Security and Privacy in Mobile Cloud Computing

Hui Suo, Zhuohua Liu, Jiafu Wan*
Guangdong Jidian Polytechnic
Guangzhou 510515, China
*Corresponding author, jiafu_wan@ieee.org

Keliang Zhou
Jiangxi University of Science and Technology
Ganzhou 341000, China
nyzkl@sina.com

Abstract — **With the development of cloud computing and mobility, mobile cloud computing has emerged and become a focus of research. By the means of on-demand self-service and extendibility, it can offer the infrastructure, platform, and software services in a cloud to mobile users through the mobile network. Security and privacy are the key issues for mobile cloud computing applications, and still face some enormous challenges. In order to facilitate this emerging domain, we firstly in brief review the advantages and system model of mobile cloud computing, and then pay attention to the security and privacy in the mobile cloud computing. By deeply analyzing the security and privacy issues from three aspects: mobile terminal, mobile network and cloud, we give the current security and privacy approaches.**

Keywords: mobile cloud computing; security; privacy

I. Introduction

In recent years, cloud computing has been become the research focus for both academia and industry. By the means of on-demand self-service and extendibility, cloud computing provides a series of services such as IaaS (Infrastructure-as-a-Service), SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service) etc. So, it is known as a new generation of information technologies. Meanwhile, with the rapid development of mobile network and portable terminals, smart phones are more and more favored by users. It is becoming a trend to use mobile terminals to access the services provided by the cloud. Therefore mobile cloud computing is grown out of the above hot technologies: cloud computing and mobility [1].

Based on the concept of cloud computing, mobile cloud computing is defined as a model for providing various IT resources and information services over the mobile network by the means of on-demand self-service. Mobile cloud computing is the application of cloud computing in combination with mobile devices [3].

Recently mobile cloud computing is becoming more and more important in our life. According to the survey from Allied Business Intelligence, more than 2.4 billion users will use the mobile device to access the cloud computing service by 2015. And several companies have offered representative mobile cloud products. For example, Google offers some cloud-based products for consumers and enterprises. The primary product among them is the Android operating system for mobile devices. Besides Google has launched new application based on mobile terminal and cloud computing, e.g. geographic search and Google Maps, Google streets. Previously, Microsoft had introduced a program called the LiveMesh, which can integrate any PC running windows operating system, smart phones running windows mobile system and MAC-based Apple computers. Meanwhile LiveMesh is a platform including software and service. Through this platform, users can access and share their data and application. Apple Inc. launched iCloud in Oct. 2011. iCloud offers cloud storage and cloud data backup service for users from any Apple device [2, 4, 7, 8, 10, 12, 16-18].

When it comes to the current research status about mobile cloud computing technology, there are several research focuses at home and abroad as follows:

How to extend the battery life of mobile devices;
How to extend the limited resource of mobile devices;
How to solve the wireless bandwidth limited and delay;
How to ensure the security and privacy of mobile cloud computing.

In this article, we primarily discuss the security and privacy of mobile cloud computing. The rest of paper is organized as follows. In Section II we will pay attention to the advantages and system model of mobile cloud computing service. Section III shows the security and privacy issues of mobile cloud computing from three aspects. Section IV talks about the current approaches for the security and privacy issues in mobile cloud computing. Section V concludes the whole article.

II. Mobile Cloud Computing Applications

A. Advantages of Mobile Cloud Computing

Nowadays more and more users enjoy the internet services through mobile equipment such as smart phones and tablet PC. However in practice the storage capacity of mobile equipment is limited, so that the obtained resources are not rich; meanwhile compared with PC, mobile equipment calculation ability is limited; and battery's sustain ability and sharing data ability with PC are poor.

For these very reasons, mobile cloud computing emerges and will resolve these problems. The follows are the very advantages of the mobile cloud computing, shown as Table I.

