Security Issues in Mobile Cloud Computing

Preeti A. Aware
Department of Computer Engineering,
S.L.R.T.C.E.
University of Mumbai, India,

Vinayak Shinde
Head of Department
Department of Computer Engineering
S.L.R.T.C.E.
University of Mumbai, India

Anand Aware
Department of Computer Engineering,
V.B.Vartak Polytechnic,Vasai Road,
affiliated to MSBTE, India

Abstract- In recent years there is rapid development in the mobile applications and mobile device hence Cloud Computing has gained the momentum. As the use of mobile devices and applications is increased it is desirable to use on-demand infrastructure, provided by cloud computing rather than traditional. So emphasis is given to the concept of Mobile Cloud Computing (MCC). Enterprise can gain fast access to business applications or infrastructure resources, by simply tapping into the cloud. Security issues have started growing as more information is placed into the cloud by individuals and enterprises. Mobile cloud computing is a procedure in which mobile applications are constructed, powered and launched using cloud computing technology. In Mobile Cloud computing through mobile application we can store information regarding sender, data and receiver on cloud. As more and more information is being stored on cloud by client, the security issues have become the major concerns, so this paper highlights several security issues in mobile cloud computing.

Keywords – Mobile cloud computing , Security issues, Mobile computing, Cloud Computing.

I. INTRODUCTION

Mobile device, cloud computing and mobile internet are the three basic elements of mobile cloud computing. A mobile user gets a rich application delivered over the internet, powered by cloud-backed infrastructure with the help Mobile Cloud Computing. Security and protection are now a day's the top most popular concern for mobile user or any business. Mobile cloud computing refers to the ease of use of services (cloud computing) in a mobile environment. The mobile users are provided optimal service using cloud computing. In mobile cloud computing, powerful configuration like memory capabilities, CPU speed etc. are not required as all the data and complicated computing components can work in the clouds [2, 4]. When using Mobile cloud computing a client application is not required in the recipient phone, since cloud computing center is accessed using mobile browser from a remote web server. This is also referred to as MobiClo [3], a combination of MObile CLOud.

The main advantages of mobile cloud computing is as follows [8], Improving data storage capacity and processing power, Extending battery lifetime, Improving reliability and availability, Scalability, , Ease of Integration. Data storage and computing are done in the cloud instead of the mobile phones with the help of mobile cloud applications. Here we have enlisted possible benefits of Mobile Cloud Computing.

1. New technical functionalities like location-awareness that enables personalization of services can be done with the help of mobile clouds.
2. Mobile Cloud Computing helps to triumph over restrictions of mobile devices in scrupulous of the data storage and processing power.

3. Security for mobile devices can be achieved by centralized monitoring and maintenance of software using mobile cloud.
4. Mobile Cloud Operators can concurrently act as virtual network operators, and provide. software, data storage provide e-payment services, ,etc. as a service to the mobile users.

II. Related Work

Mobile Cloud Computing can be defined as a mixture of cloud computing and mobile web also it is the most accepted tool for mobile users to access services and applications on the Internet Shea [5]. A simple way to define a Mobile cloud computing is a structure where both the data processing and data storage is moved outside the mobile device. Computing power and data storage are moved away from the mobile device to the cloud using mobile cloud applications". Aepona [6] describes Mobile Cloud Computing as a new paradigm for mobile applications where storage and data processing are moved outside the mobile device to centralized and powerful computing platforms situated in clouds. With the help of the wireless connection based on web browser of the mobile devices these centralized applications can be accessed [7], [8] .

III. Mobile Cloud Computing Architecture

As shown in Fig. 1, Base stations (e.g., base transceiver station (BTS) connect mobile devices to the mobile networks, the mobile users are provided with the equivalent cloud services with the help of cloud and cloud controllers that process the requests. Mobile users' requests data (location ,ID etc.) are sent to the central processors that are linked to servers giving mobile network services. Mobile users can get services from Mobile network operators like AAA (for, authorization, authentication and accounting) depending on the subscribers' data stored in databases and home agent (HA) . Following which, the subscribers' requirements are send to a cloud via the Internet. The cloud controllers, process the requests of the mobile users to give equivalent cloud services.

