

A Survey on Challenges and Security Aspects of Mobile Cloud Computing

G.N.K.Suresh Babu¹, M.Kumarasamy²

¹Associate Professor-MCA, Acharya Institute of Technology, Bangalore

²Professor, Villa College, Male, Maldives

Abstract - Mobile Cloud Computing (MCC) integrates mobile computing and cloud computing and it becomes one of the frequently used term in software industries. Mobile cloud computing becomes part of mobile users daily life transactions. Mobile devices with Internet capabilities have increased the use of mobile clouding computing. Due to hardware limitations in mobile devices, these devices can't install and run applications require heavy CPU processing or extensive memory. Cloud computing allows mobile users to synchronize their data with remote storage and utilize applications require heavy CPU processing or extensive memory such as Microsoft Office or Adobe Photoshop, as they run in a desktop computer. Further, Mobile cloud computing refers to the incorporation of the elements of mobile networks and cloud computing that offers optimal services for mobile users. It offers on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The more and more information is placed into the cloud by individuals and enterprises, security issues begins to grow and raised. In this paper the author discusses the different security issues that arise about how safe the mobile cloud computing environment is.

Keywords: cloud computing, security, privacy, mobile cloud computing

I INTRODUCTION

The market of mobile phones has expanded rapidly. Mobility has become a very popular word and rapidly increasing part in today's computing area. An incredible growth has appeared in the development of mobile devices such as, smart phone, PDA, GPS Navigation and laptops with a variety of mobile computing, networking and security technologies. In addition, with the development of wireless technology like WiMax, Ad Hoc Network and WIFI, users may be surfing the Internet much easier but not limited by the cables as before. Thus, those mobile devices have been accepted by more and more people as their first choice of working and entertainment in their daily lives. More of us use our mobile phones as mini-computers that travel with us and keep us connected 24 hours a day, and that number will surely continue to grow. Mobiles are now integral part of business world and importance of mobile

database is inevitable. According to a new study from ABI Research has revealed that 'cloud computing' will completely transform future of mobile applications development, and their use. 'Cloud computing' will dramatically reduce the requirement of advanced handsets for running mobile applications, according to the study.

II OVERVIEW OF CLOUD COMPUTING

In the era of PC, many users found that the PCs they bought 2 years ago cannot keep pace with the development of software nowadays; they need a higher speed CPU, a larger capacity hard disk, and a higher performance Operation System (OS). That is the magic of 'Moore's Law' which urges user upgrading their PCs constantly, but never ever overtaken the development of techniques. Thus, a term called 'Cloud Computing' burst upon our lives. Cloud Computing has become a popular phrase since 2007. However, there is no consensual definition on what a Cloud Computing or Cloud Computing System is, due to dozens of developers and organizations described it from different perspectives. The author C. Hewitt introduces that the major function of a cloud computing system is storing data on the cloud servers, and uses of cache memory technology in the client to fetch the data. Those clients can be PCs, laptops, smart phones and so on. The author R. Buyya describes a definition from the perspective of marking that cloud computing is a parallel and distributed computing system, which is combined by a group of virtual machines with internal links. Such systems dynamically offer computing resources from service providers to customers according to their Service level Agreement (SLA). However, some authors mentioned that cloud computing was not a completely new concept. The author L. Youseff argue that cloud computing is just combined by many existent and few new concepts in many research fields, such as distributed and grid computing, Service-Oriented Architectures (SOA) and in virtualization. Figure 1 represents the cloud computing architecture.

