International Journal of Computer Science and Business Informatics

IJCSBI.ORG

# A Survey of Mobile Cloud Computing: Advantages, Challenges and Approaches

**Mohammad Rasoul Momeni**
Department of Computer Engineering, Faculty of Electrical and Computer Engineering,
Imam Reza International University of Mashhad, Mashhad, Iran

## ABSTRACT
Despite explosive growth of mobile computing and its popularity, full exploiting from it, is difficult due to lack of sufficient processing power, storage, also problems such as mobility, frequent disconnections and so on. With exploiting cloud computing along mobile computing a new technology appears called mobile cloud computing. It can overcome these obstacles by executing mobile applications on the cloud instead of mobile devices. Mobile cloud is a new and applicable technology that covers many fields such as: healthcare, vehicular, gaming, commerce and so on. The ABI Research believes that the number of mobile cloud computing users is expected to grow from 43 million (1.1% of total mobile users) in 2008 to 998 million (19% of total mobile users) in 2015. This paper presents a comprehensive survey of mobile cloud computing and explains its advantages, challenges and approaches. Also the future research directions are given.

**Key words:**
Mobile cloud computing, mobile applications, mobile computing, mobility.

## 1. INTRODUCTION

By increasing usage of mobile computing, mobile devices play an important role in human life as most effective communication tools are ready in every place and time. Mobile users utilize various services from mobile applications such as Google apps which run on mobile devices locally or are offloaded to remote servers for remote execution.

Mobile devices are facing many problems about their resources (e.g. battery life, storage and bandwidth) and communications (e.g. mobility and security) [1], Hence QoS is not satisfying. Mobile devices cannot run resource-intensive applications due to lack of sufficient processing power and storage, hence mobile users prefer to utilize more powerful devices like PCs and laptops about resource scarcity problems.

To overcome these obstacles we can support mobile computing by cloud computing. Cloud computing can be defined as “the aggregation of

computing as a utility and software as a service" [2], also called pay-as-you-go-computing. Cloud service providers offer Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Offloading heavy computing can help mobile devices to save energy and mobile users to faster and more efficient execution. There are some resource-intensive applications that mobile devices never can run but with help of cloud computing, running them is easily, because cloud service providers have many powerful resources. As a result, with supporting of cloud computing for mobile users, mobile cloud- computing is introduced as combination of cloud computing by mobile computing and network technology, hence resource-intensive applications can be executed on resource-constraint mobile devices.

The reminder of this paper is as follows: Section 2 provides a brief overview of cloud computing including definitions, architecture and advantages. Section 3 describes mobile cloud computing, including its definitions, architecture, and motivation for developing, advantages, challenges and future research directions. Finally section 4 is conclusions.

## 2. CLOUD COMPUTING CONCEPT

For better understanding of mobile cloud computing, we need to understand cloud computing, because it is infrastructure of mobile cloud concept. The best definition for cloud computing is provided by NIST. NIST defines Cloud computing as "a model for enabling ubiquitous, convenient on demand network access to a shared computing resources that can be delivered with minimal managerial effort" [3]. It uses a simple "pay as you go" model which allows organizations or users to pay for the services they use. Hence we do not need to maintain datacenters and use expensive hardware and software, only we use when we need them. Cost reduction is the main factor to use cloud computing by small and large organizations. 91% of organizations in US and Europe said that cost reduction is the major reason for them to use cloud computing technology [4].

The cloud computing model can be considered as combination of three delivery models and four deployment models as follows.

The four deployment models are public, private, community and hybrid.

- Public: all users can access to cloud services.
- Private: cloud services are accessible for special group of users.
- Community: cloud services are shared among user groups, enterprises and etc.
- Hybrid: cloud services are composed of any combination of public, private and hybrid.



Three delivery models are IaaS, PaaS and SaaS.

- Infrastructure as a Service (IaaS): IaaS enables provision of key components such as hardware, storage and network devices. Amazon EC2 (Elastic cloud computing) and S3 (Simple storage service) are examples of IaaS.
- Platform as a Service (PaaS): It is the framework for building, testing and deploying applications. Examples of PaaS are Google App Engine and Microsoft Azure.
- Software as a Service (SaaS): It enables subscribers to use applications on pay-as- you-go basis. Examples of SaaS are Salesforce and Microsoft Live Mesh.

