Research Inventy: International Journal of Engineering And Science
Vol.6, Issue 5 (May 2016), PP -71-74
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Mobile Cloud Computing With Safe Security

Sricharan yadavalli[1], Srinivas upputuri[2], Dileep kumar V[3]
[1,2,3] *Computer Science Engineering Department, Sree Dattha Institute of Engineering & Science*

Abstract: *Now a day's Mobile Cloud computing is a emerging technology. This technology will provides so many services for mobile devices. and this technology gives so many advantages to mobile users. But there is one more issue with this technology there is a security problems and privacy issues regarding this technology. and we have solutions for this issues also but they are providing independent solutions for this issues. Now I want to propose a new system that will provide the solution for this issue is that I want to develop a Framework it is used to secure the data transmitted over the mobile device for mobile cloud computing. This frame work will provide different kinds of security properties for different kinds of data transmitted over the mobile device. and this approach will also concentrate on the issue of user preferences and mobile device performances .*

Keywords: *Mobile Cloud, Framework, Security issues.*

I. Introduction

The technology of Mobile Cloud Computing is new topic in the research. It brings various advantages for mobile devices since it enables the use of Cloud resources and services. The security issues in Mobile Cloud Computing are due to the security threats against the Cloud, the mobile devices and applications running on these devices, which can be native or mobile web applications. These threats can be classified in four categories: mobile threats, cloud threats, mashup threats and technological threats. All this menaces have as a purpose to steal user private data or to exploit mobile device resources.

Our work focuses on securing private data used by a component-based mobile cloud application. There are very few studies in this area. The existing security solutions treat independently the different types of mobile cloud security problems[1]. Solutions for security issues on mobile devices are proposed by the mobile platforms, also the services providers suggest solutions for issues in Cloud. The security issues concerning data transmission are solved by service providers using security protocols such as SSL/HTTPS[2]. However, this kind of protocols are on one hand high energy consuming and on a second hand provide security properties as a block without taking into account the type of data transmitted or the user expectations.

II. Application Models Of Mobile Cloud Computing

Cloud Computing is a new internet-based paradigm that is focused on providing services to its customers, according to their needs[3]. It offers the advantages of having on-demand computing services, paying according to the resources used and tolerance to resources alteration; moreover cloud services can be employed by different types of client platforms (e.g., mobile phones, laptops, and PDAs). A definition that is generally. This declares that Cloud Computing is defined by describing three Cloud service models: Infrastructure as a Service (e.g. servers, networks and storages), Platform as a Service (e.g. middleware services and operating systems) and Software as a Service (e.g. application programs); those are provided by cloud providers like Amazon, Google at certain prices. In addition to this service models, there were established four Cloud deployment models: Public, Private, Community and Hybrid.

Mobile Cloud Computing is a model developed as a solution to overcome the mobile devices challenges by using Cloud Computing services like storage and computing resources. It also tacks into account the context of the mobile operating conditions. In order to benefit as much as possible from the advantages offered by the Cloud, there have been several studies on mobile cloud applications models[4].

Mobile cloud applications can be classified in three categories; a feature used in defining these three categories is the mobile device involvement in the execution of a mobile cloud application. The three categories are as follows: a) The Client model: Here the mobile device is seen only as a more convenient way to access services in the Cloud. b) The Client/Cloud model: It includes applications divided into components and distributed between mobile device and the Cloud[5].

These models use techniques like: augmented execution , elasticity and mobility to overcome the mobile devices limitations by distributing the application execution. c) The Cloud model: It considers the fact that the mobile device is an integral part of the Cloud . The objective for the Cloud model approach is to provide a distributed infrastructure that exploits the storage and computing capacity of several mobile devices in order to support new applications[6]. In is made a comparison between the novel applications models proposed and developed for mobile devices. The new applications models go on the idea of separating an application into components.

III. Solutions For Security Issues

Mobile cloud applications expose user private data to different security risks. User data can be stored on the mobile side or on the Cloud side, can be accessed by applications (or application components) that run on the mobile device or in Cloud, or can be transmitted between mobile device application components and Cloud application components.

