into four layers as shown in Fig.4.1, it does not mean that the top layer must be built on the layer directly below it [2] . For example, the SaaS application can be deployed directly on IaaS, instead of PaaS. Some services can be considered as a part of more than one layer. For example, data storage service can be viewed as either in IaaS or PaaS. Given this architectural model, the users can use the services flexibly and efficiently.

V. METHODOLOGY

The proposed business model separates data storage service from that of encryption and decryption service. The separation is as visualized in fig. 5.1. Storage service is provided by one cloud service provider and encryption/decryption service is provided by another service provider.

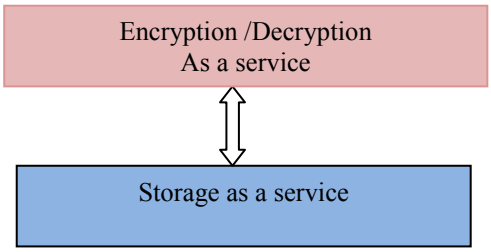


Fig 5.1: Encryption/Decryption as an independent service

This separation is required as the cloud server administrators might have illegal access to data of the users. To prevent this, the services such as storage and encryption/decryption are separated and moved to different cloud servers. Generally users use cloud environment for specific purposes. For instances SAP's ERP services [1], Salesforce.com's CRM service and so on. The data generated by these operations is saved to cloud storage. However, this study advocates an additional cloud server that takes care of encryption/decryption activities which are independent of storage service. This split responsibilities of both the servers have division of labor in functioning that provides more secure to user's data.

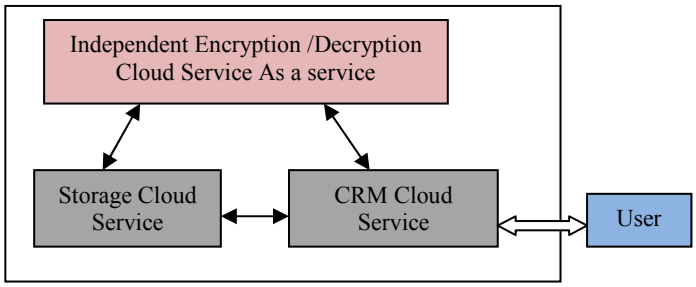


Fig. 5.2 –Proposed Business Model for storing user's data in cloud.

As can be seen in fig. 5.2, user CRM service is taken to demonstrate the new business model. As per this model users interact with CRM cloud service. In turn the CRM service interacts with both storage could service and also encryption/decryption cloud service. The interaction among them is bidirectional. The storage cloud service and encryption/decryption service and CRM service are having bi-directional communication among them.

First of all user's credentials are authenticated by CRM cloud service. Once authentication is done user can

access CRM server through which he performs data retrieval and data storage operations.

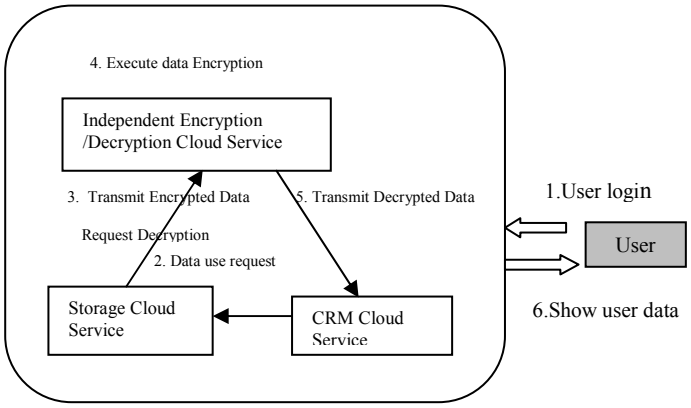


Fig. 5. 3 –Data retrieval mechanism in the proposed business model.