### 2.1 Advantages of Cloud computing

Cloud computing moves us from a traditional technology to a dynamic and flexible one. "Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services" [5].

In following some advantages of cloud computing discussed [6].

- On-demand services: service providers can configure services per subscriber requirements and they can access and use prepared services on-demand.
- Low cost: there is no need to prepare infrastructure, hardware and software. In fact, subscribers connect to the cloud and use from the infrastructure supplied by the service provider.
- Robustness and flexibility: we need robustness and flexibility for fast fault recovery and to adapt to non-deterministic nature of user behavior and service access pattern.

## 3. OVERVIEW OF MOBILE CLOUD COMPUTING

### 3.1 Definition

"Mobile cloud computing at its simplest, refers to an infrastructure where both the data storage and data processing occur outside of the mobile device" [7]. Alternatively mobile cloud computing can be defined as an integration of mobile web and cloud- computing [8], [9].

With mobile cloud computing technology, mobile devices do not need powerful configuration, because data processing and storage happen in the cloud instead of in the mobile devices.

### 3.2 Mobile cloud computing architecture

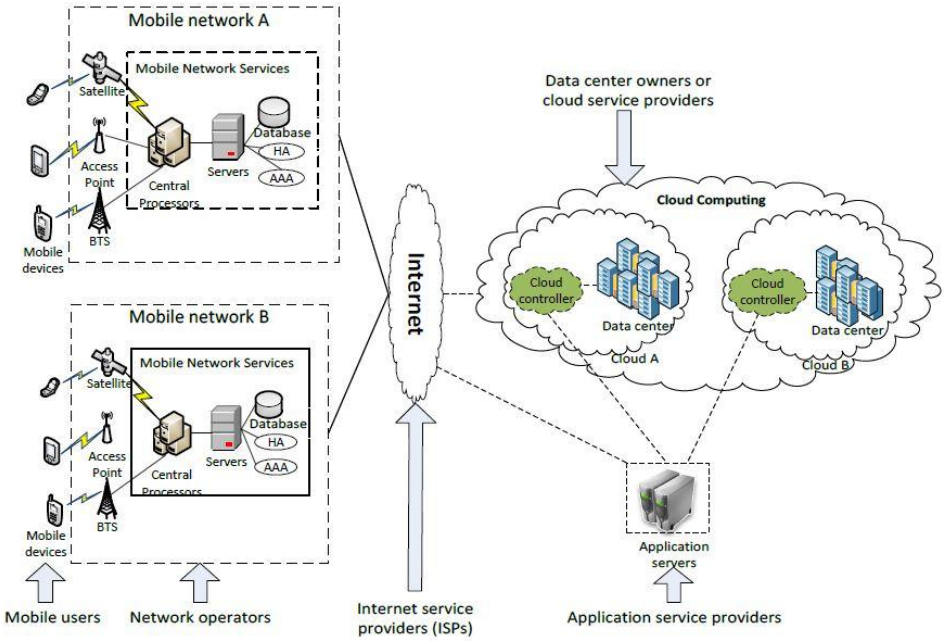


**Figure 1. Architecture of mobile cloud computing [11].**

General architecture of mobile cloud computing depicted in Figure 1. According to this figure mobile devices connect to mobile networks via BTS, access point or satellites. First request are forwarding to central processors that are connected to servers. The cloud controller receives and processes mobile user request for using cloud services. It uses the datacenter to provide different services for mobile users. In Figure 2. We see cloud computing architecture. It follows a bottom-top approach. Cloud services extensively defined in section 2. The server layer consists of virtual and physical servers and switches. This layer is responsible to allocate hardware resources to mobile client. On top of stack, client utilizes services and only pay for his/her usage. There is no concerns about hardware and software maintenance.