A. Security Issues Related to Mobile Cloud Applications

As we have said previously, Mobile Cloud Computing is a combination of mobile and Cloud Computing. Thus, the security risks are caused by the security attacks on the mobile side, the security issues on the Cloud side and also by the security attacks against the communication channels. The last studies on mobile security issues have revealed the following categories of mobile attacks: application based attacks, web-based attacks, network based attacks and physical based attacks. These attacks affect the integrity and the confidentiality of mobile data and applications. As a result, data may be corrupted, modified or deleted and the application functionality can be altered. Repackaging was the most used technique in 2011 to infect applications running under Android . An attacker takes a healthy application; changes it so that this contains malicious code and after republishes it. Technologies such as HTML5 and AJAX enabled the growth of the mobile computing market, but as a drawback these technologies introduce some security issues and provide opportunities to the malicious users to obtain user's private data. Mobile Cloud Computing provides the advantage of storing a large amount of data outside the mobile device, i.e. in the Cloud. However, the Cloud can be the target of various attacks concerning about data privacy, data ownership and location, data access and integrity. Moreover, in mobile cloud models the various components of an application may communicate or communicate with other web services and the used communication channel can be the target of network attacks such as man in the middle when the attacker connects with the victims and takes controls over their communication.

B. Existing Solutions

To secure user data and applications, the mobile platform providers (e.g. Android, iOS) implemented several security solutions. These solutions were included into the operating system of the devices. Five types of security features have been implemented by the different platforms: traditional access control, application provenance, encryption, isolation and permission-based access control. Each mobile platform implements a different strategy to secure data. Thereby, the service providers have to adapt the applications to the strategy already adopted. Applying a high level of protection implies a limitation of performance, and also a high-energy consumption of the mobile. The application of these strategies will allow securing data on the mobile device, however, when the data will be sent and stored in the Cloud, it will become out of the user control.

For the Cloud side, different solutions have been proposed to secure the data access. For example, to secure Fig. 2. Secure Mobile-Cloud framework elastic applications a solution has been developed in , but this solution is provided for a specific application model, i.e. elastic applications with code migration. Beside the elastic application model different novel application models have been proposed . However, the solution presented in cannot be applied to these new models, i.e. component-based applications.

The mobile cloud application providers have to secure the data exchanged between the mobiles and Cloud. A commonly used solution is the SSL protocol, but as it has been said previously and proved in using SSL increases the energy consumption of mobile devices. Another solution proposed for securing the communication between mobile devices is LECCSAM . LECCSAM is an architecture based on security components that aims to optimize the mobile device energy consumption. Even if LECCSAM brings several advantages in securing the communication between mobile devices, it is not adapted to the mobile cloud applications.

IV. Proposed Work

We are initially focussing on the component based solutions for mobile cloud computing in this paper we are going to develop a framework that is used for users to give their own priorities according to that priorities we are going to develop this framework base solution for mobile cloud application

According to the problem we develop a framework then we are giving a name called mobile cloud computing with security (MCCS) it is going to fulfil the following features. here the main intension is that to secure the communication between the components that is between the cloud based system and also the mobile based system. According to user requirements our framework will adapt the security services and user context requirements.

MCCS Framework has several components it is going to run these components on both systems like cloud and as well as on mobile device here are some managers each manager will have some defined things that are as follows and these security components deployed in both cloud and as well as in mobile device each of this security component satisfies one security property that is confidentiality.

A. Framework setup

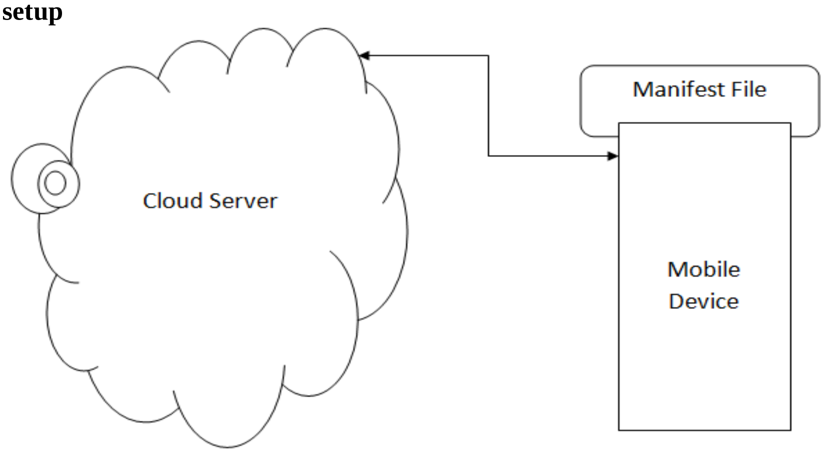

Fig1.1 Framework Setup for Cloud Server

In this application process the data is being checked and verified by the framework so that it can avoid the use of malicious data. For this integrity check the framework has proposed the following verifications a). The application is going to check if there is an existence of a file initially the device send the manifest file to the cloud server and then the cloud server checks the data available means if it matches the particular data then there is no malicious data is there and if it is not then there is malicious data available in the cloud server it means that it will perform this operation according to the credentials sent by the user .

