The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.61 e-ISSN: 2251-7545

CCmH: The Cloud Computing Paradigm for Mobile Health (mHealth)

[1] Sasan Adibi,
Platform Technologies Research Institute (PTRI)
[1] School of Business IT and Logistics
Royal Melbourne Institute of Technology (RMIT), Melbourne, Australia
sasan.adibi@rmit.edu.au

[2] Nilmini Wickramasinghe,
[2] Epworth HealthCare,
[2] Health Innovation Research Institute (HIRI)
Royal Melbourne Institute of Technology (RMIT), Melbourne, Australia
nilmini.wickramasinghe@rmit.edu.au

[3] Caroline Chan
Royal Melbourne Institute of Technology (RMIT), Melbourne, Australia
caroline.chan@rmit.edu.au

ABSTRACT— Cloud computing is a complex infrastructure revolved around (mobile and non-mobile) computing, database and storage capacity, and service delivery. This evolving concept aims to serve as the next generation heterogeneous service-based model, with centralized and decentralized clients, servers, services, and data storage entities across multiple platforms. Mobile cloud computing (mcc), which is a subset of the cloud computing space, is where a number of the cloud entities are mobile-based. This paper is focused around the idea of mcc deployment in the healthcare areas, defining the cloud computing mobile health (mhealth), (ccmh), which includes the relevant issues and challenges. The main contribution of this paper is a set of recommendations for the future expansions of both cloud computing and emerging mhealth technologies when they are merged together.

Keywords: Cloud computing, Mobile Health (mHealth), security, Quality of Service (QoS)

I. INTRODUCTION (*Heading 1*)

Cloud computing is a term referring to a cloud-based evolving infrastructure in which clients, servers, and databases are interconnected (partially through the Internet). Such an interconnection is aimed to facilitate the delivery of services and deployment of applications offered to clients on the cloud. One of the industries that can benefit from this infrastructure is the healthcare applications, in which patients, doctors, nurses, lab technicians, pharmacists, insurance and government agencies can be considered cloud entities. The focus of this paper is to explore the utilization of smartphone as the patient's cloud end-point entity and the related aspects and issues [1]. Smartphones have been the center of the attention for the past recent years and the current hardware and software capabilities found on nowadays smartphone devices are sufficient to handle health-related data acquisition, classification, delivery, and remote interactions [2]. There are however a few challenges associated to the deployment of smartphones in the healthcare space, which will be considered and discussed in this paper.

The rest of the paper is organized as follows: Section 2 provides an introductory summary to cloud computing. Section 3 summarizes the advantages and challenges concerning cloud computing. Section 4 revolves around the idea of mHealth deployed in cloud computing, which is followed by a set of recommendations in Section 5. A discussion is given in Section 6 followed by the Conclusion (Section 7) and the References, which concludes the paper.

II. INTRODUCTION TO CLOUD COMPUTING

Cloud computing provides virtually limitless functionality and services for information sharing and management in an ubiquitous, centralized/decentralized, and pervasive manner, aimed to support multiple platforms (Figure 1, adapted from [3]).

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.61 e-ISSN: 2251-7545

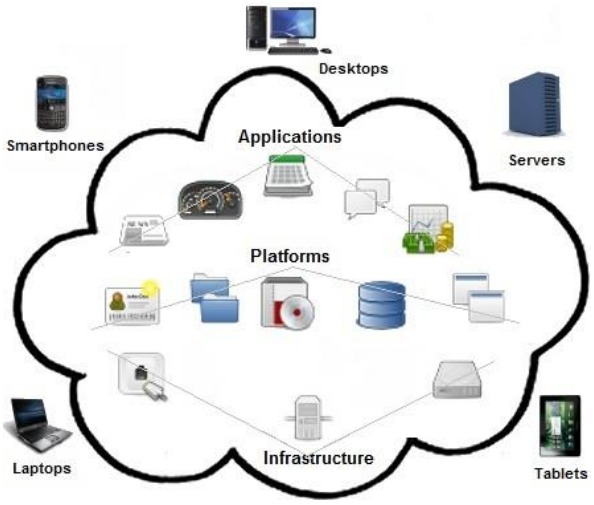

Figure 1. Cloud computing paradigm (adapted from [3])