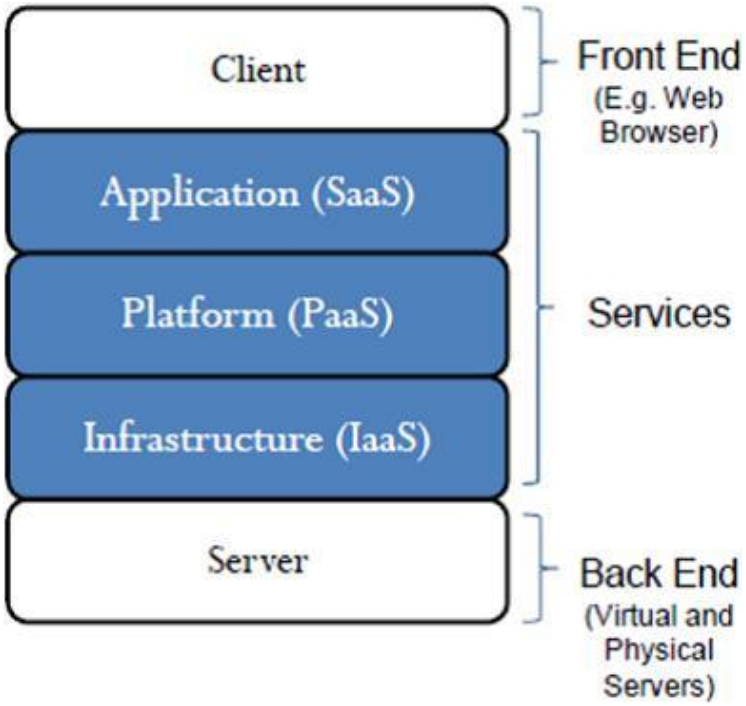


**Figure 2. Cloud computing architecture [12].**

### 3.3 Motivations for developing mobile cloud computing

Mobile devices have recently gained significant role in human life in many areas such as governmental agencies, social service providers (e.g. insurance, police), healthcare, education, and engineering organizations [13]-[15]. Despite of significant improvement in mobile devices technology, computing capabilities still is low. As mentioned mobile devices are resource-constraint devices and we need to augment them for better user experience. There are different ways to augment mobile devices mentioned in [16].

**Hardware**

Researchers aim to augment mobile devices by exploiting powerful processors, large screen and long lasting battery [17]. In this approach main focus is on CPU, Memory, Storage, Screen and Battery. This approach is low and expensive.

**Software**

Software approaches are categorized into six groups, which are remote execution, remote storage, multi-tier programming, live cloud-streaming, resource-aware computing and fidelity adaptation.

- Remote execution:



Some components of mobile applications are migrated from mobile devices to resource rich computing device(s), hence mobile devices can save energy. Remote execution (offloading or cyber foraging) is a popular option and there are many researches in this field. The efficiency of this approach is highly depends on partitioning concept.

- Remote storage:

In this approach applications and dada are kept outside the mobile devices and storage space improves significantly. By using cloud resources such as Jupiter [18] and SmartBox [19] instead of traditional resources, we have more efficiency.

- Multi-tier programming:

In this approach, we develop applications which need to less native resources. Heavy components of applications migrate from device and lightweight components remain inside the device.

- Live cloud-streaming:

In this approach [20] execution process entirely occur in the cloud and then results are transmitting to the mobile devices. There are some problems like latency, bandwidth and network traffic congestion.

- Resource-aware computing:

In these approaches [21]-[23], researchers utilize application-level resource management methods (with using software such as compiler and OS) thus requirements of mobile applications are reduced. Resource conservation is performed well via efficient selection of available execution approaches [24].

- Fidelity adaptation:

When remote resources and online connectivity are not available, this approach is an option to perform. Main idea is to decrease quality of application execution that lead to resource conservation. For better performance, researchers [25], [26] combined cyber foraging by fidelity adaptation.

Cloud computing enables virtualization technology that facilitates access to cloud services for users. Virtualization is needed for improving scalability and resource utilization ratio. It enables the illusion of infinite resources to the cloud subscribers [27].

### 3.4 Advantages

Before discussing advantages of mobile cloud computing in this section, in order to better understanding mobile cloud computing concept, we examine the definitions of mobile computing, cloud computing and network

technology. Because mobile cloud computing consists of these three main concepts.

- Mobile computing:

"Information at fingertips anywhere, anytime" [28]. Or "The mobile computing no longer requires users to maintain a fix and universally known position in the network and enables almost unrestricted mobility" [29].

