# Analysis of Security Frameworks for Mobile Cloud

Samith K S
PG Student, CSE
Thejus Engineering College
Thrissur, India

Vinitha A.V
Assistant Professor, CSE
Thejus Engineering College
Thrissur, India

## ABSTRACT

The concept of Mobile Cloud Computing is relatively new in the research. It brings various advantages for mobile devices since it enables the use of Cloud resources and services. This paper gives a survey of MCC security frameworks, which helps general readers have an overview of the MCC. The issues, existing solutions, and approaches are presented. The paper is organized as follows. In the next section, we will go through some papers and get a brief idea about MCC, which helps general readers have an overview of the MCC. The issues, existing solutions, and what is actually going on in the current cloud based mobile security research and analyze two frameworks for security of mobile cloud computing.

## General Terms

Secure Mobile-Cloud (SMC), A Private Cloud and File Characteristic-Based Framework for Mobile Security (PCFC), Security Issues In Mobile Cloud Computing.

## Keywords

Mobile cloud computing; security frameworks; security.

## 1. INTRODUCTION

The mobile security is becoming more and more important, as the increasingly prevailing Smartphones, on one hand, offer people more advanced services, such as web browsing, Instance Message, and web camera; and on the other bring us new security issues – these have been nourished by plenty of system interfaces and services offered by smartphone platforms, among which the Symbian OS is the top one according to the report. From the aspect of defense and protection, mobile devices, however, naturally limit the effectiveness of addressing security issues occur in them. Resources inside these platforms are usually scarce. The computing power and memory capability of them are hard to completely meet the requirements of running resource intensive services, such as file scanning, advanced calculating. In the case of security protection, the situation is even worse. Malware detection on handset, for instance, is not only a time-consuming task, but also one that devour much of their enriched energies. So one of the main difficulties now facing us is, what we can do to protect and secure our born deficient daily friend. A solution to the mobile device challenges is Mobile Cloud Computing, who offers Cloud Computing as a platform for powerful applications.

Many researchers are naturally led to the cloud computing. As an evolution of service-oriented architecture and virtualization, the cloud computing potentially provides infinite computational capabilities for its customers, with a method of pay-as-you-consume, which is far more different from the traditional way of network computing. This is an exciting combination for many researchers. Some of them even predict that it might “inspire our research in mobile computing over the next decade and beyond” [3].

## 2. SECURITY ISSUES IN MOBILE CLOUD COMPUTING

### 2.1 Mobile Terminal [4]

In general, mobile terminal has the following characteristics: the open operating system; supporting the third-party software; "personalization"; wireless access Internet anywhere and anytime.

#### *2.1.1 Malware*

Openness and versatility of the mobile terminal always draw the attackers' attention. Because of this the user of the mobile terminal will suffer from the economic damage or information leakage. So we need to give the solutions for malware detection and prevention in the mobile terminals.

#### *2.1.2 Software Vulnerabilities*

#### *2.1.2.1 Application Software*

At present smart phone is the main mobile terminal. And most smart phone users are used to managing the phone through the mobile phone management software, which manages the files in the mobile phone through the content synchronization between the phone and the computer. FTP (File Transfer Protocol) is usually applied to this process. The user name and password of FTP are transferred over the network and saved in the configuration file in clear text. This will cause the illegal access to the mobile phone using FTP from the computers in the same network, ultimately lead to the leakage of personal information and illegal access, intentional delete and malicious modification.

#### *2.1.2.2 Operating System*

Operating system is in charge of the management and control of the hardware and software resource. And it is so complex software that it will exits coding bugs. In some conditions, these bugs will be used to destroy the mobile phone by attackers

#### *2.1.3 Others*

Besides, security issues in the mobile terminal still come from the mobile users themselves. We need to detect and prevent anomalous behavior of users.

### 2.2 Mobile Network Security [4]

Based on the traditional network, mobile network expands the network node and the access way of users due to its mobility. The broad access ways (SMS, Wi-Fi, Bluetooth etc.) will bring more security threats such as the sensitive information leakage or malicious attack.

### 2.3 Mobile Cloud [4]

#### *2.3.1 Platform Reliability*

The cloud platform is susceptible to being attacked because of its high concentration of information resources of users. Attacks perhaps come from malicious outside, legal cloud computing user, or inside staff of the cloud computing operators.

### *2.3.2 Data and Privacy Protection*

In the cloud the ownership and management of the users' data are separated, which cause that the worries of users to their own information resource become the important obstacle for the popularization of the mobile cloud computing. In addition the users' data are stored randomly in the shared infrastructure all over the world, and users do not know the specific position in which their data are stored. So users' private information faces increased risk of exposure.