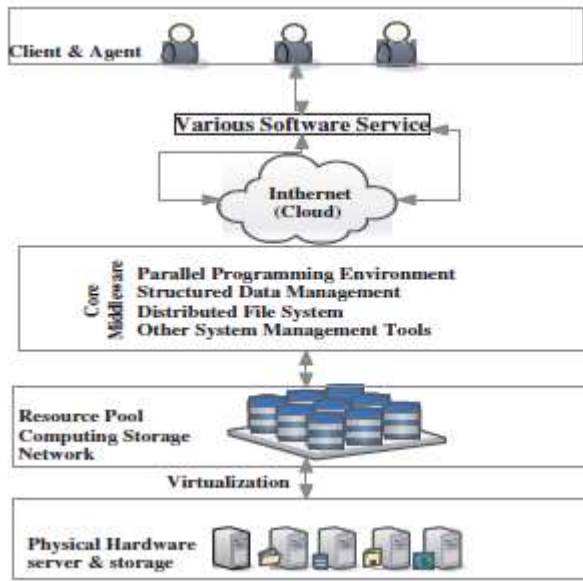


Fig.1 Cloud Computing Architecture

III OVERVIEW OF MCC

Cloud computing is called as ‘on demand computing’, ‘utility computing’ or ‘pay as you go computing’, the concept behind cloud computing is to offload computation to remote resource providers. The key strengths of cloud computing can be described in terms of the services offered by cloud service providers: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The concept of offloading data and computation in cloud computing is used to address the inherent problems in mobile. Mobile Cloud Computing Forum defines MCC as follows: “Mobile Cloud Computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smart phone users but a much broader range of mobile subscribers”. MCC can be described as a new paradigm for mobile applications whereby the data processing and storage are moved from the mobile device to powerful and centralized computing platforms located in clouds. These centralized applications are then accessed over the wireless connection based on a thin native client or web browser on the mobile devices. The mobile devices do not need a powerful configuration (e.g., CPU speed and memory capacity) since all the complicated computing modules can be processed in the clouds.

IV ARCHITECTURE OF MCC

Mobile devices are connected to the mobile networks via base stations that establish and control the connections and functional interfaces between the networks and mobile devices. Mobile users’ requests and information are transmitted to the central processors that are connected to servers providing mobile network services. The subscribers’ requests are delivered to a cloud through the Internet. In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services. Fig.2 represents architecture of mobile cloud computing.

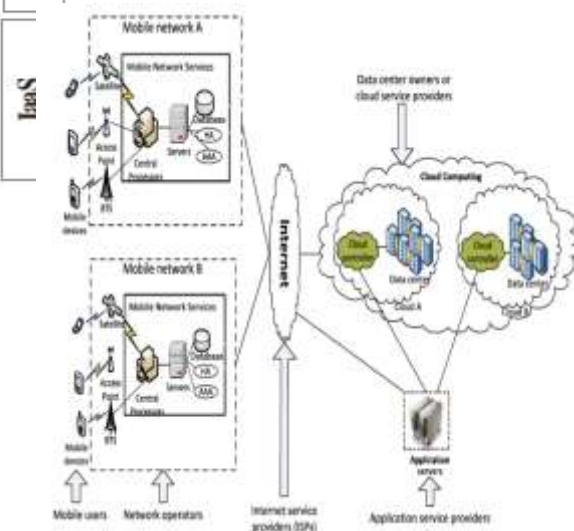


Fig.2 Mobile Cloud Computing Architecture

V LITERATURE REVIEW

Security and privacy issues of MCC have been discussed by many researchers. J. Oberheide et al. [12] proposed Cloud AV platform, malware detection system. In this architecture, mobile agent first analyses the malicious file. If its signature is not matched with the cached database, it is sent to the network service for analysis with the help of multiple detection engines running parallel on host machines with the help of virtualization technique. These techniques have the advantage of better detection of malicious software, reduced on device software complexity and power consumption but suffer from limitations of disconnected operation and accidental privacy hazard. S Zhang et al. [20] presents security framework which adapts mobile device with changing workloads, performance goals and network latency by migrating processing weblets between cloud and mobile device. They enhance this model by trustworthy weblets container, Authentication and secure session management, Authorization and access control of weblets, Logging and auditing

behaviour of weblets to make more secure framework. Although security during weblets migration can be improved by other security techniques and cloud environment can be made more trustworthy. Xiao and Gong [24] proposed lightweight algorithm for ensuring authorization in mobile cloud environment by generating automatic dynamic credential information with mutual coordination of mobile device and cloud so frequently that it is difficult for hackers to hack credential information of users. However frequent updation of secret information of user increases processing burden and energy consumption on mobile device and communication overhead between mobile and cloud. Wang and Wang [23] have proposed framework that uses cloud for providing number of live users in region based on historical data saved in cloud which helped in minimization of processing and communication overhead in cloud but doing spatial cloaking based on historical data can lead to privacy loss. The cloaking in mobile device increased processing overhead and energy consumption. Huang et al. [3] presents framework – MobiCloud in which the secure computation is done with three domains (a) cloud mobile and sensing domain (b) cloud trusted domain and (c) cloud public service and storage domain. Security to critical data is provided by isolating public cloud and trusted cloud. In this scheme client uses the services of two cloud service providers so it increases the communication cost and network latency. G. Portokalidis et al. [4] proposed scheme for threat detection in a smart phone based on CloudAV research by Oberheide et al. [10]. In cloud we have multiple replica of Smartphone which can detect different types of attacks in parallel. The proposed scheme reduced the transmission overhead below 2.5KiBps and reduced energy consumption 30%. In this technique cloud is considered fully trusted which needs to be given second thought.