- Cloud computing:

NIST defines Cloud computing as a "model for enabling ubiquitous, convenient on demand network access to a shared computing resources that can be rapidly delivered with minimal managerial effort" [3].

- Network technology:

Majority of communications occur in wireless environments.

Advantages of mobile cloud computing are:

- Improving processing power:

Resource-intensive mobile applications offload to cloud for execution, because cloud resources (specially its processors) are powerful. Thus mobile devices can virtually perform and actually deliver the results of heavy transactions that usually cannot perform [16].

- Expanded storage capacity:

Mobile applications are constrained by storage capacity on mobile devices. Due to handiness, size and price issues, Mobile devices cannot have large storage capacity. A common solution is to use infinite storage capacity of cloud resources. Amazon S3 prepares file storage service [30]. Another example is Image Exchange which utilizes large storage capacity for mobile users [31]. Also Flicker is the mobile photo sharing applications based on mobile cloud computing [32].

- Improving battery lifetime:

Long time application execution and giant processing entities lead to large amount of power consumption. A solution is to utilize offloading methods and remote application execution that significantly extend battery lifetime. In the other words, offloading heavy and energy-intensive applications to the cloud for execution can save energy. For example researchers believe offloading a compiler optimization for Image processing can reduce 41% for energy consumption in a mobile device [33].

- Improving reliability:

Due to resource scarcity in the mobile devices, providing complex encryption provisions and sufficient security services is not feasible. By storing data in the cloud storage [34], [35] mobile users ensure data protection and availability. Also cloud can provide security services such as

authentication, virus scanning and malicious code detection for mobile users [36]. To deal with data lost on mobile devices, offloading data to the cloud is efficient because cloud can backup data on a group of computers.

- Easy content and resource sharing:

By storing data and applications in the cloud, mobile users can access to contents every time, in the other words cloud service providers facilitate content and resource sharing among authorized users.

### 3.5 Challenges in mobile cloud computing

- Service availability:

Service availability is a big concern in mobile cloud computing, because majority of communications occur in wireless environments and wireless communications are not confident. Mobile users are faced with problems such as network traffic, network congestion and out-of-signal.

- Heterogeneity:

As mentioned in [10]. Heterogeneity in the mobile cloud computing refers to existence of differentiated hardware, architectures, infrastructure and technologies of mobile devices, clouds and wireless networks.

Intelligent Radio Network Access (IRNA [37]) is a model to deal with dynamics and heterogeneity of networks. In order to utilize IRNA in the mobile cloud computing, in [38] authors propose a context management architecture for acquire, management

And distribution a context Information.

- Offloading:

As mentioned in previous section, computing offloading and then remote execution is one way to improve battery lifetime. Note that offloading is not always the optimal solution to save energy, because it might consume more energy than local execution especially when the size of content is small. Methods of offloading are classified into three main directions: client-server communication methods, virtualization and mobile agents [27]. The decision of when to offload and which partitions of application need to be offloaded are important issues that need to be considered.

- Security and privacy:

Security and privacy issues are too complex in mobile cloud computing due to inherent challenges of wireless communications such as insecure nature and problems related to heterogeneity. Due to energy constraints in mobile devices, mobile users need to lightweight security algorithms. Security issues are classified into mobile application security framework and data security framework.

- Mobile application security framework:



Mobile devices are resource-constraint devices and cannot running heavy security software such as: anti-virus, intrusion detection and firewall, thus applications can be offloaded to the cloud for a detailed security assessment. For example [38] presents a method to offload the threat detection capabilities to the cloud instead of executing in the mobile device, that lead to save energy significantly. Evaluation parameters for application security frameworks are: application type, security features, assumption and scalability [39]. Also in [57] authors proposed a security framework for analyzing the security of mobile application and detecting mobile malwares. The cloud –based security approach provides strong security for mobile devices.

- Data security framework:

Data security is very important because mobile users don't have direct control on stored data on the cloud. Two important aspects of data security are:

- Data integrity:

Data integrity is a big issue for mobile users. Several solutions proposed in this area are such as [40], [41], and [43]. [42] Considers energy consumption unlike the two methods. Proposed scheme in [42] includes three main components: mobile client, cloud storage service and trusted third party and has three phases namely initialization, update and verification. Researchers used Message Authentication Code (MAC) in this method. Significant improvement in this method is this idea that checking and verification are performed on trusted third party and Mobile users only comparison the results. This improvement lead to save energy and bandwidth significantly.

