ISSN:0975-9646

Mobile Cloud Computing : Issues, Security,Advantages, Trends

Dhammapal Tayade
Research Student

Abstract :-Now days the market of mobile phone is growing at a very high speed. Every one has a mobile,tablet,fablet (tablet with calling facility).[1] Mobile user will reach 6.5 billion by the end of 2012,6.9 billion by the end of 2013.Together with an explosive growth of the mobile applications and emerging of cloud computing concept, mobile cloud computing (MCC) has been introduced to be a potential technology for mobile services. MCC integrates the cloud computing into the mobile environment and overcomes obstacles related to the performance (e.g., battery life, storage, and bandwidth), environment (e.g., heterogeneity, scalability, and availability), and security (e.g., reliability and privacy) discussed in mobile computing. This paper gives a information about mobile cloud computing application ,security, issues . The issues, existing solutions and approaches are presented.

Keywords-Mobile cloud computing, data storage, mobile user, security.

1. Introduction

Mobile devices (e.g., smartphone, tablet pcs, fablet etc) are increasingly becoming an essential part of human life as the most effective and convenient communication tools not bounded by time and place. Mobile users accumulate rich experience of various services from mobile applications (e.g., iPhone apps, Google apps, etc), which run on the devices and/or on remote servers via wireless networks. The rapid progress of mobile computing (MC) [1] becomes a powerful trend in the development of IT technology as well as commerce and industry fields. However, the mobile devices are facing many challenges in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., mobility and security) [2]. The limited resources significantly impede the improvement of service qualities. Cloud computing (CC) has been widely recognized as the next generation's computing infrastructure. CC offers some advantages by allowing users to use infrastructure (e.g., servers, networks, and storages), platforms (e.g., middleware services and operating systems), and softwares (e.g., application programs)

1.1. What is Mobile Cloud Computing?

The Mobile Cloud Computing Forum defines MCC as follows [4]:

"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 Smartphone users but a much broader range of mobile subscribers".

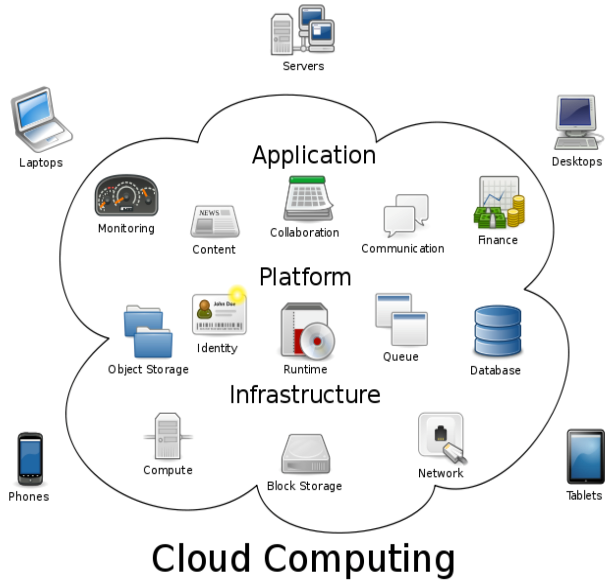

Fig.1:Cloud Computing

2. Advantages Of Mobile Cloud Computing

Cloud computing is known to be a promising solution for mobile computing due to many reasons (e.g., mobility, communication, and portability [13]). In the following, we describe how the cloud can be used to overcome obstacles in mobile computing, thereby pointing out advantages of MCC.

