A Critical Overview of Latest Challenges and Solutions of Mobile Cloud Computing

Hesham Allam
CIS Department
HCT
Dubai, UAE
hesham@hct.ac.ae

Nasser Nassiri
CIS Department
HCT
Dubai, UAE
nnassiri@hct.ac.ae

Amala Rajan
CIS Department
HCT
Dubai, UAE
arajan@hct.ac.ae

Jinesh Ahmad
CIS Department
HCT
Dubai, UAE
jahmad@hct.ac.ae

Abstract – **The unabated plethora of research activities to augment multifarious mobile devices by leveraging cloud resources have created new research field called Mobile Cloud Computing (MCC). Recently, researchers have found Mobile Cloud Computing (MCC) to be a promising venture combining the advantage of both the cloud and mobility in giving users available resources on the cloud wherever they are using their mobile phone. Despite its benefits, many challenges still remain with MCC. This paper addressed recent challenges ranging from limited computational capacity, connectivity, security, latency, and heterogeneity. Solutions for these challenges are suggested including mobile processes offloading, using HTML5 technologies to compensate for connectivity loss, SDN centralized control features for data security, utilizing the cloud for time consuming applications, and using cross platform applications neutralizes heterogeneous technologies. Finally, the paper concludes with an extracted list of new research idea for scholars to work on to further enhance MCC**

Keywords – **Cloud Computing, Mobile Cloud Computing, Security, mobile connectivity, accessibility, and Performance**

I. INTRODUCTION

Mobile cloud computing is the use of cloud computing to provide mobile users with a feature-rich array of apps, irrespective of connectivity strength, mobile operating system, or mobile phone computing or memory capacity. The Cloud can be seen as an interface that makes software resources accessible to a massive number of users, through hardware that is based in a data centre. Cloud computing has emerged in the last decade and gained considerable interest owing to the numerous advantages it provides.

There are many potential benefits of MCC that makes it an appealing venture to industry and researchers including increasing the processing power and battery life time of mobile devices, coping with the increasing services and application needs of most mobile users with low-end mobile devices, maximizing the resource sharing and reuse of existing computing resources in cloud infrastructures and Internet based applications and services. Further, MCC has the potential to eliminate existing limitations of the current mobile devices and to Leverage the mobile handsets to the existing and future cloud based network and mobile enabled service infrastructures [1].

In spite of these potential benefits of MCC, there are many challenges and issue facing the application of MCC. The research objectives of this paper is to shed the light on MCC recent challenges and extract the latest solutions for the extracted challenges with an overview of research topics for scholar to follow on.

The paper is organized as follows: section II covers MCC approaches in providing its services. Section III surveys the current literature and extract the current challenges facing MCC followed by an overview of the solutions proposed by recent research in the field. Section IV list some research idea that can be tackled by researchers to further enhance the use of MCC

I. MOBILE CLOUD COMPUTING APPROACHES

One approach to deploy MCC is that the applications that require extensive computation are offloaded to the computational cloud and the results are returned to the mobile device. Cloud service providers (CSPs) provide the physical and virtual areas in which such apps are running. In most cases, users are unaware of the location where such apps are executed. However, mobile users are ideally able to connect to such clouds anywhere and at any time. CSPs bring together various resources to form a cloud. Mobile users should be able to benefit from this cloud in storing large amounts of data, thereby protecting their data from virus attacks, data loss, or data leakage that can cause the data to be destroyed [2].

Other approaches for MCC considers the mobile phone itself as a resource provider to other mobile cloud computing seekers. This allows for what is known as mobile peer-to-peer communication. This can be done in combination with providing resources from stationary objects as well. The aim of this approach is to maximize connectivity by utilizing the maximum potential of the mobile phone [3].

978-1-5386-2859-1/17/$31.00 ©2017 IEEE

II. RECENT MOBILE CLOUD COMPUTING CHALLENGES

Considering that MCC is a relatively new technology started in 2009, there are many challenges that arose upon experimenting with the systems and after establishing several clouds led by different CSPs. Each CSP and cloud may have their own set of issues resulting from various variables, but some issues are common and seen in most clouds mobile cloud computing initiatives. Those issues are worth addressing and require further exploration.

A. Limited Computational capacity and Battery Life

When it comes to battery capacity, the mobile devices are relatively limited compared to stationary devices where is a lot of space to implement stronger, longer-lasting energy sources. Mobile phones have a limited computational capacity that limits many of its functions. For example, the use of location services like GPS consumes a lot of energy because it involves extensive use of sensors. Likewise, some apps that require a huge processing capacity, like image processing for video games, speech synthesis, natural language processing, augmented reality and wearable computing. Such services represent a computational challenge to application developers, because they are not able to implement applications that meet such a need. Given the fact that this limitation is dictated by the limited battery capacity and the small size of mobile devices, it is more likely for this problem to be solved using software developments than hardware ones [4].