978-1-4673-2480-9/13/$31.00 ©2013 IEEE

TABLE I. THE ADVANTAGES OF MOBILE CLOUD COMPUTING

	Disadvantages of mobile equipment	Advantages of mobile cloud Computing
1	Limited storage capacity	Breaking through the hardware limits
2	Limited calculation ability	
3	Poor battery's sustain ability	Intelligent balanced load
4	Poor sharing data ability with PC	Convenient access to data On-demand self-service

One is to break through the hardware limits. The mobile cloud computing enables the complex data processing and the massive data storage implemented in the cloud. So the burden of the calculation and storage on mobile equipment is reduced. The second is intelligent to balance load and to save electricity, so the mobile cloud computing can resolve the sustain problem of the battery and extend the battery life of mobile equipment. The third is convenient access to data. The forth is to reduce the management cost by the means of on-demand self-service.

B. Model of Mobile Cloud Computing

The typical model of the mobile cloud computing is shown as Figure 1, which is composed of three major components including mobile terminal, mobile network and cloud.

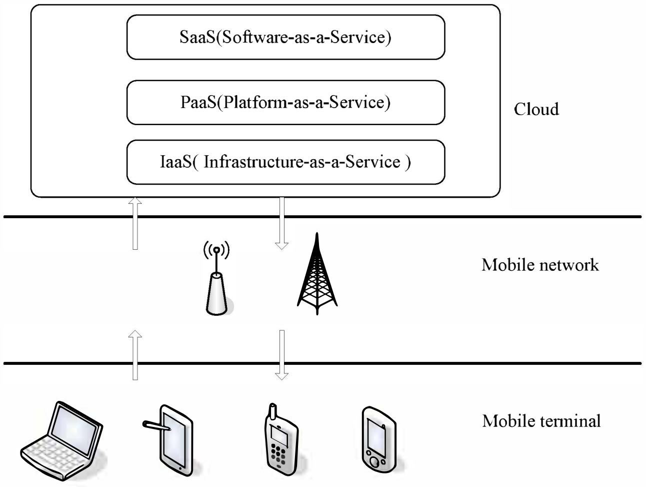
SaaS(Software-as-a-Service)
PaaS(Platform-as-a-Service)
IaaS(Infrastructure-as-a-Service)
Cloud
Mobile network
Mobile terminal

Figure 1. Model of mobile cloud computing

Mobile terminal refers to the mobile devices to access the cloud, such as smart phones, tablet PCs, notebook computers and PDAs. The cloud includes the infrastructure centers and servers providing the IT resource or information service, e.g. Infrastructure-as-a-Service (IaaS, including all kinds of servers, databases, storage devices, parallel and distributed computing systems), Software-as-a-Service (SaaS, including all kinds of software, data and information), Platform-as-a-Service (PaaS, including operation platform, support platform and development platform).

The mobile cloud computing provides service through the mobile network, so besides the mobile terminal and the cloud, the mobile network is necessary for reliable information transmission between the two.

In the process of mobile cloud computing application, above three aspects will all face the security and privacy issues. In the next section, we will discuss this question.

III. SECURITY AND PRIVACY ISSUES IN MOBILE CLOUD COMPUTING

A. Mobile Terminal

In general, mobile terminal has the following characteristics: the open operating system; supporting the third-party software; “personalization”; wireless access Internet anywhere and anytime. Just because of this, security issues in the mobile terminal are very serious. In the next, we will discuss them from the malware, software vulnerabilities and others.

1) Malware

Openness and versatility of the mobile terminal always draw the attackers’ attention. Some malware can be automatically download and carried, unknown to the user, along with useful programs and systems. By this means the malware get the illegal access to the personal information, even lead to flow increase and automatic pay without any operation of the user. Because of this the user of the mobile terminal will suffer from the economic damage or information leakage.

Aiming at the malware, some security vendors have developed the antivirus software for mobile terminals. But with the increasing of complexity of malicious attacks, anti-malware measures should provide the similar function with that of the desktop. In the meanwhile, the mobile terminals are capacity and resource limited which makes the anti-malware measures needing significant computation resource difficult to achieve. On the other hand, the malware can be spread among the mobile terminals in a variety of ways, e.g., USB interface, 3G network, Bluetooth or MMS attachments, which adds the difficulties to defect and prevent the malware.

Based on the above mentioned issues, we need to give the solutions for malware detection and prevention in the mobile terminals. And our solutions should balance the detection rate and resource consumption and software complexity.

2) Software Vulnerabilities

a) 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. As we all know, 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.