As shown in Figure 1, the entities outside the cloud are the cloud clients, which include: smartphones, servers, laptops, and tablets. According to the National Institute of Standards and Technology (NIST), cloud computing features the following six essential characteristics [4]:

A. CLOUD COMPUTING ESSENTIAL CHARACTERISTICS

Based on NIST's specifications and recommendations, cloud computing features the following six essential characteristics [4]:

- ON-DEMAND SELF-SERVICE – A client consumer can request a service, network time, resources, and storage (online renting, upload, and download) without a third-party involvement.
- FLEXIBLE ACCESSIBILITY – This characteristic translates to ubiquitous network access, where any client with any device (assumed capable of minimum functionality), is able to get connected and receive services.
- ELASTICITY PROVISION – Services and capabilities can often be extended and scaled automatically.
- METERED SERVICES – The usage quantity and quality are measured and clients are billed accordingly.
- RESOURCE POOLING – Multiple clients can be serviced simultaneously using a multi-tenant model with on-demand dynamic mechanisms.
- LOCATION INDEPENDENCE – The services provided by the cloud are often independent of the original, current, and future locations of the clients.

B. CLOUD COMPUTING SERVICE MODEL VARIATIONS

There are three main variations of cloud computing service models on top of the data centers layer (Figure 2, adapted from [1]): Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [1, 4].

- DATA CENTERS LAYER – This provides hardware capability for the cloud and is connected to the high-speed network backbone.
- INFRASTRUCTURE AS A SERVICE (IAAS) – IaaS is right on top of the data centers layer and is the most basic cloud service model in which the client is provided with network access, storage, application, and computing resources without control over underlying cloud physical infrastructure, such as Amazon CloudFormation [5].

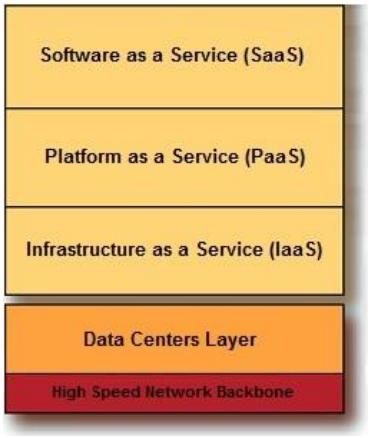

Figure 2. Service-based cloud computing architecture (adapted from [1])

- PLATFORM AS A SERVICE (PAAS) – PaaS is on top of IaaS, which provide clients with access to the operating system, programming language environment, web services/servers, and database for testing, building, and custom application deployment, such as the Google App Engine and Microsoft Azure.
- SOFTWARE AS A SERVICE (SAAS) – This is the highest layer of service model in which the client can have access to the software system and application via remote connectivity and run their applications on virtual machines and be billed for the exact amount of usage, such as Google Apps.

C. CLOUD COMPUTING DEPLOYMENT MODELS

The deployment model comes any of the following four flavors:

- PUBLIC CLOUD – This is where the cloud applications, storage, and entire resources are available in the public domain, such as Microsoft and Google clouds.
- PRIVATE CLOUD – In contrast to the public cloud, private cloud is used in for a single organization

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.61 e-ISSN: 2251-7545

- HYBRID CLOUD – Is a mix-and-match of both public and private clouds
- COMMUNITY CLOUD – Is a shared infrastructure between several organizations in support of a common shared interest.

