International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 10 October 2015

A secure mobile cloud storage and data transmission

Ms. Sonal Modh[1], Dr. M.K. Rawat[2]
M Tech Scholar[1], Head of Deptt[2]
Department of Computer Science and Engineering, Lakshmi Narain College of Technology
Indore- 453331(M.P.), India
sonalmodh@gmail.com[1], drmkrawat@gmail.com[2]

Abstract— *In the world of wireless network Cloud computing play major role rather than as a facility in a profitable manner. In addition of that it convey services that enable us to run data and data accelerated applications. The security in cloud environment is foremost durable and the private internet entrance area is also secured. But the problem is that security is not implementing in between two secure networks it is executed over untrusted network. Therefore a service is enforced to design which transfer the data in secure manner.The mobile devices are available with powerful processing ability but their storage is found shorter. Thus a service that enables us to run data and data intensive application is desired to implement for mobile devices. Instead of security in between two secure networks during the data transmission, their storage and privacy administration is required to organize in protective manner. In this paper it contributes the considerate and a cloud security literature survey to recognise the problem and also provides a clarification 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 maintain very adequate services for handling it remotely beyond installation and conservation of any software or hardware programs. This ability makes it adoptable and low cost computational resource. In cloud environment any resource distribution is provided as 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 becomes more efficient and smart. Therefore it is not defined for communication it can execute more tasks. In addition of that most of the mobile device arranges the system for internet access.

Thus in this presented work an application for mobile devices is presented using the cloud computing. So the mobile cloud is key area of concern. Now in these days a number of applications are developed using the support of mobile devices and these applications are becomes more popular due to portable use of mobile device and tablets. Some of these applications are developed for backup and storage management for smart mobile devices. Additionally some of them used for contact and private data management. In this proposed work a mobile cloud approach is required to implement which is able to manage the entire kind of data with secure aspect. This mobile application is designed for the purpose of maintaining the online mobile data. The user can sign in their username and password. The online storage mobile data contain information of every user data what they upload in cloud and also they can view their data at the same time while uploading. In case user loss the mobile, they can retrieve all the data through web.

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 untrusted network is inspire us to study about the data security of cloud and data security of network.

2. Background

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

V. Malligai et al [1] provides a secure mobile cloud concept where Mobile hand held device such as smart phones has increasingly became powerful in years. Smart phones are not only with voice oriented device but also equipped with wide capabilities with internet access. With the advent of cloud

services for mobile application, it has greatly enhanced the scalability and security. As mobile devices become more like PC's, it tends to carry and store all kinds of data such as check books, cameras, planners, mp3 players, etc., in cloud that 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 simultaneously. The user can retrieve all the data in mobile itself and can also access this data through web. Thus ,it reduces the overhead of using only mobile to get back the data which serves the purpose of making our data secure and flexible (i.e) to be available anywhere.

Cloud computing is the delivery of computing as a service rather than a product. It provides shared resources, software, and information to computers and other devices over a network. The increasing 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. We can store and retrieve the data as we like using cloud computing. 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 encrypt with the user specified key parameters to make the resource more robust. They derive a new algorithm which is very light weight and easy to compute. Here we stores the encrypted blocks into cloud and perform token checking on this encrypted blocks which gives more security to data. We verify the data effectively in case of any block modifications of files before storing to Clouds by token acknowledgment. The proposed scheme is highly efficient and resilient against attacks like Byzantine server failures, malicious data modification 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 predicts 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 hype achieved by mobile cloud computing, the growth of mobile cloud computing subscribers is still below expectations. According to the recent survey conducted by the International Data Corporation, most IT Executives and CEOs are not interested in adopting such services due to the risks associated with security and privacy. The security threats have become a hurdle in the rapid adaptability of the mobile cloud computing paradigm. Significant efforts have been devoted in research organizations and academia to build secure mobile cloud computing environments and infrastructures. In spite 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) identifies the potential problems, and (c) provides taxonomy of the state of the art.