- Authentication:

Authentication is an important initial step to guarantee the security of user data and files stored on cloud. In [43] authors proposed an authentication mechanism to authenticate the owner of the uploaded file on cloud and also integrity of mobile users' data stored on cloud. The proposed scheme includes four components namely mobile device, cloud service provider, certification authority and telecommunication module depicted in Figure 3.

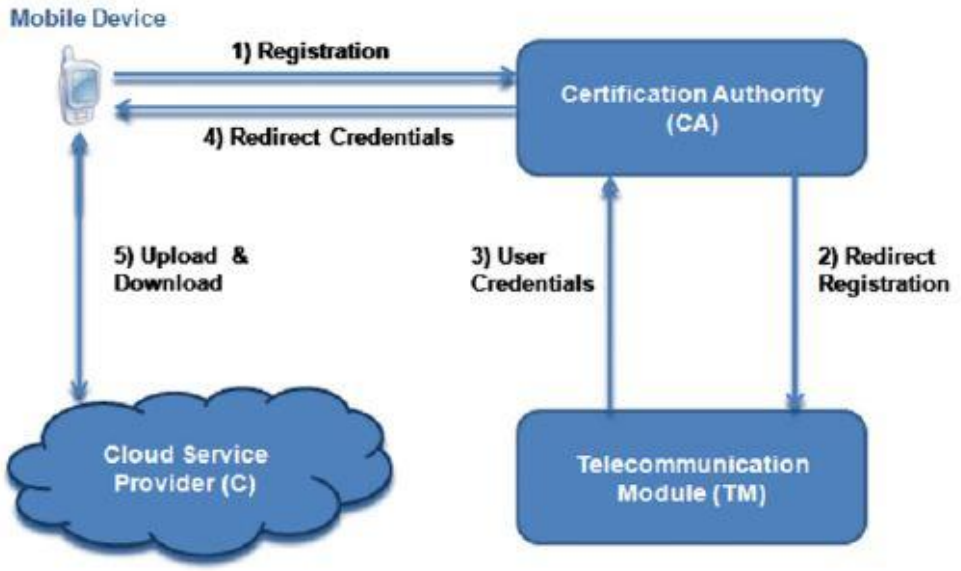


**Figure 3. Proposed scheme [43]**

The certification authority performs authentication of mobile devices in this scheme. [44] Proposes a framework that combines TrustCube [45] and implicit authentication [46], [47] to authenticate mobile users. Implicit authentication or behavioral authentication uses habits to authenticate users and maps mobile user behaviors to score. TrustCube is a policy-based cloud authentication and supports the integration of various authentication methods. Also authors in [58] proposed asymmetric encryption for providing better security. They utilized user location for providing a rigid authentication, but we know that asymmetric encryption has high power consumption and bandwidth. In [59] authors utilized secret sharing concept to propose a rigid data security framework. Their security framework is robust against related security attacks. Finally in [60] Momeni proposed a lightweight and efficient authentication protocol for mobile cloud environments. His proposed scheme is enough strong against related attacks and it is according to real communication scenarios.

- Privacy:

In [49] the authors showed that following requirements is necessary to ensure users' Privacy: protection against misuse, adjustment of laws (for more security in special circumstances), ease of use and identification of pirated datasets. Anonymous routing such as onion routing can be used to prepare privacy for mobile nodes in a decentralized mobile cloud [40]. Examples in P2P domain are [49], [50] and [51].

- Seamless communication:



Due to heterogeneity of wireless communications, maintaining a seamless communication between mobile users and mobile service provider is difficult. Mobility and frequent disconnections decrease resource utilization ratio [16]. One solution after disconnection is local execution. Note that Results obtained before disconnection is not sufficient and execution must be resumed.

- Improving the efficiency of data access:

Handling the data resources on cloud is difficult due to some problems such as low bandwidth, mobility and limitation of resource capacity of mobile devices. One easy solution to improve the efficiency of data access is a local storage cache [11]. For example [52] addresses three issues: maintaining seamless communication among subscribers and cloud, handling cache consistency and supporting data privacy. Proposed scheme has two main functional blocks namely RFS client on the mobile device and RFS server on cloud. In proposed scheme authors using RESTful web service [53] for service provider and HTTP for communication protocol. Also it addresses issues such as wireless connectivity and data privacy.