This is only one example of the software vulnerabilities. In fact the vulnerabilities of application software are very common. Because the application software itself is relatively not rigorous, so the attackers can intrude the mobile phone over the bug of the application software.

b) 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.

3) Others

Besides, security issues in the mobile terminal still come from the mobile users themselves. First of all, the mobile users are usually lack of security awareness; secondly the mobile users themselves also may mis-operate. So we need to detect and prevent anomalous behavior of users.

Because of above issues in mobile terminal, attacks can cause privacy leakage, information loss and devices damage through all kinds of attack methods, as shown in Figure 2.

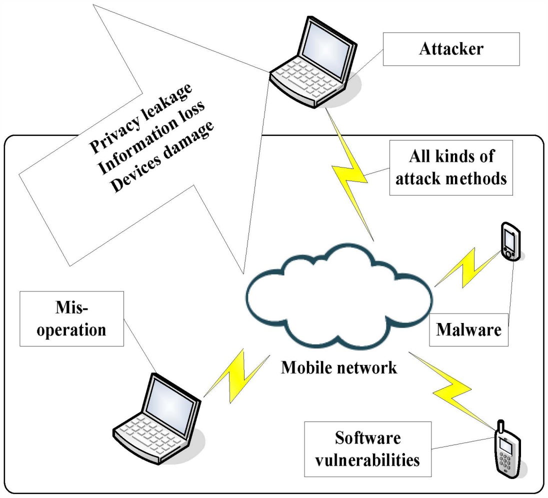

Figure 2. Mobile terminal security issues

B. Mobile Network Security

Based on the traditional network, mobile network expands the network node and the access way of users due to its mobility. The network node is extended to the mobile devices including smart phones, tablet PCs and so on; the mobile devices can access to the network in a large numbers of ways, for example users of smart phones can use phone service, Short Messaging Service (SMS) and other internet service through 3G networks. Besides, most smart phone also can access to the network through Wi-Fi and Bluetooth.

So broad access ways will bring more security threats such as the sensitive information leakage or malicious attack. For instance, various kinds of public place (such as Café, restaurant and airport, etc.) can provide free Wi-Fi, and many people will open a laptop and access Internet through free Wi-Fi. In this case, the potential information leakage will happen. Besides of this kind of public Wi-Fi, even the private Wi-Fi is also confronted with security risks, because the encryption mechanism of Wi-Fi is a weakness. Moreover the interaction between the mobile devices and the mobile cloud service providers also is frequent through different interfaces. This will cause more security risks too.

C. Mobile Cloud

1) Platform Reliability

The cloud platform is susceptible to being attacked because of its high concentration of information resources of users. On the one hand, the target of the malicious attacker is stealing valuable information or service. These attacks perhaps come from malicious outside, legal cloud computing user, or inside staff of the cloud computing operators. On the other hand, the target of the malicious attacker is to close the service of the cloud. For example, DOS (denial of service) attack will destroy the platform availability and close the service of the cloud. When users deliver all their data to the cloud service providers without selecting the expensive backup and disaster recovery service, they will be faced with the risks of the loss of data. In recent years, such events happened in the cloud providers now and again. So the cloud provider should integrate the current security technologies to ensure the service, and the users should not too depend on the cloud provider.

2) Data and Privacy Protection

The data security and privacy protection are the important issue in the mobile cloud. First of all, 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. [11]

To protect the sensitive data, the single means is not enough. We need a complete security solution to protect the data security and privacy of users.

IV. CURRENT SECURITY AND PRIVACY APPROACHES FOR MOBILE CLOUD COMPUTING

Now, according to the above issues, we will look into the current approaches for the security and privacy of the mobile cloud computing, and further detail on the control of the mobile terminal, the network access and transmission security, privacy protection, key management and encryption, access control, and so on.

A. *Aiming at Mobile Terminal Security*

1) Anti-malware

For the mobile terminal, there are two things to do aiming at malware. The one is to detect and remove the malware. To overcome the resource restriction of mobile terminals, we can move the malware detection to the cloud. By this way we can improve the detection rate and lower the resource consumption of the mobile terminals. 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. This legal software means it is authenticated and accredited, and it can be restored in the mobile terminal.