# 3. CURRENT SECURITY APPROACHES FOR MOBILE CLOUD COMPUTING

## 3.1 Aiming at Mobile Terminal Security

### *3.1.1 Anti-Malware*

To overcome the resource restriction of mobile terminals, we can move the malware detection to the cloud. And when a malware is detected, legal software from the cloud can be assigned to the mobile terminal and be run to remove the malware. To prevent the mobile devices from being installed malware, the users should be careful of their behaviors.[4]

### *3.1.2 Software Vulnerabilities*

For software vulnerabilities, on the one hand, the users should pay attention to the update information of mobile phone operating system, and timely download and install the patches or revamped versions from the research and development company of the operating system. Meanwhile, they should be careful of downloading the third party software.[4]

### *3.1.3 Regulating User’s Behavior*

Much malware is downloaded and run because of the users' mis-operation or lack of security awareness. So improving the security awareness of the users is the key measure to prevent the malware.[4]

## 3.2 Aiming at Mobile Network Security [4]

Only encrypted information is relatively secure during the transmission over the mobile network, in no matter which way the mobile terminals access the mobile network. For all kinds of access ways, researching the security protocol is the core to reduce various attacks.

## 3.3 Aiming at Mobile Cloud Security [4]

### *3.3.1 Protection to Platform Reliability*

First of all, the cloud providers should integrate the current security technologies including VPN technology, authentication and access control, encryption and other technical means, and so that they can provide the continuous available service against various attacks such as DOS attacks and information stealing. Secondly the cloud providers should offer complete backup and recovery solution in order to recover the users' data when serious attacks happen.

### *3.3.2 Data Encryption and Key Management*

To prevent sensitive information from leaking, the data should be stored in cipher text in the cloud. However encryption will reduce the utilization rate of the data, so the focus is moved to efficiently analyzing and processing the cipher text.

### *3.3.3 Authentication and Access Control*

Now there are two kinds of authentication approaches which attract significant attention. The one is user-centric identity authentication. In this approach, a user is identified and defined through identifiers or attributes, and a user can be allowed to have multiple identifiers. The other is behavioral authentication in which we can identify users by their habits and behavior such as memorized data, their belongings. When users finish the data transmission to the cloud, the access control will play a direct role.

# 4. SECURITY FRAMEWORKS

Here we are going to see two security frameworks proposed in the papers [1] and [3].

## 4.1 Secure Mobile-Cloud (SMC) [1]

The Component-based mobile cloud application models with different execution locations, and with no security solutions provided for data transmitted between components. Assuming that there is no need to apply the same security level for all data transmitted between the components. Moreover, it allow the users to choose the security level they want to apply to their data and to adapt the security level applied according to the mobile device energy consumption.

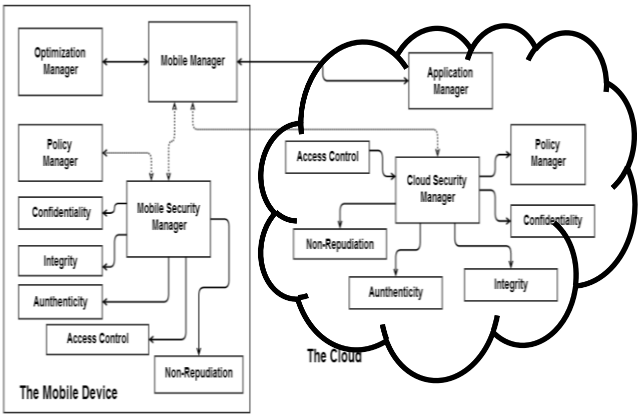

**Fig 1: Secure Mobile-Cloud Framework [1].**

Secure Mobile-Cloud (SMC) has to fulfill the following features: to ensure the integrity of an application at setup and to secure the communication between the same application components. This architecture has to be able to adapt the security services according to the user needs, device characteristics and user context.

SMC framework (see Fig. 1) has several components running in the Cloud and on the mobile: 1) five kinds of managers where each manager has a well-defined functionality (see Table.1)) the security components deployed in both Cloud and mobile device. Each security component satisfies one security property (e.g. integrity or confidentiality).