### 3.6 Future research directions

Some problems may occur when mobile users try to use cloud resources, such as disconnection, congestion and signal attenuation. These problems lead to user dissatisfaction and decreasing quality of service. Instead of communicating with a remote cloud, a better solution is to connect to Cloudlet [54]. A cloudlet is resource rich computer or cluster of computers which is Connected to the Internet and available for use by close mobile devices [11]. This approach enables mobile devices to bypass latency and bandwidth issues caused by connecting to remote cloud. In the absence of close cloudlets mobile users may using local execution or connection to remote cloud server.

- Security, trust and privacy:

With the development of cyber-crime applying security, trust and privacy is required to protect mobile user contents and success of mobile cloud computing. Indeed, how cloud service providers ensure confidentiality of user content is a critical factor. Trust establishment based on the service provider's reputation and aggregation of trust from each service node would be a valuable approach that requires future research [10].

- Low bandwidth:

Due to inherent problems of wireless environment, still bandwidth is a big problem for mobile users. One solution is to use 4G networks that improve bandwidth capacity for mobile users. Advantages of 4G networks are: broading mobile coverage area, differed services, etc. [55]. [56] Discusses

about 4G wireless network issues such as architecture, quality of service, etc.

## 4. CONCLUSIONS

Mobile cloud computing aims to augment the resource-constraint mobile devices, but currently it is like a baby that requires attention. The ABI research believes more than 240 million business will use services provided by cloud service providers through mobile devices by 2015. Mobile cloud computing is a growing technology that includes both cloud computing and mobile computing benefits. Also it is highly applicable for mobile devices. This paper has given an extensive and survey of mobile cloud computing technology including its definitions, architecture, motivation for developing, advantages, challenges and future research directions. For better understanding of mobile cloud computing before describing it, cloud computing is described.

## REFERENCES

[1] M. Satyanarayanan, 1996. "Fundamental challenges in mobile computing," in Proceedings of the 5th annual ACM symposium on Principles of distributed computing, pp. 1-7.

[2] W. Vogels, A head in the clouds the power of infrastructure as a service, in: Proceedings of the1st Workshop on Cloud Computing and Applications, CCA'08.

[3] Mell P, Grance T (2011) the nist definition of cloud computing (draft). http://csrc.nist.gov/publications/drafts/800–145/Draft-SP-800-145_cloud-definition.pdf.

[4] Ponemon (2011) Security of cloud computing providers study. http://www.ca.com/~/media/Files/ IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf

[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin and I. Stoica, . 2009. above the clouds: a Berkeley view of cloud computing, Technical Report UCB/EECS-2009-28.

[6] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, 2010. A. Konwinski, et al., A view of Cloud computing, Communication ACM. Vol.53, pp. 50–58.

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

[8] Jacson H. Christensen, 2009. "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.

[9] L. Liu, R. Moulic, and D. Shea, 2011. "Cloud Service Portal for Mobile Device Management," in Proceedings of IEEE 7th International Conference on e-Business Engineering (ICEBE), pp. 474.

[10] Z. Sanaei, S. Abolfazli, A. Gani, and R. K. Buyya, 2013. "Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges," IEEE Communications Surveys & Tutorials, Vol.16, pp. 369-392.

[11] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang., 2013. "A Survey of Mobile

Cloud Computing: Architecture, Applications, and Approaches" Wiley wireless communications and mobile computing, Vol.13, pp. 1587-1611.

[12] Modi, C., Patel, D., Borisaniya, B., Patel, B., Rajarajan, M., 2013. "A survey on security issues and solutions at different layers of Cloud computing" springer Journal of Supercomput, Vol.63, pp. 561–592.

[13] K. Bent. (2012, May) Obama: Government Agencies Have One Year To Deploy Smartphone-Friendly Services.

[14] T. Khalifa, K. Naik, and A. Nayak., 2011. "A Survey of Communication Protocols for Automatic Meter Reading Applications," IEEE Communications Surveys & Tutorials, Vol. 13, No. 2, pp. 168–182.