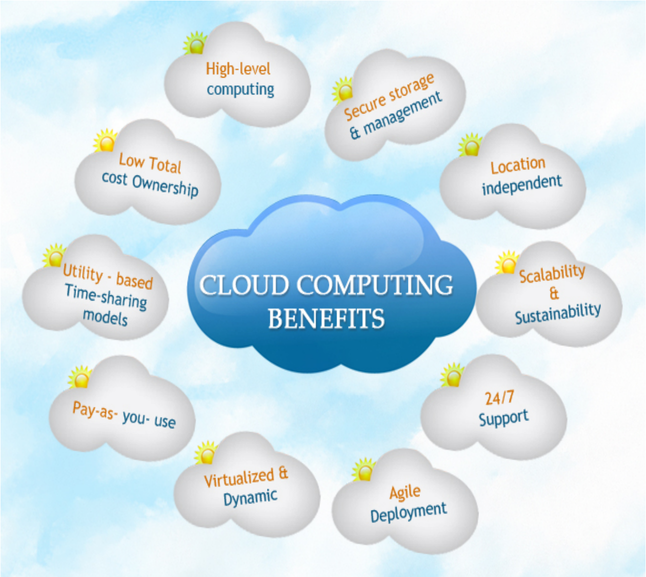

Fig.12 : Advantage of Cloud Computing

2.1 Extending battery lifetime: Battery is one of the main concerns for mobile devices. Several solutions have been proposed to enhance the CPU performance and to manage the disk and screen in an intelligent manner to reduce power consumption. However, these solutions require changes in the structure of mobile devices, or they require a new hardware that results in an increase of cost and may not be feasible for all mobile devices. Computation offloading technique is proposed with the objective to migrate the large computations and complex processing from resource-limited devices (i.e., mobile devices) to resourceful machines (i.e., servers in clouds). This avoids taking a long application execution time on mobile devices which results in large amount of power consumption. evaluate the effectiveness of offloading techniques through several experiments. The results demonstrate that the remote application execution can save energy significantly. Especially, [8] evaluates large-scale numerical computations and shows that up to 45% of energy consumption can be reduced for large matrix calculation. In addition, many mobile applications take advantages from task migration and remote processing. For example, offloading a compiler optimization for image processing [10] can reduce 41% for energy consumption of a mobile device. Also, using memory arithmetic unit and interface (MAUI) to migrate mobile game components [11] to servers in the cloud can save 27% of energy consumption for computer games and 45% for the chess game.

3. Issues In Mobile Cloud Computing

Cloud is extremely powerful to perform computations while computing ability of mobile devices has a limit so many issues occur to show how to balance the differences between these two. So there are some issues in implementing cloud computing for mobile. These issues can be related to limited resources, related to network, related to security of mobile users and clouds [4]. Some issues are explained as follows:

3.1 Limited Resources

Having limited resources in mobile device make use of cloud computing in mobile devices difficult. Basic limitations related to limited resources are limited computing power, limited battery and low quality display.

3.2 Network related issues

All processing in MCC is performed on the network. So there are some issues related to the network like Bandwidth, latency, availability and heterogeneity

3.3 Security

Most of mobile devices have almost same functionalities like a desktop computer. So mobile devices also have to face a number of problems related to security and privacy. To overcome this problem threat detection services are now performed at clouds but this also has to face a lot of challenges. Some security issues are like device security, privacy of mobile user and securing data on cloud etc.There are so many security threats like viruses, hacking, Trojan horses in mobile devices also. The use of global positioning system (GPS) in mobile devices gives birth to the privacy issues.

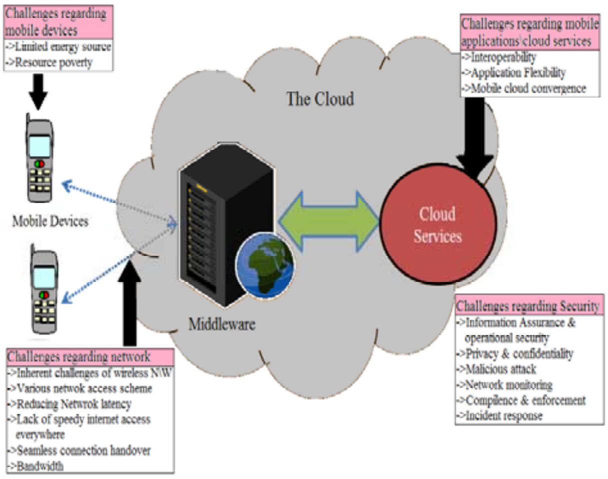
Challenges regarding mobile devices
->Limited energy source
->Resource poverty
Challenges regarding mobile applications\cloud services
->Interoperability
->Application Flexibility
->Mobile cloud convergence
The Cloud
Mobile Devices
Cloud Services
Middleware
Challenges regarding network
->Inherent challenges of wireless N\W
->Various netwok access scheme
->Reducing Netwrok latency
->Lack of speedy internet access everywhere
->Seamless connection handover
->Bandwidth
Challenges regarding Security
->Information Assurance & operational security
->Privacy & confidentiality
->Malicious attack
->Network monitoring
->Compilence & enforcement
->Incident response