The latest developments in mobile devices technology have made smartphones as the future computing and service access devices. Users expect to run computational intensive applications on Smart Mobile Devices (SMDs) in the same way as powerful stationary computers. However in spite of all the advancements in recent years, SMDs are still low potential computing devices, which are constrained by CPU potentials, memory capacity and battery life time. Mobile Cloud Computing (MCC) is the latest practical solution for alleviating this incapacitation by extending the services and resources of computational clouds to SMDs on demand basis. In MCC, application offloading is ascertained as a software level solution for augmenting application processing capabilities of SMDs. The current offloading algorithms offload computational intensive applications to remote servers by employing different cloud models. A challenging aspect of such algorithms is the establishment of distributed application processing platform at runtime which requires additional computing resources on SMDs. In this paper Muhammad Shiraz et al [4] reviews existing Distributed Application Processing Frameworks (DAPFs) for SMDs in MCC domain. The objective is to highlight issues and challenges to existing DAPFs in developing, implementing, and executing computational intensive mobile applications within MCC domain. It proposes thematic taxonomy of current DAPFs, reviews current offloading frameworks by using thematic taxonomy and analyzes the implications and critical aspects of current offloading frameworks. Further, it investigates commonalities and deviations in such frameworks on the basis significant parameters such as offloading scope, migration granularity, partitioning approach, and migration pattern. Finally, they put forward open research issues in distributed application processing for MCC that remain to be addressed.

The contribution of cloud computing and mobile computing technologies leads to the newly emerging mobile cloud computing paradigm. Three major 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 streaming data. To the best of our knowledge, it is the first work to study the partitioning problem for mobile data stream applications, where the optimization 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. Different from existing works, the framework not only allows the dynamic 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 scalability because it is designed on the elastic cloud fabrics. Based on the framework, we design a genetic algorithm for optimal computation partition. Both numerical evaluation and real world experiment have been performed, and the results show 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.

1. Mobile devices are built with efficient computing but the storage and backup is not much secure.

2. Transmission of data between two secure devices is performed using public and untrusted network.

3. 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.

4. Proposed Solution

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.

1. Providing a secure and different level of data management scheme for private data storage and normal data storage

2. Solution incorporate the additional security of private data management

3. During data transmission is based in trust management and token based data exchange.

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

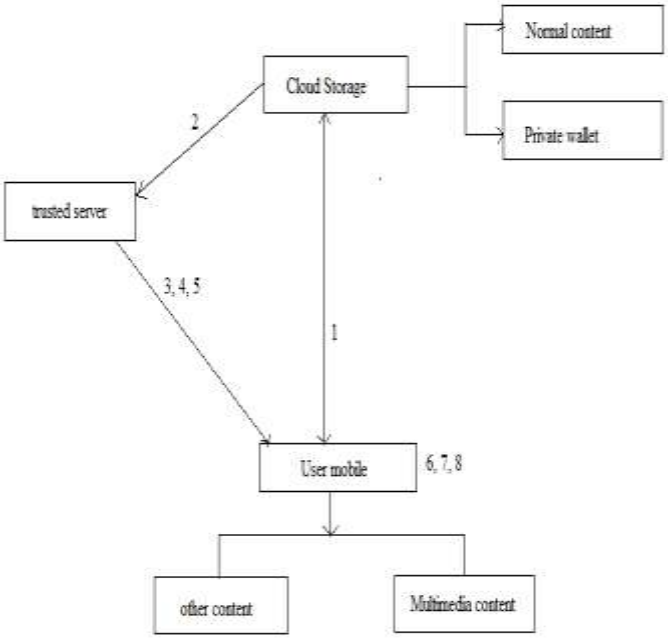

Figure 1: proposed system

In order to achieve the desired objectives the above given solution is proposed 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. (3) Authentication server responds the user with a screen for accepting the user id. (5) After submitting the user id to the authentication server, (4) server asks a password which is one of the information which is submitted during the registration process in random manner. (6) After answering and server validation the user mobile can access the cloud storage. Therefore when a user (7) making a

service request to the cloud storage the user (8) mobile pre-estimate the file type, their sensitivity rating and file size. In response of that the authentication server generates a token for data service and utility.

5. Conclusion and 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.

References

[1] V. Malligai, V. Venkatesa Kumar, "Cloud Based Mobile Data Storage Application System", International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), Vol. 2 Issue Special 1 Jan-March 2014

[2] P. Srinivas, K. Rajesh Kumar, "Secure Data transfer in Cloud Storage Systems using Dynamic Tokens", International Journal of Research in Computer and Communication technology, IJRCT, ISN 278-5841, Vol 2, Isue 1, January ,2013.

[3] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, "Towards secure mobile cloud computing: A survey", © 2012 Elsevier B.V. All rights reserved

[4] Muhammad Shiraz, Abdullah Gani, Rashid Hafeez Khokhar, and Rajkumar Buyya, "A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing", IEEE Communications Surveys & Tutorials, VOL. 15, NO. 3, THIRD QUARTER 2013

[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)