Secure Mobile Cloud Storage and Data Transmission

Akanksha Samadhiya  
Sushila Devi bansal collage of Engineering Indore  
apusam009@gmail.com

Trapti ozha  
Sushila Devi bansal collage of Engineering Indore  
trapti_ozha@yahoo.com

Abstract
Cloud computing provide efficient computing experience and computational resources. In addition of that it offers secure data hosting services. The security to the cloud is essentially strong and private internet access area is also secured. But the data transmission between two secure networks is performed over unreliable network. Therefore a secure data transfer service is required to design. On the other hand the mobile devices are built with efficient processing ability but their storage support is found weak. Thus a data hosting service is desired to implement in mobile devices. Additionally the security during data transference, storage and private management is required to consolidate. Therefore this paper provides the understanding and a cloud security literature survey for problem identification and also provides a solution to overcome the reported problems.

Keywords— cloud computing, mobile computing; secure storage, secure data transmission, privacy.

1. INTRODUCTION
The cloud is a new generation computing and it provides very effective services for utilizing it remotely without any installation and maintenance of any software or hardware programs. It is adoptable and economic resource. In cloud environment provides a service therefore a software can be kind of service for example Google doc. Any user can get the services directly from the service provider using the internet. Now in these days the mobile devices are becoming more efficient and smart. Therefore it is not only for communication it can perform more tasks. Additionally most of the mobile devices provide a system for internet access.

Thus there is an application for mobile devices based upon cloud computing. These days, many applications are developed using the support of mobile devices and these applications are becoming more popular due portable use of mobile device and tablets. Some of these applications are developed for backup and storage management of smart mobile devices. In this work a mobile cloud concept is desired to design which is capable to manage the entire kind of data with secure manner. This application is designed for the maintenance of online mobile data. Users are provided with a unique username. In the online storage the details about his data and whatever he uploaded in cloud, stored and can be viewed simultaneously. In the case of theft or lost of mobile, data can be easily retrieved from cloud.

Therefore the private and sensitive data is managed over the cloud platform through the mobile device. But security on cloud and during data transmission through the public area network is leads to study about the cloud data security and network based data security.

2. BACKGROUND
In this section the recent efforts on the mobile data management and security is reported which makes an essential contributions.

V. Malligai et al [1] provides a secure mobile cloud concept where Mobile hand held device such as smart phones have progressively became powerful in recent years. Smart phone is not only voice oriented device but it is also equipped with wide capabilities like internet access, various applications etc. As mobile devices are overcoming computers, it tends to carry and store all kinds of data such as m-Passbooks, cameras, planners, mp3 players, etc., in cloud it can be accomplished for Google Android phones. The primary objective of “cloud based mobile data storage system” is to create a full-fledged Android app where we can store all kind of mobile data in cloud and access it concurrently. The user can access the data in mobile from anywhere in the world.

Cloud computing has been designed to remit computing as a service. It accommodates shared resources, software and information to computers and other devices over a network. The sprouting network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. Using cloud computing we can store and retrieve the data easily. To maintain the data securely in distributed environment i.e., on clouds P. Srinivas et al [2] propose an effective and flexible distributed scheme with Token Generation algorithm for data files checking as a secure and dependable cloud storage service. A new scheme...
was introduced to inscribe with the user specified key parameters to make the resource more potent. They derive a new algorithm which is very light weight and easy to compute. Here we store the encrypted blocks of data into cloud and perform token checking on this encrypted blocks which secure the data. In case of any block modifications we substantiate the data effectively of files before storing to Clouds by token acknowledgment. The proposed strategy is highly efficient and expansive against attacks like Byzantine server failures, malicious data alteration attack. Two way verification of file blocks which results more robust and ensure that data will not be modified before reaching to clouds.

Mobile cloud computing is gaining popularity among mobile users. The ABI Research anticipate that the number of mobile cloud computing subscribers is expected to grow from 42.8 million (1.1% of total mobile users) in 2008 to 998 million (19% of total mobile users) in 2014. Despite the plugging acquired by mobile cloud computing, the expansion of mobile cloud computing subscribers is still not up to the apprehension. According to the recent survey conducted by the International Data Corporation, most IT Executives and CEOs are uninterested in adopting such services since there are risks associated with security and privacy. The security perils have become a barricade in the rapid adaptability of the mobile cloud computing paradigm. Indicative efforts have been devoted in research organizations and academia to build secure mobile cloud computing environments and infrastructures. Despite of the efforts, there are a number of loopholes and challenges that still exist in the security policies of mobile cloud computing. Abdul Nasir Khan et al [3] provide review on: (a) highlights the current state of the art work proposed to secure mobile cloud computing infrastructures, (b) identification of the potential problems, and (c) provides taxonomy of the state of the art

The augmentation of cloud computing and mobile computing technologies leads to the newly emerging mobile cloud computing prototype. Three considerable approaches have been proposed for mobile cloud applications:

1. Extending the access to cloud services to mobile devices.
2. Enabling mobile devices to work collaboratively as cloud resource providers.
3. Augmenting the execution of mobile applications on portable devices using cloud resources.