VI SECURITIES AND CHALLENGES OF MCC

The main objective of mobile cloud computing is to provide a convenient and rapid method for users to access and receive data from the cloud, such convenient and rapid method means accessing cloud computing resources effectively by using mobile devices. The major challenge of mobile cloud computing comes from the characters of mobile devices and wireless networks, as well as their own restriction and limitation, and such challenge makes application designing, programming and deploying on mobile and distributed devices more complicated than on the fixed cloud devices. In mobile cloud computing environment, the limitations of mobile devices, quality of wireless communication, types of

application, and support from cloud computing to mobile are all important factors that affect assessing from cloud computing.

Security for Mobile Users: Mobile devices such as cellular phone, PDA, and smart phone are exposed to numerous security threats like malicious codes (e.g., virus, worm, and Trojan horses) and their vulnerability. In addition, with mobile phones integrated global positioning system (GPS) device, they can cause privacy issues for subscribers. Mobile devices today have all the functionalities of a standard computer. This, like for the standards computers, poses a security threat to the mobile devices as well. The threat detection services run on the mobile devices to combat these security threats, warrant intensive usage of resources, both in terms of computation and power. A possible solution is to move these detection services to the cloud. It saves the device CPU and memory requirements with increased bandwidth as the price to be paid. This approach has the following benefits:

- Better detection of malicious software
- Reduced on-device resource consumption
- Reduced on-device software complexity

Mobile Cloud Computing Security: Securing mobile cloud computing user's privacy and integrity of data or applications is one of the key issues most cloud providers are given attention. Since mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: Mobile network user's security; and cloud security.

Mobile Network User's Security: Numerous security vulnerabilities and threats such as malicious codes are known to the different mobile devices such as Smartphones, PDAs, cellular phones, laptops, and the like. Some applications to these devices can cause privacy issues for mobile users. There are two main issues concerning the subscriber's security.

Security for mobile applications: The simplest ways to detect security threats will be installing and running security software and antivirus programs on mobile devices. But since mobile devices are constrained with processing and power limitations, protecting them from these threats could be more difficult compared to regular computers. Several approaches have been developed transferring threat detection and security mechanisms to the cloud. Before mobile users could use a certain application, it should go through some level of threat evaluation. All file activities to be sent to mobile devices will be verified if it is malicious or not. Instead of running anti-virus software or threat detection programs locally, mobile devices only performs lightweight

activities such as execution traces transmitted to cloud security servers.

Privacy: Providing private information such as indicating your current location and user's important information creates scenarios for privacy issues. For example, the use of location based services (LBS) provided by global positioning system (GPS) devices. Threats for exposing private information could be minimized through selecting and analyzing the enterprise needs and require only specified services to be acquired and moved to the cloud. This leads to concerns that companies will use or sell this information as well as concerns that the information could be given to government agencies without the user's permission or knowledge.

Data Ownership: Another issue that arises from mobile cloud computing relates to the ownership of purchased digital media. With cloud computing it becomes possible to store purchased media files, such as audio, video or e-books remotely rather than locally. This can lead concerns regarding the true ownership of the data. If a user purchases media using a given service and the media itself is stored remotely there is a risk of losing access to the purchased media.

Data Access and Security: Related issues of access and security are significant to applications that rely on remote data storage and internet access in order to function. For example a user stores all of their calendar and contact information online, power outages can affect their ability to function from day to day. Mobile cloud computing is vulnerable due to multiple points at which access can be interrupted. Reception and high speed availability can vary greatly for mobile devices utilized by the users. Fig.3 represents the overview of challenges faced by mobile cloud computing.

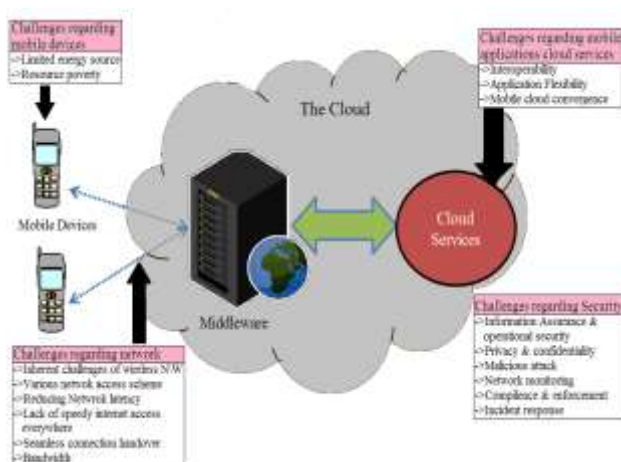


Fig.3 – challenges of mobile cloud computing

VII APPLICATIONS OF MOBILE CLOUD COMPUTING

Mobile applications gain increasing share in a global mobile market. Various mobile applications have taken the advantages of MCC. In this section, some typical MCC applications are introduced.