Solution: With regard to energy limitations, some researchers [5] showed that offloading components interface in mobile games to cloud servers can save battery energy usage by 27% for computer games, and 45% for chess games. Another solution is to use short range access points. For mobile devices to perform under high speed connectivity for longer ranges, the battery is compromised. Therefore, creating shorter ranges can allow access to be unrestricted while maintaining a longer battery life (less energy consumption). Additionally, longer range could lead to latency issues, which impacts interactive performance, even with a good bandwidth. Others including Kakero and Paulson and Zhang [6], suggested using offloading techniques by moving the complicate processes from the mobile device with limited resources to other servers that are more resourceful with cloud capacity to save battery life of mobile devices. Similarly, further attempts [7] suggesting developing an application model that enables the application to seamlessly use resources from the server whenever needed. This is known as application elasticity, where the application is dynamic and interactive instead of being a software controlled by outside factors. When this application is launched, the elastic application manager can monitor the requirements needed for the resource by the weblets of the app and determine the time for launching. Since the computing weblet is intensive, it usually limits the processors in the mobile device and can be launched on the cloud on more than one platform. Ideally, the mobile device is able to adapt to the required workload when elastic apps are used. However, it is argued that the effect of elastic applications to conserve battery life and improve device performance is not well-confirmed by research [8].

B. Connectivity

Maintaining connectivity across different connection mechanisms used in a challenge for MCC. In case of 3G connectivity, there is an increased data cost and latency. As users move, there is variability in signal strength that disrupts ongoing processes. This could be due to variability in location signal reception or the present of blind spots that have no connectivity at all. Accordingly, development of systems that overcome such problems is necessary for MCC to manifest its promising potential [3].By nature, mobile devices have limited network bandwidth, compared to wired networks. The Quality of Signal (QoS) delivered to the user is affected by non-proportionate delay in execution of the applications, the dismissal of always-on connectivity, and the excess utilization of limited mobile resources. Not only does this limitation in resources affect signal, but it also takes its toll on the processes of applications [4].

Solution: Satyanarayanan et al. [9] proposed the use of Virtual Machine (VM) technology "to rapidly instantiate customized service software on a nearby cloudlet" as a solution to this problem. They propose that the service is used over a wireless LAN. Therefore, considering that the cloudlet is a resource-rich trusted computer(s) that has excellent connectivity to the internet, the mobile phone acts as a thin client and the user can guarantee good connectivity even as they move. Further, a new technology that offers a solution for data caching utilizing for a mobile device is the HTML5. This technology allows the cloud application to continue performing even if there is some interruption in the connection [10].

C. Data Security and Privacy Issues

One of the major issues facing MCC is data security. Parasad and Gyani[11] focused on some [1]security concerns related to MCC including loss of physical security, handling of encryption and decryption keys, security and auditing issues of virtual machines, less norms for data integrity, and services platform incompatibility from various vendors. Further, when offloading data to the cloud, there is concern about data safety and privacy. The offloading process places the data of the user at risk of data breach and invasion of personal information. There is also the concern about intended violations, which are seen as a specific person hacking a particular device for the sake of sabotaging or stealing important information. Although different from hackers who violate the data of random users, such premeditated attacks could even be more harmful and have a negative impact of user's privacy [3]. Moreover, a flaw in the encryption algorithm on the CSP's part can result in

unauthorized access to one's information. Any user can access sensitive information when security fails to protect the data of the victim user [12].Social media and online payment seem to be the most vulnerable resources for hacking since it carries important and crucial data for users and users seem to be less careful when sharing information especially with social media [1]. Another issue with lack of security is piracy. When pirated material is distributed among mobile networks, they have a much wider exposure to unwanted users than they do in other devices. An encryption and decryption procedure can restrict access to such material by providing keys prevent unauthorized access to digital materials [**3**].

Solution: One of the measures that can be taken to address the piracy issue is the provision of encryption and decryption keys to access these contents. A coding or decoding platform must be done before any mobile user can have access to such digital contents. Data integrity issue could be resolved by authenticating every access instance by users. With regards to authentication, there must be a proper authentication procedure to secure mobile data access [14]. With regards to network security, some researcher including [22] suggested using features of SDN including its centralized control that permits a dynamic authentication of legitimate hosts based on information about the host which is obtained during the registration.

D. The Role of Malware in Security

The wide array of mobile applications used by mobile phones to access other mobile devices isan attractive medium for malware creators. The issue is no longer caused by unauthorized users accessing unauthorized data. Rather, it is happening because people are agreeing on installing malware on mobile devices that can transfer and leak personal data to malware creators.