[15] R. Buyya, C. Vecchiola, and T. Selvi, 2013. Mastering Cloud Computing. Morgan Kaufmann, USA.

[16] S. Abolfazli, Z. Sanaei, Ejaz Ahmed, Abdullah Gani, Rajkumar Buyya, 2013. "Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies, and Open Challenges" IEEE Communications Surveys & Tutorials, Vol.16, pp. 337-368.

[17] K. Jackson. (2009) Missouri University Researchers Create Smaller and More Efficient Nuclear Battery.

[18] Y. Guo, L. Zhang, J. Kong, J. Sun, T. Feng, and X. Chen, 2011. "Jupiter: transparent augmentation of smartphone capabilities through cloud computing," in Proc. ACM MobiHeld '11, Cascais, Portugal.

[19] W. Zheng, P. Xu, X. Huang, and N. Wu, 2010. "Design a cloud storage platform for pervasive computing environments," Cluster Computing, vol. 13, no. 2, pp. 141–151.

[20] G. Lawton, "Cloud Streaming Brings Video to Mobile Devices, 2012." IEEE Computer, vol. 45, no. 2, pp. 14–16.

[21] B. Seshasayee, R. Nathuji, and K. Schwan, 2007. "Energy-aware mobile service overlays: Cooperative dynamic power management in distributed mobile systems," in Proc. IEEE ICAC'07, Jacksonville, Florida, USA, p. 6.

[22] Y. J. Hong, K. Kumar, and Y. H. Lu, 2009. "Energy efficient content-based image retrieval for mobile systems" in *Proc.* IEEE ISCAS '09, Taipei, Taiwan, pp. 1673–1676.

[23] Kremer, J. Hicks, and J. Rehg, 2003. "A compilation framework for power and energy management on mobile computers," Languages and Compilers for Parallel Computing, pp. 115–131.

[24] S. Gurun and C. Krintz, 2003. "Addressing the energy crisis in mobile computing with developing power aware software," vol. 8, no. 64.

[25] J. Flinn and M. Satyanarayanan, 1999. "Energy-aware adaptation for mobile applications," in *Proc.* ACM SOSP' 99, vol. 33, pp. 48–63.

[26] E. D. Lara, D. S. Wallach, and W. Zwaenepoel, 2001. "Puppeteer: Component-based adaptation for mobile computing," in Proc. USENIX USITS, pp. 14–25.

[27] Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, 2013. "Mobile cloud computing: A survey" Elsevier Future Generation Computer Systems, Vol.29, pp. 84–106.

[28] M. Satyanarayanan, 2011. "Mobile computing: the next decade," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 15, no. 2, pp. 2–10.

[29] T. Imielinski and H. Korth, 1996. Introduction to Mobile Computing, ser. The Springer International Series in Engineering and Computer Science, vol. 353, pp. 1–43.

[30] http://aws.amazon.com/s3/

[31] E. Vartiainen, and K. V. -V. Mattila, 2010. "User experience of mobile photo sharing in

the cloud," in Proceedings of the 9th International Conference on Mobile and Ubiquitous Multimedia (MUM).

[32] http://www.flickr.com/

[33] U. Kremer, J. Hicks, and J. Rehg, 2001. "A Compilation Framework for Power and Energy Management on Mobile Computers," in Proceedings of the 14th International Conference on Languages and Compliers for Parallel Computing, pp. 115 - 131, August.

[34] W. Zheng, P. Xu, X. Huang, and N. Wu, 2010. "Design a cloud storage platform for pervasive computing environments," Cluster Computing, vol. 13, no. 2, pp. 141–151.

[35] W. Zeng, Y. Zhao, K. Ou, and W. Song, 2009. "Research on cloud storage architecture and key technologies," in *Proc. ACM ICIS '09*, Seoul, Republic of Korea, pp. 1044–1048.

[36] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian. 2008. "Virtualized in-cloud security services for mobile devices," in Proceedings of the 1st Workshop on Virtualization in Mobile Computing, pp. 31-35.

[37] A. Klein, C. Mannweiler, and H. D. Schotten, 2009. "A Framework for Intelligent Radio Network Access Based on Context Models," in Proceedings of the 22nd WWRF meeting 2009.