**Table 1 .Description Of the Managers [1]**

| Manager | Description |
|---|---|
| Mobile Manager | It collects data and events that occurs on the mobile side and sends them to the appropriate manager to be analyzed. |
| Mobile Security Manager<br>Cloud Security Manager | Both provide the composition of the security properties. The Mobile Security Manager ensures security composition on the mobile side and the Cloud Security Manager ensures that composition on the Cloud side. |

| | |
|---|---|
| Optimization Manager | It sends the information collected from sensors (e.g. network sensor, energy sensor) to the mobile manager. |
| Application Manager | It checks the application integrity at the setup. |
| Policy Manager | It determines which security components are required for a specific security level. |

### *4.1.1 Application Integrity at Setup*

Application integrity has to be verified at installation and update. In this way it can be avoid the use of malicious application and the loos of private data. For this integrity check the framework proposed has to accomplish the following verifications: 1) if the application exists, 2) the application signature and 3) the application access described into the "manifest" file. Then the signature is verified.

The next step is to verify the "manifest" file. User's give the authorization without thinking. The framework provides: a function whose feature is to analyze the different access levels recorded in "manifest" file and to evaluate the risks for the access authorized by user; and, a function of comparison between manifest files.

Events that signal an application setup are gathered by Mobile Manager. For the install operation this manager sends the application name, signature and 'manifest' file to the Application Manager where they are verified. For the update operation the new manifest file and the old manifest file are sent to be compared and verified. The results are sent back to Mobile Manager.

### *4.1.2 Secure the Communication*

To secure the exchange of data between parts of an application running on the mobile device and in Cloud, the reasoning based on LECCSAM because it offers a solution very flexible for the security management.

Security of data transmitted is done by the following managers: Mobile Security Manager and Cloud Security Manager. They receive parameters like: the security level needed and the data to secure. Each manager uses its Policy Manager to determine the security properties for the security level to be applied. In the case of data transmitted between the mobile device and the Cloud, the security managers receive data from Mobile Manager. In Cloud, application components communicate directly with the Cloud Security Manager.

Mobile Manager keeps the information about user options regarding the data security level for the applications installed. It receives the information regarding user context, mobile battery level, and network availability from the Optimization Manager. It also intercepts the data that has to be transmitted to Cloud; for each data transmitted is defined a sensibility level. Optimization Manager monitors the user context, battery level and network availability. These parameters may change frequently, so whenever there is a change the information is sent to the Mobile Manager [1].

## 4.2 A Private Cloud and File Characteristic-Based Framework for Mobile Security (PCFC) [3]

### *4.2.1 Limitations of Current Cloud Based Mobile Security*

1) Internet Connectivity and its bandwidth. The third generation of telecommunication has brought us wide area wireless services such as mobile TV and video call. Assume that one user has been cut off from Internet connection because of some reasons - who knows what these reasons may be. Apparently, without a cloud server, it is like a powerful computer without electricity - looks great, but useless.

2) Privacy and Security Paradox. We aim at securing our mobile devices and send out files to cloud for malware detection.

3) Burden issues. The traffic of data targeted at cloud server would certainly add to the network burden.

4) Economic concerns. The customers choose a payment of pay-as-you-use, and others pay a fixed amount of money monthly for unlimited access, invariably it follows a method of consume-more-pay-more. For this reason, the current cloud based mobile security, with high probability, will debit a user's bank account for this extra fee.

5) Timeliness. The minimal time delay in current mobile cloud is hard to be guaranteed, because of the reasons we discuss above.

### *4.2.2 The PCFC Framework for Mobile Security*

Due to those limitations of traditional cloud based mobile security, a new framework named PCFC (Private Cloud and File Characteristic Based) can be used. [3]

### *4.2.2.1 A High-Level Architecture*

A high-level architecture of PCFC is shown in figure 2. In which, a private cloud is connected directly or belongs to a core network (no matter it is a GSM, WCDMA, CDMA2000, or TD-SCDMA system), while a traditional mobile cloud is deployed over Internet. The main characteristics of this framework are shown below.

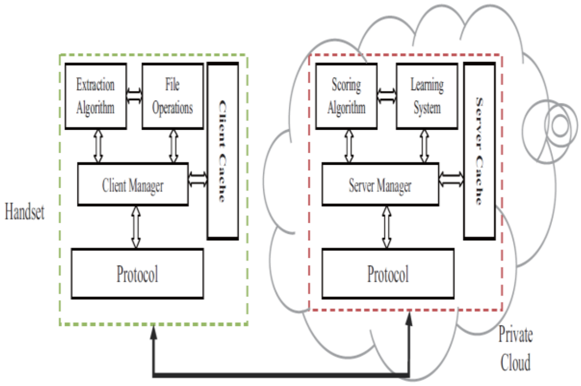

**Fig 2: High Level Architecture of PCFC [3]**

1) Private cloud based. What has to be mentioned here is, "private" does not mean that the cloud server in PCFC should be absolutely isolated. Indeed, it is just an indicator of those clouds that belong or directly connected to a core network. So it is totally up to a mobile carrier how the implementation is going to be carried out.