Fig. 5.3 shows data retrieval operation in detail. As per the user's instructions the CRM cloud service interacts with storage cloud service and makes data usage request [5]. Then the storage cloud service sends encrypted data which is available in to encryption/decryption service and requests for decryption. The encryption/decryption service takes encrypted data and simply decrypts it and sends the decrypted data to CRM cloud service. SSL (Secure Sockets Layer) is used for encryption and decryption purposes [6]. The last step is that the CRM cloud service sends requested data to end user. Thus secure communication is taking place across all components as part of proposed data retrieval mechanism.

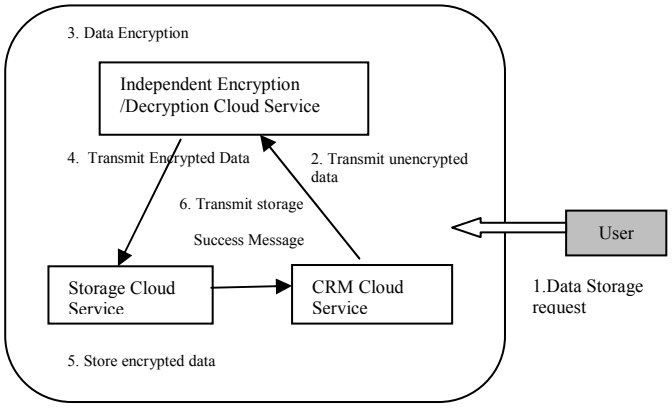


Fig. 5.4 – Data storage mechanism in the proposed business model.

As can be seen in fig. 5.4, after due authentication, the end users sends data storage request to CRM cloud service. In turn the CRM cloud service sends unencrypted data to encryption/decryption cloud service. The encryption/decryption cloud service actually encrypts the given content and sends it to storage cloud service where it is stored. Then the storage cloud service sends resultant message to CRM cloud service.

VI. CONCLUSION

During transmission of data in the cloud server , each character is recognized by using the token to determine whether the transfer was deliberately tampered with during the process. The communication between mobile users can be recognized by the unique token which is generated after login by the user. The data storage is taken place at one cloud server while the security mechanisms are applied at another cloud server. This ensures the transparency in storage and retrieval. When user sends data to cloud service provider, he has to send it as plain text to encryption/decryption service provider. Then the encryption/decryption service provider encrypts data and sends it to another service provider who is responsible for storage. Thus a secure storage of data is ensured.

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.

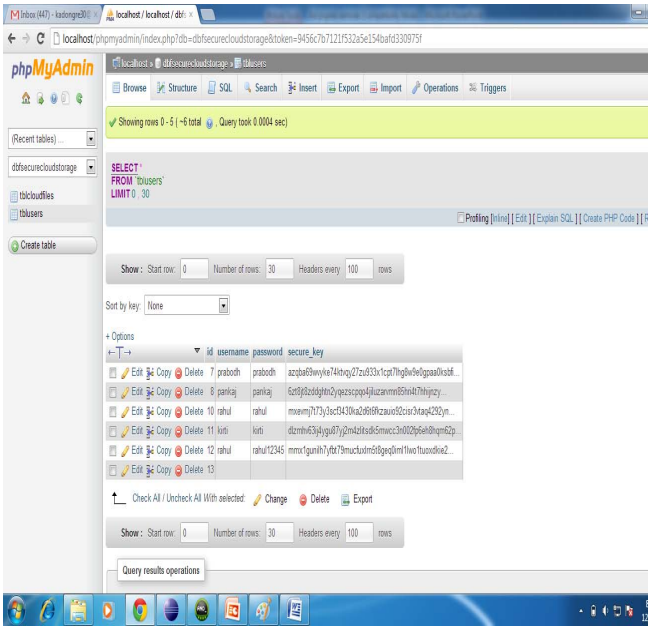
[3] Claudio E. Palazzi, Macro Ferrarese FTP4Android: A Local/Remote File Manager for Google Android Platform, 3rd IEEE International Workshop on Digital Entertaintment, networked Virtual Enviroments and Creative Technology, 2011.