Fig.3. Challenges regarding Implementation of Cloud Computing in Mobile Applications

3.4 Low Bandwidth: Bandwidth is one of the big issues in MCC since the radio resource for wireless networks is much scarce as compared with the traditional wired networks. A solution to share the limited bandwidth among mobile users who are located in the same area (e.g., a workplace, a station, and a stadium) and involved in the same content (e.g., a video file). The authors model the interaction among the users as a coalitional game. For example, the users form a coalition where each member is responsible for a part of video files (e.g., sounds, images, and captions) and transmits/exchanges it to other coalition members. This results in the improvement of the video quality. However, the proposed solution is only applied in the case when the users in a certain area are interested in the same contents. Also, it does not consider a distribution policy (e.g., who receives how much and which part of contents) which leads to a lack of fairness about each user's contribution to a coalition.considers the data distribution policy which determines when and how much portions of available bandwidth are shared among users from which networks (e.g., WiFi and WiMAX). It collects user profiles (e.g., calling profile, signal strength profile, and power profile) periodically and creates decision tables by using Markov Decision Process (MDP) algorithm. Based on the tables, the users decide whether or not to help other users download some contents that they cannot receive by themselves due to the bandwidth limitation, and how much it should help (e.g., 10% of contents). The authors build a framework, named RACE (Resource-Aware Collaborative Execution), on the cloud to take advantages of the computing resources for maintaining the user profiles. This approach is suitable for users who share the limited bandwidth, to balance the trade-off between benefits of the assistance and energy costs.

3.5 Availability: Service availability becomes more important issue in MCC than that in the cloud computing with wired networks. Mobile users may not be able to connect to the cloud to obtain service due to traffic congestion, network failures, and the out-of-signal.

4. Security In Mobile Cloud Computing

4.1 Security framework in Mobile Cloud Computing

Mobile cloud computing is growing day by day due to the popularity of cloud computing and increasing uses of mobile devices. Many researchers are showing their interest towards this technology. There are many issues in mobile cloud computing due to many limitations of mobile devices like low battery power, limited storage spaces, bandwidth etc. Security is the main concern in mobile cloud computing. Security in mobile cloud computing can be explained by broadly classifying it into 2 frameworks [5].

4.1.1 Security of data/files

The main issue in using mobile cloud computing is securing the data of mobile user stored on mobile cloud. The data/file of a mobile user is very sensitive; any unauthorized person can do changes in it, to harm the data. So the main concern of cloud service provider is to provide the security of data/files created and manipulated on a mobile device or cloud server. The data/file security is very essential for owner of the data/file as it can contain any confidential information of his.

4.1.2 Security of mobile applications or application models

Securing the mobile applications or application model is also important because these provide better services to mobile users by utilizing cloud resources. These mobile application models use the services of the cloud to increase the capability of a mobile device. In this paper we are going to discuss the security of data or files of mobile users stored on mobile cloud.

4.2 Why data storage security is needed

The data of owner is stored on the cloud server; once the data is stored the owner does not have that data on his own device. Thus, there is risk related to data security and confidentiality of the data. It is not accepted by the owner that his data/file is disclosed to someone who is not an authorized person. Before discussing why data security is needed there is a need to discuss the security threats to the data stored on the cloud. There are following security risk related to data stored on the cloud server.These attacks affect the data stored on the cloud. For owner the integrity of the data is very important. If any unauthorized person performs changes in data of other person then it can harm the integrity of the data. Any person after finding confidential information of other person can harm that person. So, data confidentiality is also a concern of data owner. Authentication of user is also important to verify who the originator of the file is.