2) File characteristic based. Instead of sending out to cloud an entire file for malware detection, PCFC advocates that only data regarded as the vital security characteristic of the file would be delivered.

In the case that one mobile user is unable to establish a valid Internet connection, his mobile device with PCFC adopted, however, will still be under protection – it do not need an Internet connection at all. And for the same reason, not only the data transmission speed between the mobile device and cloud server may be dramatically increased – in other words, the time interval between a "Request" and "Response" would be potentially reduced; but also the burden issues that we mentioned above would be eliminated – the cloud server is now comparatively isolated from the Internet, so no matter how large is the size of the data to be transmitted, it would not lead to any troubles that we worried before.

What is more exciting for a mobile user is that he will not be charged extra fee for getting his device fully protected. The file characteristic based method would further enhance the improvement. It certainly reduces the amount of data to be transmitted and processed and, what is more important, to protect the privacy of the mobile user, which is then double-guaranteed by Encryption related techniques.

### *4.2.2.2 Main Components*

A PCFC system includes at least three major components, namely mobile client, private cloud service, and PCFC protocols. The details are discussed below.

#### *4.2.2.2.1 Mobile Client*

A PCFC mobile client is a lightweight APP run on handset. Illustrated in figure 3, it is made up of four sub-components. During these four, the client manager is the coordinator of them; And under the control of client manager, an extraction algorithm is used to mine useful data from those files protected– certainly, this goal should be achieved by interacting with the component of file operations, which provides all those interfaces for, e.g., opening, accessing, or even deleting a file (in the case it has been marked as dangerous). Besides these three, the cache part provides an easy way to check, if a file to be processed has been scanned before.

#### *4.2.2.2.2 Cloud Service*

The sub-components of private cloud service are also shown in the figure 3 (on the right side of the figure, while the left side is mobile client). Similar as the mobile client, the manager in server takes charge of scheduling out how operations should be performed; and these operations are roughly classified as two types.

1) Scoring process. This is done by both the server manager and scoring algorithm. In detail, the scoring algorithm provides a way of how the data received from a mobile client should be analyzed, and a score will finally be given to indicate the risk severity of the file.

2) Learning process. The learning system aims at training the scoring algorithm if needed. Since there is not a fixed principle to determine whether or not a file scanned is malicious, we have to refresh the scoring algorithm from time to time, with various training sets.

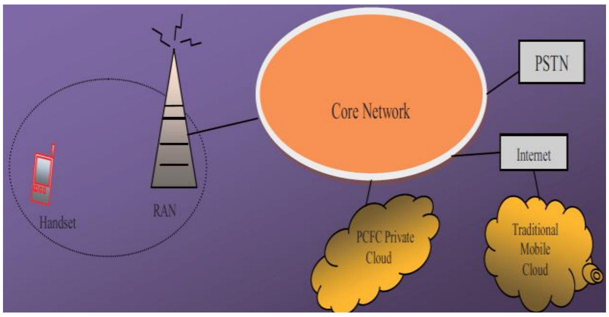

**Fig 3: Main Components of PCFC [3]**

#### *4.2.2.2.3 Protocol*

The protocol component is offered with the purpose of establishing a secure and stable connection between mobile client and cloud server, based on which data can be transmitted, and negotiations can be carried out before operation begins (e.g. what scoring algorithm should be used, what data content of a file should be extracted and sent out).

In detail, it consists of three phases (see the figure 4, in which {m}k denotes a message encrypted with key k; KPc means RSA Public key of Client; KPs means RSA Public key of Server and Kdh is the key of DH algorithm).

1) Handshake phase. It is a simple step to verify if both the client and server are ready for a further operation.

2) Authentication phase. This phase is secured with RSA algorithm. First step is to make sure that the cloud server the client is currently talking to is exactly the one as expected. To achieve this, a random number encrypted with the public key of the targeted server is sent out from the client, which should be the same with the number that the server sends back as a response – a fake server does not have a correct private key to decrypt the message containing the number, so it is unable to pass the authentication. The second step in this phase is to guarantee that the mobile client has a valid access to the cloud server. Those user id and password delivered from the client are verified by the server to check the validity of the access. Together with the authentication message, DH algorithm related parameters are also exchanged in this phase – DH algorithm is widely used to negotiate a symmetric key between two entities.