Mobile Commerce: Mobile commerce (m-commerce) is a business model for commerce using mobile devices. The mcommerce applications generally fulfill some tasks that require mobility (e.g., mobile transactions and payments, mobile messaging, and mobile ticketing). The m-commerce applications can be classified into a few classes including finance, advertising and shopping. The m-commerce applications have to face various challenges (e.g., low network bandwidth, high complexity of mobile device configurations, and security). Therefore, m-commerce applications are integrated into cloud computing environment to address these issues. Author proposes a 3G E-commerce platform based on cloud computing. This paradigm combines the advantages of both 3G network and cloud computing to increase data processing speed and security level based on PKI (public key infrastructure). The PKI mechanism uses an encryption-based access control and an over-encryption to ensure privacy of user's access to the outsourced data.

Mobile Learning: Mobile learning (m-learning) is designed based on electronic learning (e-learning) and mobility. However, traditional m-learning applications have limitations in terms of high cost of devices and network, low network transmission rate, and limited educational resources. Cloud-based m-learning applications are introduced to solve these limitations. For example, utilizing a cloud with the large storage capacity and powerful processing ability, the applications provide learners with much richer services in terms of data (information) size, faster processing speed, and longer battery life. Benefits of combining m-learning and cloud computing to enhance the communication quality between students and teachers. In this case, smartphone software based on the open source JavaME UI framework and Jaber for clients is used. Through a web site built on Google Apps Engine, students communicate with their teachers at anytime. Also, the teachers can obtain the information about student's knowledge level of the course and can answer students' questions in a timely manner.

Mobile Healthcare: The purpose of applying MCC in medical applications is to minimize the limitations of traditional medical treatment. Mobile healthcare

(m-healthcare) provides mobile users with convenient helps to access resources (e.g., patient health records) easily and quickly. Besides, m-healthcare offers hospitals and healthcare organizations a variety of on-demand services on clouds rather than owning standalone applications on local servers. There are a few schemes of MCC applications in healthcare. Author presents five main mobile healthcare applications in the pervasive environment.

- Comprehensive health monitoring services enable patients to be monitored at anytime and anywhere through broadband wireless communications.
- Intelligent emergency management system can manage and coordinate the fleet of emergency vehicles effectively and in time when receiving calls from accidents or incidents.
- Health-aware mobile devices detect pulse-rate, blood pressure, and level of alcohol to alert healthcare emergency system.
- Pervasive access to healthcare information allows patients or healthcare providers to access the current and past medical information.
- Pervasive lifestyle incentive management can be used to pay healthcare expenses and manage other related charges automatically.

VIII CONCLUSION

In this paper the author discussed some points about cloud computing and security challenges of mobile cloud computing. Mobile cloud computing is one of mobile technology trends in the future since it combines the advantages of both mobile computing and cloud computing, thereby providing optimal services for mobile users. Mobile Cloud Computing, as a development and extension of Cloud Computing and Mobile Computing, is the most emerging and well accepted technology with fast growth. The combination of cloud computing, wireless communication infrastructure, portable computing devices, location-based services, mobile Web etc has laid the foundation for the novel computing model. In this paper the author has given an overview of Mobile Cloud Computing that includes architecture, benefits, key challenges, present research and open issues. With the high increasing of data computation in commerce and science, the capacity of data processing has been considered as a strategic resource in many countries. Mobile cloud computing (MCC), as a development and extension of mobile computing (MC) and cloud computing (CC), has inherited the high mobility and scalability, and become a hot research topic in recent years. The author concludes that there are three main optimization approaches in MCC, which are focusing

on the limitations of mobile devices, quality of communication, and division of applications services. Firstly, using virtualization and image technology can address it effectively, and immigrate task from terminal to cloud is also a good way to achieve better results. Secondly, as we know the quality of communication in wired network is better than in wireless network, so reducing the proportion of data delivery in wireless environment is an effective way to improve the quality. In addition, upgrading bandwidth is envisaged to be a simple way to increase performance but it incurs additional cost to users. Deploying an effective elastic application division mechanism is deemed to be the best solution to guarantee the application service in Mobile cloud computing.