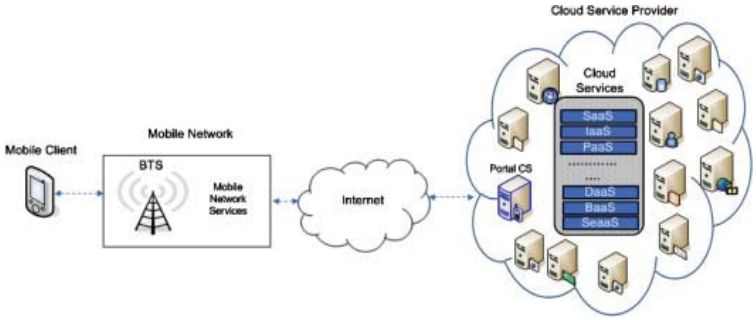

Figure 1. Mobile cloud computing architecture

IV. Issues in Mobile Cloud Computing

Issues in mobile cloud computing is broadly classify into 9 main category. Study of all issues of mobile cloud computing are given in table 1.

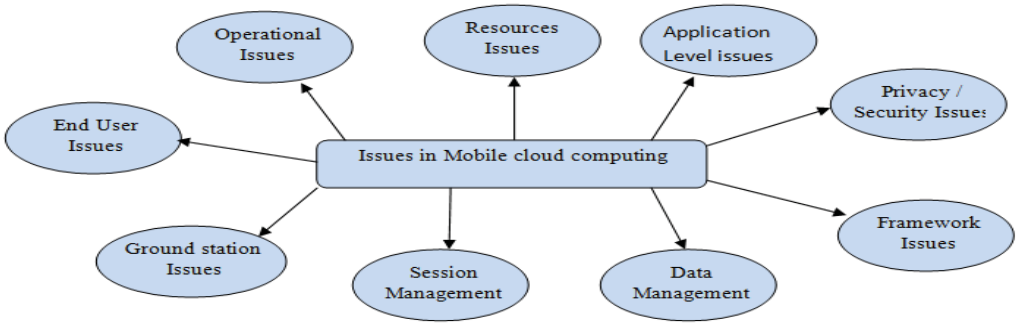

Figure 2. Issues in mobile cloud computing

Table 1: Study of all issues of mobile cloud computing

Sr. No	Type of Issues in mobile cloud computing	Methods under issue	Description about issue	Issues arise in particular type
1	Operational issue	Off loading method	Off loading job from mobile device to the cloud.	1. Physical distance from mobile device to the cloud. 2. Heterogeneity of the system being used.
		Cost benefit analysis	It determine resource usage e.g. energy and power consumption.	1. Mobility management 2. Connection protocol
2	Resources (Limited) Issues	-	Mobile computing devices are having very limited resources.	1. Battery Backup 2. Limited computing power
3	Application level issue	-	This type of issue is mainly concern with performance measurement of system and QOS.	1. Availability 2. Fault tolerance
4	Privacy, security and trust	1. General cloud security 2. Mobile cloud security	It mainly deals with problem of computation or data storage using cloud for mobile device	1. Low bandwidth 2. Availability 3. Heterogeneity
5	Framework consciousness issue	-	Provide information regarding user location, other users in surrounding area and resource in user's environment. Also use to provide information regarding resource availability and processing.	1.Context consciousness mobile application may not always behave in same way the user want due to - imperfect context information
6	Data management	-	Data can be access, stored and shared with external user or device	1.Data access 2. Data portability 3. Interoperability
7	Session Management	1.Session initiation 2.Session management 3.Session Termination	Maintaining session under continuous changing environment conditions is difficult	1. Session management 2. Data encryption / decryption
8.	Ground Station issues	Location of ground station	Ground station needs to be at every possible location so as to cover the entire area for maximum coverage.	1. Base station
9	End user issue	-	It describe regarding end user such as participating, interoperability and cost.	1. Incentives to collaborate 2. Presentation and usability issues.

V. SECURITY AND PRIVACY CLASSIFICATION

Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices.. Malicious codes are the major security threat faced by mobile devices . Due to GPS, privacy is a major concern for subscribers. Security of mobile cloud computing is sub-divided into two main categories security modules and privacy modules. Security module mainly concerned with security for cloud and security of mobile network . By using, access control authentication and malware detection the device can be secured,and this is done by the security module . Privacy module determines user data encryption/decryption and sensitive data management model, as shown in fig.3. Now we will see the concept of general cloud security, mobile cloud security and privacy in detail.