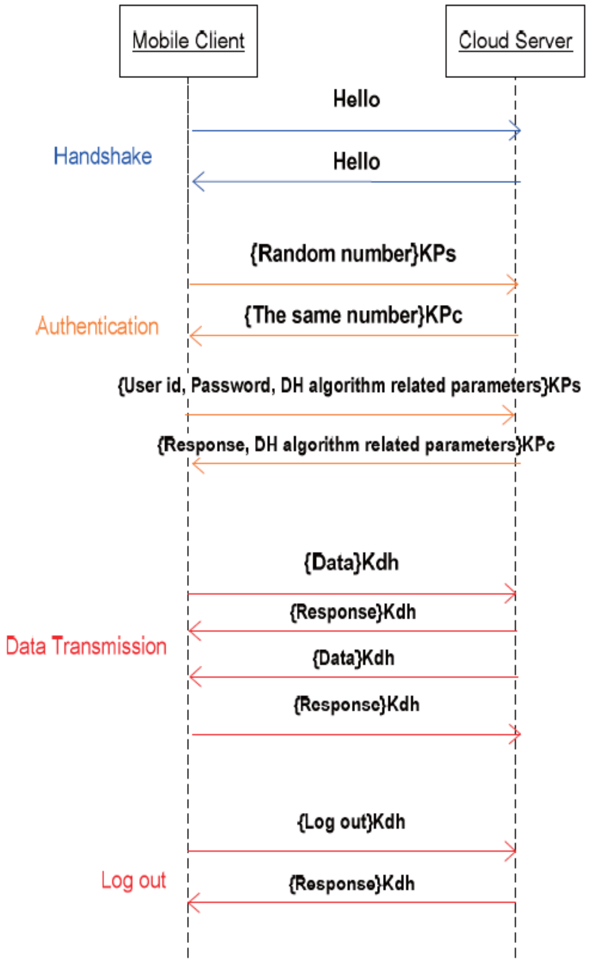

**Fig 4: Protocol of PCFC [3]**

3) Data transmission phase. After the last two phases, the client and server are now ready to receive data. All the data should be encrypted with the DH key, which has been negotiated in the authentication phase.

4) Log out phase. It indicates the client is trying to end the connection with the server. So that all the resources allocated before can be freed and then, both the client and server will return to standby state [3].

## 5. CONCLUSION

Mobile Cloud Computing introduces many security issues due to the fact that it combines mobile devices with Cloud services and because there is not a well-defined application model. The security issues are treated independently and the existing security solutions are supplied separately by various providers.

Secure Mobile-Cloud (SMC) framework aims to secure data communication between the same application components. The most important characteristics of our framework is that: 1) it allows applying different security properties to different kinds of data and not the same properties to all the data processed by the application, 2) the user preferences are taken into consideration and 3) the mobile device performances (e.g. energy consumption) are also taken into account. The framework provides also a solution to verify the integrity of an application. At the moment we are working to an approach to secure data transmitted between the Cloud components [1].

Following a general workflow of "Mobile device sends out suspicious files – Cloud server residing in Internet processes files – Result issued and sent back to mobile device", the Protocol Client Manager Extraction Algorithm File Operations Protocol Server Manager Scoring Algorithm Learning System Handset Private Cloud Client Cache Server Cache current cloud based mobile security frameworks have some limitations in common. In order to overcome those shortcomings, a new framework called as PCFC can be used [3].

## 6. REFERENCES

[1] Popa ,D. Cremene, M. Borda, M. Boudaoud, K. 2013. A security framework for mobile cloud applications. Roedunet International Conference (RoEduNet), 1-4.

[2] ZHOU Lian-chi, XIU Chun-di. 2012. Cloud Security Service Providing Schemes Based on Mobile Internet Framework. International Conference onComputer Science and Electronics Engineering (ICCSEE), 307-311.

[3] Xuesen Lin. 2011. Survey on Cloud Based Mobile Security and A New Framework for improvement. IEEE International Conference on Information and Automation (ICIA), 710-715.

[4] HuiSuo, Zhuohua Liu, Jiafu Wan, Keliang Zhou. 2013. Security and Privacy in Mobile Cloud Computing. 9th InternationalWireless Communications and Mobile Computing Conference (IWCMC), 655-659.

[5] Hoang, T. Dinh, Chonho Lee, DusitNiyato, and Ping Wang. 2011. A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches. Accepted in Wireless Communications and Mobile Computing – Wiley.

[6] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong. 2009. Securing Elastic Applications on Mobile Devices. In CCSW'09.

[7] M. Satyanarayanan. 2010. Mobile computing: the next decade. in Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS).

[8] Jon Oberheide, Evan Cooke, Farnam Jahanian. 2008. CloudAV: N-version antivirus in the network cloud. Proceedings of the 17th conference on Security symposium .

[9] ENISA. 2009. Cloud Computing Benefits, risks and recommendations for information security.