5. Data Storage Security With Various Available Solutions

For the last few years Mobile Cloud Computing has been an active research field, as mobile cloud computing is in initial stage, limited surveys are available in various domain of MCC. In this paper our main focus is on securing the data storage in mobile cloud computing. Significant efforts have been devoted in research organizations to build secure mobile cloud computing. This paper explores the various methodologies for data security in Mobile Cloud Computing. Itani et Al. [6] proposed an Energy efficient framework for integrity verification of storage services using incremental cryptography and trusted computing. In this paper the authors provided a framework for mobile devices to provide data integrity for data stored in cloud server. Incremental cryptography has a property that when this algorithm is applied to a document, it is possible to quickly update the result of the algorithm for a modified document, rather than to re-compute it from scratch. In this system design three main entities are involved:Mobile User (MU): Mobile user/client is a person who utilizes the storage services provided by Cloud service provider (CSP).Cloud Service Provider (CSP): CSP provides storage services to client. CSP is also responsible for operating, managing and allocating cloud resources efficiently. Trusted Third Party (TTP): TTP installs coprocessors on remote cloud; who is associated with a number of registered mobile user/client. Coprocessor provides secretkey (SEK) to mobile user and is also responsible for generating message authentication code for mobile client.There are a number of operations involved in this scheme shown by

1) Updating File on the Cloud: Before uploading file on cloud, mobile user is required to generate an incremental Message Authentication Code (MAC file) using SEK. MACfile = $\sum$ HMAC (Filek , SEK). (1)Where, n is total logical partitions of file and Filek is kth part of the file. After generating MAC file, mobile client uploads the file on the cloud and stores MAC file on local storage.

2) Inserting or deleting a block: At any time mobile client can insert (delete) a data block in file stored on cloud server. For this client sends request to CSP, in its response CSP sends requested file to mobile client as well as to trusted coprocessor (TCO) associated with that client. TCO generates MACtco and sends it to client to match this MAC generated by TCO (MACtco) with MAC stored in client's local storage (MACfile). If these two MAC matches , the client can perform insertion/deletion in the file and again computes MACfile with help of old MACfile, SEK and inserted/deleted block. For avoiding communication overhead only updated block is uploaded on cloud server.3) Integrity Verification: At any time mobile client can verify the integrity of data stored on cloud server by sending request to cloud server, on receiving request cloud server sends file to TCO for integrity verification. TCO generates incremental authentication code and sends it to mobile client directly. Now mobile client compares this MACtco with stored MACfile to verify integrity. If these two matches then integrity is verified.

Where,

(1) MC generate MACfile and stores MACfile in local memory

(2) MC uploads file on server

(3) CSP stores file on cloud

(4) MC sends request to CSP for performing insertion/deletion in the file

(5a) CSP sends requested file to MC

(5b) CSP forwards requested file to TCO

(6) TCO sends MACtco to MC directly

(7) MC compares MACfile and MACtco for verifying integrity

(8) MC insert/delete a block in file and computes MAC for that block
(9)MC uploads updated block on cloud
(10) CSP stores updated file.

Jia et al. [7] provide a secure data service mechanism through Identity based proxy re-encryption. This mechanism provides confidentiality and fine grained access control for data stored in cloud by outsourcing data security management to mobile cloud in trusted way. The goal of this protocol is that only authorized persons/sharer can access the data while unauthorized sharer will learn nothing. Identity based encryption is that user encrypt the data through his identity (Id). This encryption scheme is based on bilinear pairing.

A bilinear map is e: G1 × G2 →GT where G1 and GT be cyclic multiplicative group with prime order q and g be generator of G1, having the properties of bilinearity, non degeneracy and computability. Proxy based re-encryption is used by mobile user to provide access control capability to cloud, which could grant access to an authorized users by transferring cipher text encrypted by data owner's identity to one with sharer's identity. In this mechanism 3 entities are involved: Data owner (DO), Data Sharer (DS) and Cloud Servers (CSs). Both DO and DS utilize data storage service to store and retrieve file. CSs provide services to mobile clients.

This protocol has following phases:

1) Setup Phase: Here system master key(SEK) and system parameters are generated, where SEK is private to data owner.

2) Key Generation Phase: In this phase decryption key corresponding to user's identity (dkid) is generated by following equation: dkid=H1(Id)s where, Id∈ {0,1}* , H1: {0,1}*→ G1 and s∈Zq is randomly selected.

3) Encryption Phase: Here file F is divided into k blocks such that F=(n1,n2……..nk), for each block ni data owner performs encryption by:Ni=(gr,n,e(gs,H1(ID)r)) (2)where, r∈Zp is randomly selected.After implementing encryption of F, mobile user uploads encrypted file (EF)=(N1,N2…………Nk) to cloud.