Solution: There is more than one way to solve this issue. First, mobile users need to be educated about using anti-spyware and anti-malware programs and knowing what to expect when they use a mobile device connected to the cloud. Second, the cloud can design and implement its own apps. That way, in the event of a security thread, the cloud can restore the lost data from trusted backups in the cloud itself. Continuous improvement of the infrastructure of the cloud enhances security in more than one way and gives an overall safer experience for all mobile users [1].

E. Latency

The standard architecture of mobile cloud involves three elements: Mobile client, Transmission channel and Cloud. This basic structure involves latency as the request is sent to the cloud and back to the mobile device upon completion. Further, Part of the accessibility issue originates from the added security layers to prevent unauthorized access to data [15].

Solution: This problem could be tackled with the more developed architecture of introducing a cloudlet which is installed between the client and the cloud and contains copies of the cache. The purpose of this cloudlet is to decrease latency, serve only a few users, and it makes connectivity relatively faster and easier [15, 16]. Another solution was proposed by Satyanarayana [9] using the cyber foraging approach where mobile augmentation is executed by offloading applications to non-mobile computing devices to provide heavy functionality and to conserve local resources including mobile energy. For media latency, some researchers [23] suggested using a 3C architecture based on SDN that focuses on collection, computation, and consumption. Using SDN, first data is collected and small portion of the video processing is handled at the network edge, and then a large video processing takes place on the cloud.

F. Heterogeneity

Heterogeneity in MCC is the existence of various types of hardware, architectures, infrastructure, and technologies of mobile devices, clouds, and wireless networks. MCC is used in a heterogeneous environment ranging from different interfaces on the wireless network different nodes in the mobile device, and different wireless technologies such as WiMAX, GPRS, WLAN, CDMA2000 and WCDMA. Heterogeneity could cause MCC to fail to fulfil its proposed benefits as being efficient in energy use of mobile devices, always being connected, and scalability of on-demand wireless connection [17].

Solution: Madhavapeddy et al. [18] propose a cloud OS called Mirage which they base on the idea of virtualization technology. Mirage produces a neutral and cross-platform applications that can work to mobile devices and cloud servers. Using such an approach, applications are developed on normal OS such as Linux and then compiled into a kernel that is able to run directly on mobile devices and virtual clouds avoiding heterogeneity issues. Another solution is to use Service Oriented Architecture (SOA) which is well known in neutralizing the difference among specific technology, vendors, and business policies that incorporates different services towards generating complex a applications and services. A good example is Facebook which delivers multimedia YouTube content without the need to follow YouTube differentiation standards [19].

G. User Interface issues

Mobile device sizes are relatively small. This means that most apps rely on interfaces that have few static elements, such as scroll bars, palettes, and pop-up menus and icons. Another drawback is the reduced typing speed due to lack of screen size. Such interfaces are considered easy-to-use, but further development is required to design easy interfaces without static elements. Another issue is that the tasks performed on mobile phones are assumed to be different from regular desktop tasks. Mobile devices are assumed to be used for

viewing data and less data entry, contrary to desktop computers. Accordingly, user interface designers keep that point in mind when designing software [. 20].

Solution: To solve the problem of lack of computational capacity of mobile devices, running applications on a remote host and using the mobile device primarily for the user interface is a more reliable option, assuming that the remote servers are more stable and will be able to restore data in case of mobile device crashing [20].

III. FUTURE RESEARCH PERSPECTIVES

Finally, research directions pertaining to the burgeoning field of MCC opened new research and innovation opportunities. Developing security measures and establishing a neutral environment where technology heterogeneity is neutralized seamlessly are the most prominent issues that demand researchers' attention. The following are some research idea that can by tackled by researchers to enhance MCC potential:

Here are a few research ideas that could resolve some of the issues seen in MCC today:

- Develop security measures that are compatible with the low-energy status of mobile phones
- Examine ways to decrease cost of application elasticity
- Create cloudlets with minimum energy requirement and increased computing power
- Maximize computational capacity of mobile devices to overcome the current limited capacity that restricts development of high-demand applications.
- Apply a theoretical framework to a real-life situation to double-check that proposed solutions to problems are achieved by the methods expected
- Design UI with less static elements for mobile devices

IV. CONCLUSION

Mobile cloud computing is a relatively new field with challenges arising every day. It has become popular because it combines the advantages of both mobile computing and cloud computing. However, because of the nature of mobile devices, MCC encounters several challenges that could hinder its claimed benefits. Example of the challenges limited computational capacity and battery life, data security and privacy issues heterogeneity of MCC technology, connectivity issues, lack of a unified user mobile user interface, and lack of interoperability. This research paper list current MCC challenges and offer solutions as proposed by recent research.

V. REFERENCES

[1] R. Change, J. Gao, V. Gruhan, J. He, G. Roussor, and W. Tsai, "Mobile Cloud Computing Research – Issues, Challenges, and Needs," in 7th International Symposium on Service-Oriented System Engineering, 2013.