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

[39] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, 2013. "Towards secure mobile cloud computing: A survey" Elsevier Future Generation Computer Systems Vol.29, pp.1278–1299.

[40] A. Tanenbaum and M. Van Steen, 2007. "Distributed Systems: Principles and Paradigms," Pearson Prentice Hall.

[41] W. Wang, Z. Li, R. Owens, and B. Bhargava, 2009. "Secure and efficient access to outsourced data," in ACM Cloud Computing Security Workshop (CCSW), pp. 55 - 66.

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

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

[44] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, 2010."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.

[45] Z. Song, J. Molina, S. Lee, S. Kotani, and R. Masuoka. 2009. "TrustCube: An Infrastructure that Builds Trust in Client," in Proceedings of the 1st International Conference on Future of Trust in Computing.

[46] M. Jakobsson, E. Shi, P. Golle, and R.Chow, 2009. "Implicit Authentication for Mobile Devices," in Processing of the 4th USENIX Workshop on Hot Topics in Security (HotSec).

[47] E. Shi, Y. Niu, M. Jakobsson, and R. Chow. 2010. "Implicit Authentication through Learning User Behavior," in Proceedings of the implicit authentication Security Conference (ISC).

[48] M. Fahrmair, W. Sitou, B. Spanfelner, 2011. Security and privacy rights management for mobile and ubiquitous computing, in: Workshop on UbiComp Privacy, pp. 97–08.



[49] J. Han, Y. Zhu, Y. Liu, J. Cai, L. Hu, 2005. Provide privacy for mobile p2p systems, in: 25th IEEE International Conference on Distributed Computing Systems Workshops, pp. 829–834.

[50] J. Han, Y. Liu, Rumor, 2006. Riding: anonymizing unstructured peer-to-peer systems, in: Proceedings of the 2006 14th IEEE International Conference on Network Protocols, 2006, ICNP'06, pp. 22–31.

[51] G. Ghinita, P. Kalnis, S. Skiadopoulos, 2007. Prive: anonymous location-based queries in distributed mobile systems, in: Proceedings of the 16th International Conference on World Wide Web , ACM, New York, USA, pp. 371–380.

[52] Y. Dong, J. Peng, D. Wang, H. Zhu, F. Wang, Sun C. Chan, and Michael P. Mesnier, 2011. "RFS: a network file system for mobile devices and the cloud," ACM SIGOPS Operating Systems Review, vol. 45, no. 1, pp. 101-111.

[53] Jacson H. Christensen, 2009. "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.

[54] M. Satyanarayanan, P. Bahl, R. Caceres, N. Davies, 2009. The case for VM-based cloudlets in mobile computing, IEEE Pervasive Computing Vol.8, pp. 14–23.

[55] M. Rahman and F. A. M. Mir, 2007. "Fourth Generation (4G) Mobile Networks - Features, Technologies & Issues," in Proceedings of the 6th IEEE International Conference on 3G and Beyond, pp. 1.

[56] U. Varshney and R. Jain, 2002. "Issues in emerging 4G wireless networks," Computer, vol. 34, no. 6, pp. 94 – 96.

[57] S. Zonouz, A. Houmansadr, R. Berthier, N. Borisov, W. Sanders, 2013." Secloud: A cloud-based comprehensive and lightweight security solution for smartphones"; Proc: Elsevier.

[58] Md. AI-Hasan, Kaushik Deb, Mohammad Obaidur Rahman, 2013. "User Authentication Approach for Data Security between Smartphone and Cloud"; Strategic Technology (IFOST), 8th International Forum on, Publisher: IEEE.

[59] Hong gang Wang, Shaoen Wu, Min Chen, Wei Wang, 2014. "Security Protection between Users and the Mobile Media Cloud", IEEE Communications Magazine.

[60] 60. Momeni, M. R., 2014. A Lightweight Authentication Scheme for Mobile Cloud Computing. International Journal of Computer Science and Business Informatics, Vol. 14, No. 2, pp. 153-160.

This paper may be cited as:

Momeni, M. R., 2015. A Survey of Mobile Cloud Computing: Advantages, Challenges and Approaches. *International Journal of Computer Science and Business Informatics, Special Issue: Vol. 15, No. 4, pp. 14-28.*