III. Cloud computing advantages and challenges

A. CLOUD COMPUTING ADVANTAGES

Cloud computing is an evolving concept with promising capabilities because of its infrastructure's portability, mobility, and connectivity to high-speed data transport mechanisms. Therefore the advantages of cloud computing can be categorized as followed [1, 6]:

- HIGH EFFICIENCY – All cloud-based systems and services (e.g., applications, storage) benefit from highly efficient client-based usages, which are adaptive and can accommodate many clients with dynamic capabilities.
- SCALABILITY AND FLEXIBILITY – The adaptability of cloud-based systems according to the usage trend fluctuations has made cloud services easily scalable to the sudden increase of clients and flexible to the service delivery modes.
- IMPROVED RELIABILITY – Running applications on virtual machines with real-time back-up systems is a proven method to increase reliability, which is one of the advantages of cloud computing.
- VIRTUALLY LIMITLESS RESOURCES – The provision of service elasticity means that once the client is offered a service, services and capabilities can often be extended and scaled automatically.
- OVERALL COST-EFFICIENT – The flexibility, improved reliability, and higher efficiency lead to cost reduction.
- ANYWHERE-ANYTIME AVAILABLE – This translates to ubiquitous network access, where any client with any device (assumed capable of minimum functionality), is able to get connected and receive services.
- EASE OF USE – Requesting services via cloud computing has taken the ease-of-use bar to a whole new level due to the fact that any device is able to get connected and receive services independent of the location.

B. CLOUD COMPUTING CHALLENGES

Despite all the benefits and advantages associated to cloud computing, there are a number of disadvantages and challenges concerning the infrastructure, deployment, service, and delivery models, which are categorized as followed [1, 6, 7, 8]:

- SECURITY AND PRIVACY – Providing security and privacy is a huge obstacle for cloud computing due to the nature of the communication channel with distributed clients accessing resources, anywhere and anytime. The security concerns are broken down to the followings:
  - *Centralized data security*: Due to the nature of the cloud computing data distribution (which can be centralized and/or distributed), providing security measures for both topologies become very challenging and important.
  - *Safeguarding backend data*: This in particular is important for public clouds, outside of corporate firewalls, prone to various types of attacks.
  - *Virtualization security*: Recent studies have shown that hypervisor and virtual machines are prone to VM-based rootkits [9].
  - *Identity concealment*: The identity of clients accessing resources on the cloud is another challenge, especially when scalability becomes a factor
  - *Shared-tenancy attack*: It's been shown that eavesdropping software can be loaded into a shared server running VM and monitor the client's activities.
  - *Brute force attacks*: A virtualized infrastructure can be used for launching brute force attacks trying to decrypt private data.
  - *Denial of Service (DoS)*: This is a major risk factor to business continuity when an adversary targets a service provider by transmitting a large number of attach queries, which will either slow the service provider down or stops the service completely.
  - *Data availability*: This is the opposite of DoS, where a service provider will try to ensure its services are available to the clients most of the time. The higher the probability of service availability, the better.
- *Interoperability* – Service providers have to ensure that they support different client platforms, which is an ongoing task.
- Other issues and challenges include: *Managing the cloud, the contractual relationship, dealing with cloud-exit strategies, and activity monitoring*.

IV. Cloud computing from mHealth perspective

Electronic Health (eHealth) is the body of knowledge and efficient practices concerning health-related sensors, acquisition, usage, storage, information retrieval, and devices. Another objective of eHealth is to apply best engineering practices in dealing with the followings: Health systems and infrastructures, healthcare standards,

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.61 e-ISSN: 2251-7545

Mobile Health (mHealth), telemedicine, and health-based cloud computing.

Mobile Health (mHealth) is the practice of eHealth supported by smartphones. Figure 3 (adapted from [10]) shows the mHealth big picture, where the biomedical data is captured at the body-worn sensor end. The data is transmitted to a data collector (smartphone) via a link technology (i.e., Bluetooth, Bluetooth Low Energy, ZigBee) [11]. The data collector transmits the information to the cloud/Internet via the cell-tower, which in turn will be received by a number of cloud entities. In a healthcare scenario, the cloud entities include: patients, family, coach, doctors, nurses, lab technicians, pharmacists, medical database, insurance and government agencies.