REFERENCES

- [1] Chetan S., Gautam Kumar, K. Dinesh, Mathew K. and Abhimanyu M.A., "Cloud Computing for Mobile World," 2010. (<http://chetan.ueuo.com/projects/CCMW.pdf>)
- [2] C. Hewitt, "Orgs for scalable, robust, privacy-friendly client cloud computing," *Internet Computing, IEEE*, vol. 12, no. 5, pp. 96–99, 2008.
- [3] D. Huang, X. Zhang, M. Kang and J. Luo, "MobiCloud: building secure cloud framework for mobile computing and communication," in Proceeding 5th IEEE International Symposium on Service Oriented System Engineering, SOSE '10, Nanjing, China, June 2010.
- [4] G. Portokalidis, P. Homburg, K. Anagnostakis and H. Bos, "Paranoid Android: versatile protection for smartphones," in Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), September 2010, pp. 347-356.
- [5] Han Qi, Abdullah Gani, "Research on Mobile Cloud Computing: Review, Trend and Perspectives" in Proceedings of the Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP), IEEE, Pages 195-202, 2012
- [6] J. Hurwitz, R. Bloor, M. Kaufman, and F. Halper, *Cloud computing for dummies* vol. 1: For Dummies, 2009.
- [7] K. Kumar and Y. Lu, "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy," *IEEE Computer Society*, vol.43, no. 4, April 2010.
- [8] L. Liu, R. Moulic, and D. Shea, "Cloud Service Portal for Mobile Device Management," in Proceedings of IEEE 7th International Conference on e-Business Engineering (ICEBE), pp. 474, January 2011.
- [9] L. Youseff, M. Butrico, and D. Da Silva, "Toward a unified ontology of cloud computing," in *Grid Computing Environments Workshop, 2008.GCE'08*. IEEE, 2008, pp. 1–10.
- [10] Min Choi, Jonghyuk Park, Young-Sik Jeong, Springer Science, Business Media, LLC 2011, 'Mobile cloud computing framework for a pervasive and ubiquitous environment'.
- [11] M. Satyanarayanan, "Mobile computing: the next decade," in Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS), June 2010.

- [12] Oberheide, J., Veeraraghavan, K., Cooke, E. and Jahanian, F. 2008, Virtualized in-cloud security services for mobile devices. In Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt), 31-35.
- [13] Peter Schoo, et al. „Challenges for Cloud Networking Security“, <http://www.hpl.hp.com/techreports/2010/HPL-2010-137.pdf>.
- [14] Roger Collings, „Mobile Cloud Adoption Challenges in the Enterprise“; <http://cloudcomputingtopics.com/2012/04/mobile-cloud-adoption-challenges-in-the-enterprise>.
- [15] R. Buyya, C. Yeo, and S. Venugopal, “Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities,” in *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on*. IEEE, 2008, pp. 5–13.
- [16] S. Chetan, G. Kumar, K. Dinesh, K. Mathew, and M. Abhimanyu, “Cloud computing for mobile world,” available at chetan.ueuo.com.
- [17] Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, Anand Ghalsasi, “Cloud Computing – The business perspective”, *Decision Support Systems*, Volume 51, Issue 1, Pages 176-189, 2011
- [18] Sun Microsystems, Inc., “Introduction to Cloud Computing Architecture”, White Paper, 1st Edition, (2009) June.
- [19] S. Morrow, “Data Security in the Cloud”, *Cloud Computing: Principles and Paradigms*, Edited by Rajkumar Buyya, James Broberg and Andrzej Goscinski Copyright 2011 John Wiley & Sons, Inc., (2011) pp. 573-592.
- [20] S. Jeong, X. Zhang, A. Kunjithapatham, and S. Gibbs, “Towards an elastic application model for augmenting computing capabilities of mobile platforms,” *Mobile Wireless Middleware, Operating Systems, and Applications*, pp. 161–174, 2010.
- [21] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud security and privacy: an enterprise perspective on risks and compliance*: O'Reilly Media, Incorporated, 2009.
- [22] Toby Velte, Anthony Velte, Robert C. Elsenpeter, “Cloud Computing: A Practical Approach”, *Tata McGraw Hill Professional*, 2009
- [23] Wang, S. and S. Wang X., “In-device spatial cloaking for mobile user privacy assisted by the cloud”, in *Proceeding 11th International Conference on Mobile Data Management, MDM '10*, Missouri, USA, May 2010.
- [24] Xiao, S. and Gong, W., 2010. Mobility can help: protect user identity with dynamic credential. In *Proceeding 11th International Conference on Mobile Data Management, MDM '10*, Missouri, USA, May 2010.
- [25] Xiaopeng Fan, Jiannong Cao, and Haixia Mao. “A Survey of Mobile Cloud Computing,” *ZTE Communications*, 9(1):4-8, Mar 2011.