Zhou et Al. [9] proposed a scheme for efficient and secure data storage operations by introducing the concepts of Privacy Preserving Cipher text Policy Attribute Based Encryption (PP-CP-ABE) and Attribute Based Data Storage (ABDS) system. Through PP-CP-ABE lightweight devices can securely outsource encryption/decryption operations to Cloud Service Provider (CSP). The entities involved in this scheme are:Data Owner (DO): A DO can be a wireless mobile device or a sensor which uses the storage service of cloud.Trust Authority (TA): TA is responsible for distributing cryptographic keys and is very trusted.Encryption Service Provider (ESP): ESP encrypts the file of data owner without knowing the actual encryption key. In this scheme encryption operations are offloaded to ESP.Decryption Service Provider (DSP): DSP provides decryption service to data owner. DSP does not have any information about actual content.Storage Service Provider (SSP): SSP provides storage services to clients; before uploading file on cloud, file is encrypted by ESP.

6. CONCLUSION

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. The requirement of mobility in cloud computing gave birth to Mobile cloud computing. MCC provides more possibilities for access services in convenient manner. It is expected that after some years a number of mobile users will going to use cloud computing on their mobile devices. According to a recent study by ABI Research, a New York-based firm, more than 240 million business will use cloud services through mobile devices by 2015.Thattraction will push the revenue of mobile cloud computing to $5.2 billion. With this importance, this paper has provided an overview of mobile cloud computing in which its definitions, security, issues and advantages have been presented. Mainly it discussed about security of data stored in cloud and importance of data security. This paper has explored a number of mechanisms for providing data security so that Mobile Cloud Computing can be widely accepted by a number of users in future. It also proposed a mechanism to provide confidentiality, access control as well as integrity to mobile users.

REFERENCES

[1] Portio Research,"Mobile subscribers worldwide," http://www.onbile.com/info/mobile-subscribers-worldwide.

[2] Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wirel. Commun. Mob. Comput. ,2011.

[3] White Paper, Mobile Cloud Computing Solution Brief. AEPONA, 2010.

[4] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Accepted in Wireless Communications and Mobile Computing - Wiley.

[5] Abdul Nasir Khan, M.L. Mat Kiah , Samee U. Khan, Sajjad A. Madani , "Towards secure mobile cloud computing: A survey," Future Generation Computer Systems (2012), doi:10.1016/j.future.2012.08.003, in press.

[6] W. Itani, A. Kayssi, A. Chehab, "Energy-efficient incremental integrity for securing storage in mobile cloud computing," in: Proc. Int. Conference on Energy Aware Computing, ICEAC '10, Cairo, Egypt, Dec. 2010.

[7] W. Jia, H. Zhu, Z. Cao, L. Wei, X. Lin, "SDSM: a secure data service mechanism in mobile cloud computing," in: Proc. IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai, China,Apr. 2011.

[8] J. Yang, H. Wang, J. Wang, C. Tan, D. Yu1, "Provable data possession of resource constrained mobile devices in cloud computing," Journal of Networks 6 (7) (2011) 1033–1040.

[9] Z. Zhou, D. Huang, "Efficient and secure data storage operations for mobile cloud computing," IACR Cryptology ePrint Archive: 185, 2011.

[10] S.C. Hsueh, J.Y. Lin, M.Y. Lin, "Secure cloud storage for conventional data archive of smart phones," in: Proc. 15th IEEE Int. Symposium on Consumer Electronics, ISCE '11, Singapore, June 2011.

[11] W. Ren, L. Yu, R. Gao, F. Xiong, "Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing," Journal of Tsinghua Science and Technology 16 (5) (2011) 520–528.

[12] Niroshinie Fernando, Seng W. Loke , Wenny Rahayu, "Mobile cloud computing: A survey," Future Generation Computer Systems 29 (2013) 84–106.

[13] Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review," Journal of Emerging Trends in Computing and Information Sciences, 2012.

[14] Preeti Garg,Dr.Vineet Sharma ,"Secure Data Storage in Mobile cloud computing" Internatyional Journal of Scientific Research, Volume 4 ,Issue 4,April-2013.

[15] K. Hwang, S Kulkarni and Y. Hu, "Cloud security with virtualized defence and Reputation-based Trust management," Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695-3929 -4.

[16] Ronald L. Krutz, Russell Dean Vines "Cloud Security A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc.,2010