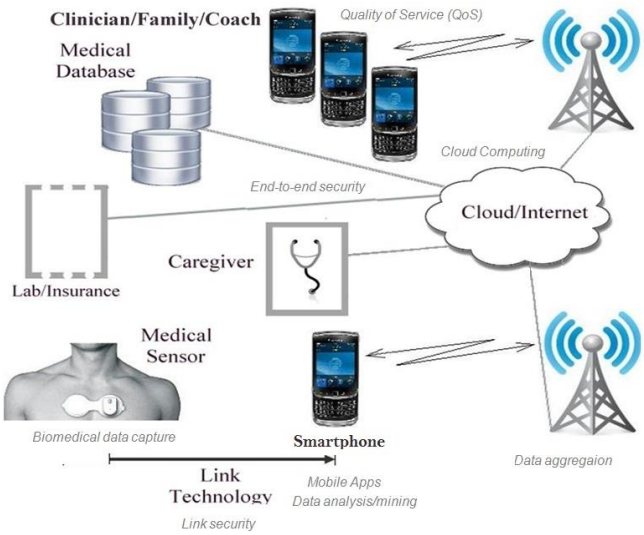

Figure 3. Mobile Health in cloud computing (adapted from [10])

The deployment of mobile technologies in the medical field (mHealth) has already gained overall acceptance in the medical community, those social aspects of this migration is still on ongoing topic of research. Merging mHealth with cloud computing (Mobile Cloud Computing "MCC") results (CCmH) in an increased accessibility to healthcare facilities and providers, improved quality, and more efficient processes.

In this section we discuss the details and issues concerning mHealth (CCmH).

A. Wireless Body Area Network (WBAN) in CCmH

The usage of sensors used on patients bodies is an emerging technology in the mHealth space. Monitoring these sensors in the CCmH perspective is a challenging issue. Reference [12] presents a sensor-based WBAN-CCmH framework in which continuous patient monitoring is done on the cloud using personal and cloud medical servers. The prototype ran four simultaneous sensors capturing Electrocardiography (ECG), Electromyography (EMG), Electroencephalography (EEG), and Pulse Oxiometer (SPO2) data. The sensor data is captured by an Android Python-based Samsung Galaxy S and is transmitted to the cloud.

Reference [13] presents a similar framework and the related prototype that captures, analyzes and transmits ECG data from the patient's bedside to the cloud. This reference addresses the issues concerning to cost and scalability in a non-disruptive method.

B. Medical Imaging Data Management in CCmH

Since remote monitoring/handling is an essential tool in the CCmH paradigm, medical imaging becomes more important compared to the classical face-to-face treatment models. Reference [10] focuses on the cloud side, where a Hospital Management System (HMS) is created to provide fundamental connectivity between the home and primary healthcare systems. This framework is optimized for handling compressed medical images, providing efficient and fast-access storage, fast mobile access, preserving security and privacy requirements, and conforming to the healthcare standards, such as HL7 and HIPAA.

C. Mobile Health Record (MHR) in CCmH

The shift from Electronic Health Record (HER) to Mobile Health Record (MHR) is inevitable once smartphones become prominent interfaces for interconnecting patients to the healthcare space. Reference [6] discusses MHR for CCm in terms of privacy and security mandates, where the cloud providers are expected to support security of MHRs against external attacks. There are methods to cover the secure handling and storage of the MHRs information, which will be discussed in Section 5.

D. Government Regulations for CCmH

From governments' perspectives, the following mandates are of great importance [8]:

- Having a physical cloud located inside the governments' territories.
- Mitigating existing and new security threats, rising the need for deploying Security as a Service to adopt both public and private clouds.
- Combat the possibilities for Denial of Service (DoS) and in particular; Distributed DoS attacks.
- Investigate cloud services for public health, science, education, and law enforcement responses.