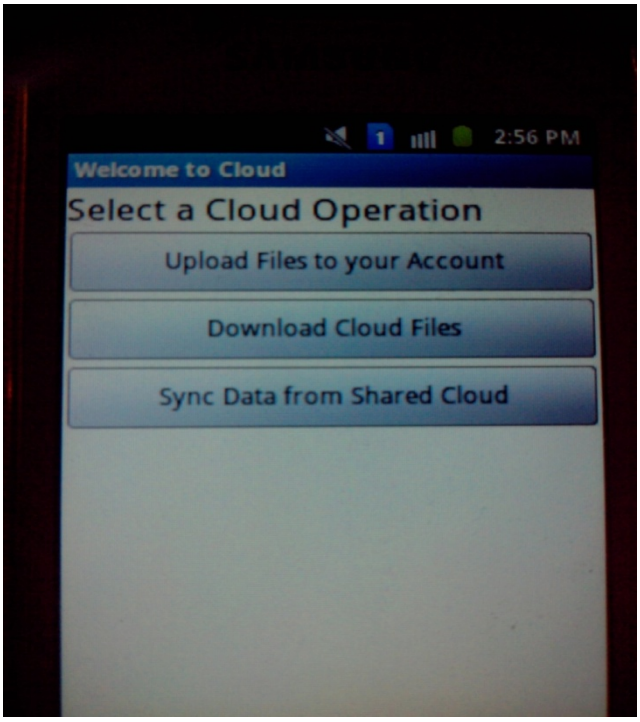
[4] Dinesh C "Data Integrity and dynamic storage way in cloud computing" 2011.

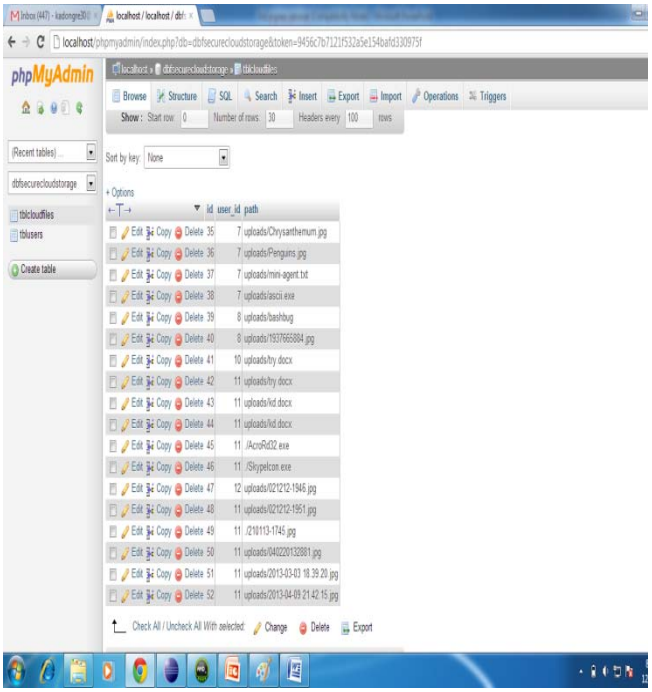
[5] Towards Secure and Dependable Storage Services in Cloud Computing Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE-2011.

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

[7] Zaheer Ahmad a, Keith E. Mayes b,*, Song Dong a, Kostas Markantonakis b "Considerations for mobile authentication in the cloud" 2011.


phpMyAdmin
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Triggers
SELECT *
FROM `tbusers`
LIMIT 0 , 30
tblcloudfiles
tblusers
Create table
Query results operations


2:56 PM
Welcome to Cloud
Select a Cloud Operation
Upload Files to your Account
Download Cloud Files
Sync Data from Shared Cloud


phpMyAdmin
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Triggers
tblcloudfiles
tblusers
Create table