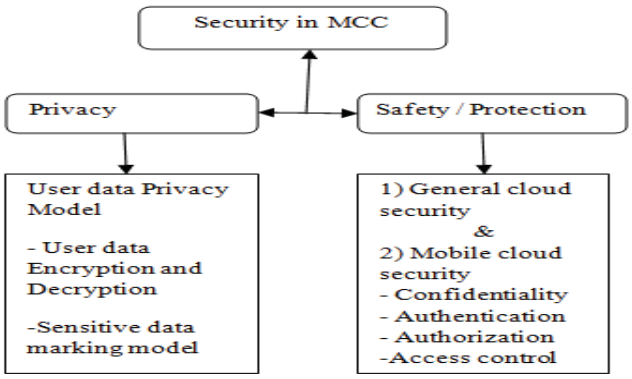

Figure 3. Mobile cloud computing Privacy and Safety classification

A) Security in Mobile Cloud Computing

Security for mobile application, one way to protect the device from threat is by installing and running security software .Mobile devices are resource controlled, protecting them from the threats is very difficult Oberheide et al [9].show a method to move to the clouds for detection of threat. It is an extension of the CloudAV platform comprising of network service and host agent. File activity on a system is scrutinized by Host agent running on mobile devices . If an particular file is absent in a cache of previously scrutinized files, then the file is transferred to the include network service for verification.

B) General cloud security:

J. Brodkin, Gartner [19] summarizes seven security risks that users need to consider in mobile Cloud computing;

1. Regulatory compliance: the cloud service providers should be ready to endure to external audits and security accreditations
2. Privileged user access: uploading sensitive data to the cloud would increase the problem of loss of direct physical and personnel control over the data.
3. Data location: the exact physical location of user's data is not transparent, which may lead to confusion on specific authorities and obligations on local privacy requirements.
4. Long-term viability: even if the cloud company itself goes out of business there should be assurance that user's data would be safe and accessible

C) Mobile cloud security:

The basic way to detect security threats will be installing and running security software and antivirus programs on mobile devices. But since mobile devices have processing and power limitations, protecting them from these threats could be more challenging compared to regular computers. Several approaches have been developed moving threat detection and security mechanisms to the cloud. Before a particular applications is used by a mobile, it should go through some level of threat assessment. All file activities to be sent to mobile devices will be tested if it is malicious or not. Instead of running anti-virus software or threat detection programs locally, mobile devices only performs trivial activities such as execution traces transmitted to cloud security servers. Security in mobile cloud computing, between user and mobile device is determined by three main parts malware detection authentication, and access control. To make the secure communication between mobile device and cloud, X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, S. Jeong,[20] propose the protection of resilient applications on mobile devices for cloud computing, named as 'weblet'.' Weblet' is use to migrate the data/information to and from mobile device and cloud. So as far as security concern, it include 3 main parts, they are explain as follows.

1. Authorization for weblets that could be executing on somewhat unreliable cloud environments to access sensitive user data.
2. Authentication between the 'weblets' that would be distributed between the device and the cloud,
3. Establishment and verification of reliable 'weblet' execution of cloud nodes.

VI. NEED OF PROTECTION AND ISSUES IN PROTECTION

So with the help of above discussion we conclude that, resource limitation is the most significant issue for mobile devices, such as less memory capacity, small screen size, and limited battery power as compared with desktop computers. Because of the resource limitation, the mobile cloud is most often regarded as a *SaaS cloud*, which

means that data handling and computation are typically performed in the cloud. E.g. Smart phones which often uses web browser to access the cloud.
Other reasons which affect the mobile cloud is bandwidth and latency. To improve the latency we can use Wi-Fi but it may decrease bandwidth when numerous mobile devices are present. Similarly, connectivity might be irregular. As providers of cellular construct their networks, the conditions will get better, but dead spots might still be present. We observe that application security has become a primary protection concern for mobile users, as mobile devices usually carry highly sensitive personal information. Compared to traditional desktop, if we are downloading some application from cloud, we can be able to provide security in terms of, virus and malware detection, and information leak detection. These can be possible by just installing antivirus for the desktop, but this is not possible for mobile device because of above mention problems such as less memory capacity limited battery, small screen size,. To overcome this problem [22] COSMOS that is Cloud Orchestrated Services for MObile Security, this infrastructure is use to support heterogeneous devices in terms of both platforms and architectures, for securing mobile applications. In this context, the cloud computing paradigm can be force to unload security-oriented functions from the devices to the cloud infrastructure. Furthermore, mobile applications can be encapsulated in a virtual environment in the cloud, and transparently accessed by mobile users through a remote connection.