[2] S. Khan, M.. Shiraz, A. Wahab, A. Gani, and Z. Rahman, "A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing," The Scientific World Journal, vol. 2014, p. 27, 2014.

[3] N. Fernando, S. loke, W. Rhayau, "Mobile cloud computing: A survey, Future Generation Computer Systems," Futrue Generation Computer Systems, vol. 29, no. 1, pp. 84-106, 2013.

[4] M. Alzadeh, W. Hassan, "Challenges and opportunities of Mobile Cloud Computing," in 9th International Wireless Communications and Mobile Computing Conference, Sardinia, 2013.

[5] E. Cuevo, D. Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Pahl, "MAUI: making smartphones last longer with code offload," in 8th international conference on Mobile systems, applications, and services , San Francisco, 2010.

[6] R. Kakerow, "Low power design methodologies for mobile communication," in IEEE International Conference on Computer Design: VLSI in Computers and Processors, 2002.

[7] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjith, S. and Joang, "Securing elastic applications on mobile devices for cloud computing," in 2009 ACM workshop on Cloud computing security , Chicago, Illionois, 2009.

[8] Rudenko, P. Reiher, G. Popek, and G. Kuenning, "Saving portable computer battery power through remote process execution," CM SIGMOBILE Mobile Computing and Communications Review, vol. 2, no. 1, pp. 19-26, 1998.

[9] M. Satyanarayanan, P. Gahl, R. Cacores, and N. Davis "The Case for VM-Based Cloudlets in Mobile Computing," IEEE Pervasive Computing, vol. 8, no. 4, pp. 14-23, 2009.

[10] S.Shafique, T. Ahmad, K. Rafique, and S. Islam, "Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues," in 2011 IEEE International Conference on Cloud Computing and Intelligence Systems, Beijing, 2011.

[11] M. Prasad, J. Gyani, and R. Murt, "Mobile Cloud Computing: Implications and Challenges," Journal of Information Engineering and Applications, vol. 2, no. 7, 2012.

[12] M. C. Sapna Malik, "Privacy and Security in Mobile Cloud Computing: Review," International Journal of Computer Applications, vol. 80, no. 11, pp. 20-26, 2013.

[13] M. Cooney, "The 7 most common challenges to cloud computing," Network World, 11 July 2012.

[Online].Available: http://www.networkworld.com/article/2189909/cloud-computing/the-7-most-common-challenges-to-cloud-computing.html. [Accessed 8 april 2017].

[14] L. Ioana, O. Juric, L. Krivale, G. Aloso, "Calling the Cloud: Enabling Mobile Phones as Interfaces to Cloud Applications," In: Bacon J.M., Cooper B.F. (eds) Middleware 2009. Middleware 2009. Lecture Notes in Computer Science, vol. 5896, 2009.

[15] T. Shon, , J. Cho, I. Han, H. Choi, "Toward Advanced Mobile Cloud Computing for the Internet of Things: Current Issues and Future Direction," Mobile Networks and Applications, vol. 19, no. 3, pp. 404-413, 2014.

[16] Dinh, C. Leee, D. Niyato, P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless communications Mobile Coputing , vol. 13, no. 18, pp. 1587-1611, 2011.

[17] A. Madhavapeddy, R. Jrier, J. Growcroft, S. Hand, "Multiscale not multicore: efficient heterogeneous cloud computing," in 2010 ACM-BCS Visions of Computer Science Conference , Edinburgh, United Kingdom, 2010.

[18] Z. Sanaei, S. Abolhafiz, and R. Guyya, "Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges," IEEE Communications Surveys & Tutorials , vol. 16, no. 1, pp. 369 - 392, 2014.

[19] Landay, T. Houfmann, "Uer Interface Issues in Mobile computing," in IEEE 4th Workshop on Workstation Operating Systems. WWOS-III, Napa, CA, 1993.

[20] B. Sotomayor, R. Montero, I. Lorent, and I. Foster, "Virtual Infrastructure Management in Private and Hybrid Clouds," IEEE Internet Computing, vol. 13, no. 5, pp. 14-22, 2009.

[21] T. Harmer, P. Wright, C. Cunningham, R. Perrot "Provider-Independent Use of the Cloud," Euro-Par 2009 Parallel Processing. Euro-Par 2009. Lecture Notes in Computer Science, Vols. vol 5704. Springer, Berlin, Heidelberg, pp. 454-465, 2009.

[22] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 1, pp. 602-622, 2016.

[23] Y. Wen, J. Chakareski, P. Frossard, D. Wu and W. Zeng, "Guest Editorial Special Issue on Visual Computing in the Cloud: Mobile Computing," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 27, no. 1, pp. 1-5, 2017.