CloudAV is an exact example for anti-malware. CloudAV is a new model for malware detection on mobile terminal based on providing antivirus as an in-cloud network service. CloudAV provides several important benefits as follows: better detection of malicious software; eliminating the impact of antivirus vulnerabilities; retrospective detection of previously infected hosts; enhanced forensics capabilities; improved deploy ability and management. And it includes cross-platform host agent and a network service with ten antivirus engines and two behavioral detection engines, which greatly improves the detection rate [5-6, 9].

The other is prevention to malware. To prevent the mobile devices from being installed malware, the users should be careful of their behaviors. This will be discussed in detail in the following section of users' behavior.

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.

On the other hand, to reduce the software vulnerabilities, we should adopt a series of technical measures. For example, checking the software legitimacy and integrity is the important procedure before the software is applied.

3) Regulating Users' 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. For example, don't click the unexplained links; be careful of receiving the data transmission from strange phone; avoid install new unauthorized software; shut down the interface of Bluetooth or Wi-Fi etc. so that the transmission possibility of the malware will be reduced; and so on.

B. *Aiming at Mobile Network Security*

Now we will discuss how to protect the mobile network security from two aspects. The one is data encryption. Because only encrypted information is relativly secure during the transmission over the mobile network, in no matter which way the mobile terminals access the mobile network. The other is the security protocol. For all kinds of access ways, researching the security protocol is the core to reduce various attacks.

C. *Aiming at Mobile Cloud Security*

1) Protection to Platform Reliability

The reliability and availability of the mobile cloud computing platform are significant for both of the cloud providers and users. 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. By these means the cloud platform can improve the quality of service and increase the users' confidence.

2) Data Encryption and Key Management

The sensitive data need encryption technology in the survival period from storage to transmission. 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. The current research on the cipher text processing is the privacy homomorphism algorithm. Meanwhile key management is another important work for enterprise users.

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. By this way we can research a desired user-centric identity management mechanism for mobile clouds [13]. The other is behavioral authentication in which we can identify users by their habits and behavior such as memorized data, their belongings. Through this implicit authentication we can reduce a risk of fraud in mobile cloud.

When users finish the data transmission to the cloud, the access control will play a direct role. Now there are two kinds of access control mechanism. One is to assign the access permission to a level of account, and all the tenants share this delegated account. The other is to pre-assign the access permissions to the associated tenant accounts using the Access Control List (ACL) mechanism [14, 15].

4) *Privacy Protection*

So far, to protect the data privacy, the governments from all over the world have already developed the protection plan and strategy. For example, the British government introduced the Data Protection Act in 1998, and the European Union issued European Union data protection directive in 1995, and so on. On the other hand, technology methods have always played important roles in privacy protection. P3P (Platform for Privacy Preferences) is a very example, which is announced by the WWW consortium as an electronic agreement on personal data privacy protection between the network service providers. Now the 40% of the top 100 global internet sites are in use or plan to use P3P technology that is also recommended by some scholars.

To sum it up, the current approaches for the security and privacy of the mobile cloud computing are shown as Table II.

TABLE II. SECURITY ISSUES AND CORRESPONDING CURRENT APPROACHES

Security issues		**Current approaches**
Mobile terminal	Malware software	Detection and prevention CloudAV
	Software vulnerabilities (application software; operating system)	Installing the system patches Checking the software legitimacy and integrity
	Others(lack of security awareness, mis-operation)	Regulating the users' behavior
Mobile network	Information leakage or Malicious attack	Data encryption
		Security protocol
Mobile cloud	Platform reliability	Integrating the current security technologies; Key management and data encryption; Authentication and access control Privacy and data protection
	Data and privacy protection	

V. CONCLUSIONS

Recently, the mobile cloud computing is becoming a new hot technology. And the security solution for it has become a research focus. With the development of the mobile cloud computing, new security issues will happen, which needs more security approaches. In this article, we concisely reviewed advantages and models of mobile cloud computing, and analyzed security and privacy issues from three layers, which are mobile terminal, mobile network and mobile cloud. Then, according to the issues we gave the current approaches such as anti-malware, privacy protection, key management and encryption, access control, and so on.