For this overall setup we are taking an Android mobile device and cloud server according to the configuration of that particular mobile device only the data will be selected and it will sent to the particular mobile device according to the hardware configuration of the mobile device basically the Android mobile device will sent an manifest file in that the user will clearly mentions the hardware configuration of the mobile device. It will handle the risks that are getting by the user at that particular time. Here the new manifest file and old manifest file will be compared by this framework and it will provide the authentication property to the mobile device. Finally the results are sent back to the manager for remaining operations .

B. Communication Security

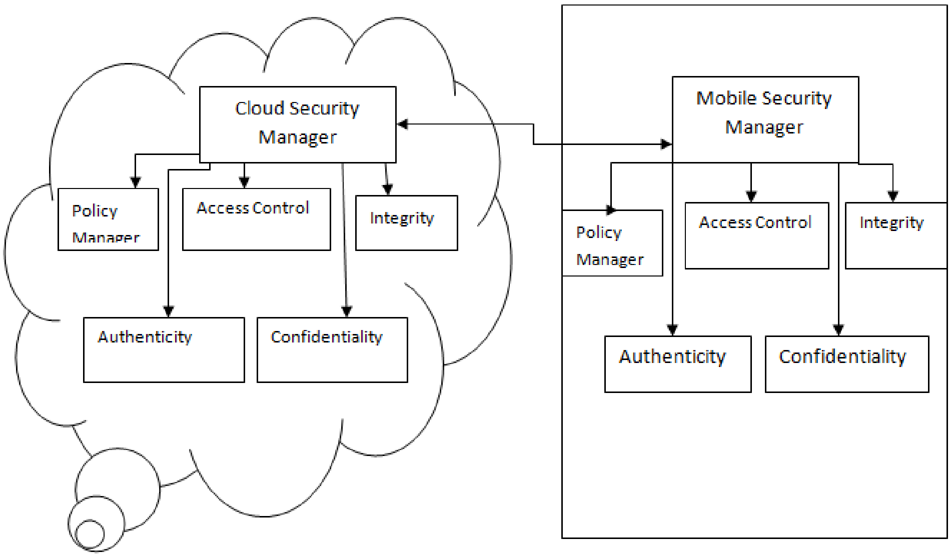

Fig1.2 Mobile Cloud With Safe Security

For security concern we are using LECCSAM because it provides a solution very flexible for the security management our intension is to extend the data security among the cloud as well as on mobile device.

Security concerns can be done by the following managers those are Mobile security manager and Cloud security manager. They are going to receive the contents like mobile hardware configuration according to that hey provide the solutions to the mobile device with respect to the cloud server . in this process the cloud applications are directly communicate with the cloud server and gives the appropriate solutions to the mobile device manager.

Mobile manager will keep the data regarding the user options given by the mobile device user. And finally the cloud manager will provide the authentication to the mobile device manager and gives the required data that was asked by the mobile device user. So it is not a threat for the mobile device user

V. Conclusion

Mobile Cloud computing provides so many solutions for the mobile device users but there is no particular framework for getting all these services in one hand we proposed a framework that will provide the solution for this problem means with security we are given a solution to this problem and that is according to the user requirements hardware configuration and software configuration according to that the user will get the service from the cloud server this framework provides a solution to verify the integrity of an application.

References

[1]. Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V2”,

[2]. M. Armbrust, et al., „Above the Clouds: A Berkeley View of Cloud Computing”, February, 2009.

[3]. ENISA, “Cloud Computing Benefits, risks and recommendations for information security”, November, 2009,

[4]. B.G. Chun and P. Maniatis, “Augmented Smartphone Applications Through Clone Cloud Execution,” in Preceedings of the 12th Workshop on Hot Topics in Operating Systems (HotOS XII), USENIX, 2009.

[5]. X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, “Securing Elastic Applications on Mobile Devices”, In CCSW’09, November, 2009, Chicago, Illinois, USA.

[6]. V. March, Y. Gu, E. Leonardi, G. Goh, M. Kirchberg, B. S. Lee, “μCloud: Towards a New Paradigm of Rich Mobile Applications”, in the 8th International Conference on Mobile Web Information Systems (MobiWIS), June, 2011.