VII. CONCLUSION

Mobile cloud computing is consisting of 3 main parts they are mobile device, mobile internet and cloud computing. Mobile cloud computing use to provide best possible services for mobile users.
Cloud computing is integrated with the mobile environment with the help of Mobile Cloud Computing . This overpowers disadvantage of the mobile device related to the performance such as storage, battery life, bandwidth, environment such as heterogeneity, scalability, and availability, and security issues such as privacy discussed in mobile computing.

REFERENCES

[1] http://andromida.hubpages.com/hub/cloud-computing-architecture.

[2] http://www.mobilecloudcomputingforum.com/

[3] MobiCloud: Building Secure Cloud Framework for Mobile Computing And Communication, 2010 Fifth IEEE International Symposium on Service Oriented System Engineering.

[4] http://www.readwriteweb.com/archives/why_cloud_computing_is_the_future_of_mobile.php.

[5] White Paper, "Mobile Cloud Computing Solution Brief," AEPONA, November 2010.

[6] SDSM: A Secure Data Service Mechanism in Mobile Cloud Computing 978-1-4577-0248-8/11/$26.00 ©2011 IEEE

[7] Jacson H. Christensen, "Using RESTful web-services and cloud computing to create next generation mobile applications," in Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications (OOPSLA), pp. 627-634, October 2009.

[8] A Survey of Mobile Cloud Computing:Architecture, Applications, and Approaches by Hoang T. Dinh, Chonho Lee, Dusit Niyato.

[9] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian. "Virtualized in-cloud security services for mobile devices," in Proc 1st Workshop on Virtualization in Mobile Computing (MobiVirt), pp. 31-35, June 2008.

[10] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid Android: versatile protection for smartphones," in Proc 26th Annual Computer Security Application Conference (ACSAC), pp. 347-356, September 2010.

[11] H. Zhangwei and X. Mingjun, "A Distributed Spatial Cloaking Protocol for Location Privacy," in Proc 2nd Intl Conf on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468, June 2010.

[12] W. Itani, A. Kayssi, and A. Chehab, "Energy-efficient incremental integrity for securing storage in mobile cloud computing," International Conference on Energy Aware Computing (ICEAC), pp. 1, January 2011.

[13] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, "Authentication in the clouds: a framework and its application to mobile users," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW), pp. 1-6, 2010.

[14] Mobile cloud computing: A survey Niroshinie Fernando , Seng W. Loke , Wenny Rahayu Department of Computer Science and Computer Engineering, La Trobe University, Australia

[15] E. Walker, W. Brisken, J. Romney, To lease or not to lease from storage clouds, Computer 43 (2010) 44–50

[16] X. Jin and Y. K. Kwok, "Cloud Assisted P2P Media Streaming for Bandwidth Constrained Mobile Subscribers," in Proceedings of the 16th IEEE International Conference on Parallel and Distributed Systems (ICPADS), pp. 800, January 2011.

[17] G. Huerta-Canepa and D. Lee, "A virtual cloud computing provider for mobile devices," in Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS), no. 6, 2010

[18] A. Klein, C. Mannweiler, J. Schneider, and D. Hans, "Access Schemes for Mobile Cloud Computing," in Proceedings of the 11th international Conference onMobile Data Management (MDM), pp. 387, June 2010

[19] J. Brodkin, Gartner: Seven cloud-computing security risks. http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853, 2008.

[20] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, S. Jeong, Securing elastic applications on mobile devices for cloud computing, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, CCSW'09, ACM, New York, NY, USA, 2009, pp. 127–134.

[21] M. Fahrmair, W. Sitou, B. Spanfelner, Security and privacy rights management for mobile and ubiquitous computing, in: Workshop on UbiComp Privacy, pp. 97–08

[22] http://crewman.uta.edu/projects/cloud-orchestrated-services-for-mobile-security