In this paper, Lei Yang et al [5] focus on the third approach in supporting mobile data stream applications. More specifically, author study how to optimize the computation partitioning of a data stream application between mobile and cloud to achieve maximum speed/throughput in processing the uploading data. To the best of our knowledge, it is the first work to study the partitioning problem for mobile data stream applications, where the augmentation is placed on achieving high throughput of processing the streaming data rather than minimizing the make span of executions as in other applications. They first propose a framework to provide runtime support for the dynamic computation partitioning and execution of the application. Apart from existing works, the framework not only allows the active partitioning for a single user but also supports the sharing of computation instances among multiple users in the cloud to achieve efficient utilization of the underlying cloud resources. Meanwhile, the framework has better scaling ability because it is designed on the elastic cloud fabrics. On the basis of the framework, we compose a genetic algorithm for optimal computation partition. Both numerical assessment and real world experiment have been performed, and the outcome shows that the partitioned application can achieve at least two times better performance in terms of throughput than the application without partitioning.

3. PROPOSED WORK

In order to provide the secure mobile cloud data storage services the following issues are considered.

- Mobile devices are built with efficient computing but the storage and backup is not much secure.
- Transmission of data between two secure devices is performed using public and untrusted network.
- Data in cloud is stored at random in the cloud space private and sensitive data can be mismanaged and produces the redundancy during their management.

Thus the following computational and properties are required to fulfill in proposed solution. The desired system can be simulated in the following manner.

The above given solution is proposed to achieve the desired objectives and simulated using figure 1.

In this given system the blocks are representing the objects of modules and the number labelled on links are shown the
activity between two modules. In this diagram first block is user mobile device which contains different kinds of data some of them are sensitive and private additionally some other kinds of data is also available on mobile. In addition of that the cloud storage where the data is classified in two kinds of storage space first the private wallet where an additional cryptographic security is implemented during data storage. Additionally for other non-sensitive data can be parked on normal storage. In this system a third part is also available which is used for trust and authentication management.

1) The flow of activity is initiated from the user mobile device. Thus user first makes a connectivity request from cloud storage server.

2) The cloud storage initiates the authentication server, which is the trusted third party server. Cloud server send request to trusted server to check user is trust worthy or not...

3) Authentication server responds the user with a screen for accepting the user id. The user id is the unique identification of the particular user.

4) After submitting the user id to the authentication server, server asks a password which is one of the information which is submitted during the registration process in random manner.

5) These correct data insure the trusted server that the user is trust worthy and can provide the access to the client.

6) After answering and server validation the user mobile can access the cloud storage. Like uploading and downloading the data.

7) There for user making a service request to the cloud storage to access all type of data like normal content or private wallet.

8) Mobile pre-estimates the file type, their sensitivity rating and file size. In response of that the authentication server generates a token for data service and utility.

The proposed solution leads to solve the issue of small storage space for user data collection and also provides the solution during the data transfer and man in middle attack. Therefore the following solution is incorporated in this solution.

- Providing a secure and different level of data management scheme for private data storage and normal data storage.
- Solution incorporates the additional security of private data management during data transmission is based in trust management and token based data exchange.

In figure 2 all the process flow about the proposed system is illustrated:

- In the beginning of process client listed the request to cloud storage server. Here the client is a user who can already register in server.

- Server initiates the authentication request using trusted third party server.

- After that trust estimation done in trusted third party end. Trusted server check the authentication of client according to his user attributes.
Now if trusted server satisfied with client attributes and consider the request as a trusted request then client get permission to access server. Else trusted server sends a message and exit.

- If client get the the permission to access sever then he could perform the utility.

4. FUTURE WORK

In this presented work a mobile cloud concept is proposed for design. This cloud is able to preserve the data on cloud and user can access these data when required. In order to provide security on storage and data transmission a new model for computing is also provided. This model includes the concept of third party trust management, cryptographic data transmission and privacy preserving data management through mobile and cloud interaction.

In near future proposed technique is developed using the JAVA technology for cloud data management. Android technology is used for mobile device data support. Additionally their performance and security is computed and published in next.

5. REFERENCES


[5] Lei Yang, Jiannong Cao, Yin Yuan, Tao Li, Andy Han, and Alvin Chan, “A Framework for Partitioning and Execution of Data Stream Applications in Mobile Cloud Computing”, 2012 IEEE 5th International Conference on Cloud Computing (CLOUD)