ACKNOWLEDGMENT

The authors would like to thank the National Natural Science Foundation of China (No. 61262013), the Natural Science Foundation of Guangdong Province, China (No. S2011010001155), and the High-level Talent Project for Universities, Guangdong Province, China (No. 431, YueCai Jiao 2011) for their support in this research.

REFERENCES

[1] CSA(cloud security alliance), "security guidance for critical areas of focus in cloud computing," http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011.

[2] M. Chen, "AMVSC: a framework of adaptive mobile video streaming in the cloud," in Proc. of IEEE Globecom 2012, Anaheim, California, USA, Dec. 3-7, 2012.

[3] W. Song and X. Su, " Review of mobile cloud computing," in Proc. of 2011 IEEE 3rd International Conf. on Communication Software and Networks (ICCSN), May 2011, pp. 1-4.

[4] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the internet of things: a review," in Proc. of 2012 Int. Conf. on Computer Science and Electronic Engineering, Hangzhou, China, March, 2012, pp. 648–651.

[5] J. Oberheide, E. Cooke and F. Jahanian, "CloudAV: N-Version antivirus in the network cloud," in Proc. of the 17th USENIX Security Symposium, July 2008.

[6] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in Proc. of Workshop on Virtualization in Mobile Computing (MobiVirt'08), June 2008.

[7] H. Suo, J. Wan, L. Huang and C. Zou, "Issues and challenges of wireless sensor networks localization in emerging applications," in Proc. of 2012 Int. Conf. on Computer Science and Electronic Engineering, Hangzhou, China, March, 2012, pp. 447–451.

[8] M. Chen, J. Wan and F. Li, "Machine-to-machine communications: architectures, standards, and applications," KSII Transactions on Internet and Information Systems, vol. 6, no. 2, pp. 480–497, Feb. 2012.

[9] J. Oberheide, E. Cooke and F. Jahanian, "Rethinking antivirus: executable analysis in the network cloud," USENIX Workshop on Hot Topics in Security (HotSec'07), August, 2007.

[10] P. Shu, F. Liu, H. Jin, M. Chen, F. Wen, Y. Qu and Bo Li, "eTime: energy-efficient transmission between cloud and mobile devices," in Proc. of IEEE INFOCOM 2013 - Mini Conference, Turin, Italy, Apr. 14-19, 2013.

[11] D. Feng, M. Zhang, Y. Zhang and Z. Xu, "Study on cloud computing security," Journal of Software , vol. 22, no. 1, 2011, pp. 71− 83.

[12] J. Wan, H. Yan, H. Suo and F. Li, "Advances in cyber-physical systems research," KSII Transactions on Internet and Information Systems, vol. 5, no. 11, Nov. 2011, pp. 1891–1908.

[13] X. Wang, M. Chen, T. Kwon, L. Yang and V. Leung, "AMES-Cloud: ramework of adaptive mobile video streaming and efficient social video sharing in the clouds," IEEE Transactions on Multimedia, 10.1109/TMM.2013.2239630, Feb. 2013.

[14] X. Tianyi, H. Dijiang, M. Deep and A. Shingo, "MobiCloud: a Geo-distributed mobile cloud computing platform," in Proc. of 8th International Conf. on Network and Service Management (CNSM), 2012.

[15] H. Takabi, B. James and D. JosHi, "Security and privacy challenges in cloud computing environments," IEEE Security and Privacy, vol. 8, no. 6, 2010, pp. 24-31.

[16] X. Nie and H. Suo, "Security in the cloud computing: a review," in Proc. of 2nd international Conf. on computer science and network technology. Changchuan, China, Dec. 2012, pp. 2145-2149.

[17] H. Suo, J. Wan, D. Li and C. Zou, "Energy management framework designed for autonomous electric vehicle with sensor networks navigation," in Proc. of the 12th IEEE Int. Conf. on Computer and Information Technology, Chengdu, China, October, 2012, pp. 914–920.

[18] M. Chen, S. Gonzalez, Y. Zhang and V. Leung, "Multi-agent itinerary planning for wireless sensor networks," Quality of Service in Heterogeneous Networks, vol. 22, pp. 584–597, 2009.