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.61 e-ISSN: 2251-7545

E. Cellular technology requirements for CCmH

There are numerous cellular technologies that can be deployed in the CCmH picture. A cellular network covers the interaction between the smartphone and tower. The tower is tied to the back-end of the cloud either directly or indirectly. The Third Generation Partnership Project (3GPP) oversees the progression of many of the most recent cellular technologies, including HSPA (High Speed Packet Access), EEDGE (Evolved Enhanced Data Rates for GSM Evolution), and LTE (Long Term Evolution). Different technologies limit the system based on the available bandwidth, delay budget, and data rate. Reference [10] covers these technologies and compares all the different limitations they have on bandwidth, delay, and data rates. For CCmH applications, it has been shown that LTE (then LTA-Advanced "LTA-A" as LTE's the next generation cellular technology) appears to offer relatively higher bandwidth with lower (network access, as well as, end-to-end) delays, with promising overall connectivity improvements, which is more suitable for CCmH applications.

F. Benefits and challenges of CCmH deployment

Most of the benefits and challenges mentioned in Section 3 are applicable here, however the more focused benefits are:

- Increased battery life due to efficient cloud network connectivity (e.g., connectivity-on-demand, low-power prolong connectivity)
- Easy management of HER, MHR, and Personal Health Record (PHR)
- Faster access to healthcare personnel to avoid health crises
- Easy creation and management of circle of trust in regards to the patient's health conditions
- Efficient access to medical information and data management both for the private and public sources.

More specific issues and challenges revolving around CCmH are [1], [14]:

- Personal security and privacy, which include: anonymity, authentication, authorization, encryption, and accountability
- Low bandwidth normally available to mobile usage specially during the peak hours
- Anywhere availability is another issue that mobile coverage is not available in all locations
- Interoperability between different mobile platforms
- Limitations on the processing power, memory, and on-device gadgets
- Reliability of mobile applications
- Limitations of Quality of Service (QoS) offered through cellular/Wi-Fi networks.
- Other challenges which often are not very much discussed but could have significant implications to the implementation, include: potential disruption in a loss of interconnectivity (e.g. termination of access due to vulnerability issues or natural disaster) and the strict regulations in some countries in regard to transfer and storage of data as many cloud providers especially the larger ones are based overseas or operate overseas servers. Other business related issues such as data ownership, use and control of data, are also of major concern.

V. Recommendations for CCmH deployments

The deployment of mHealth in the cloud space (CCmH) has a number of benefits and challenges, which have been discussed in this paper. In this section, the roadmap to better CCmH deployment is provided with the following set of recommendations:

A. Security and privacy for CCmH

As mentioned in Sections 3 and 4, security and privacy were the most important challenges of a diverse space like a cloud. The following security-related amendments require attention [14]:

- Security and privacy on the smartphone – Identity concealment and anonymity are required to preserve the user's privacy and security. Strong encryption and decryption algorithms are required. For this, NIST's requirements suggest the deployment of Suite-B algorithms [15], [16], [17], [18], [19].
  - Suite-B cryptographic algorithms, including: the Elliptic Curve Diffie-Hellman (ECDH) for the key agreement, the Advanced Encryption Standard - Galois/Counter Mode (AES-GCM) for the encryption-authentication, Elliptic Curve Digital Signature Algorithm (ECDSA) for the digital signatures, and the Secure Hash Algorithm (SHA) for message digest and integrity schemes. Suite-B uses Elliptic Curve Cryptography (ECC) exclusively for key exchange and digital signature.
- Security once the data is on the network – Since both centralized and distributed data topologies are possible in cloud computing, providing security measures for both topologies become very challenging and important, including: contact information, names, doctor notes, prescriptions, medications, medical information, and procedures, must all be protected using the strongest cryptographic algorithms available (e.g., Suite-B).
- Secure transmission – VPN-based (end-to-end secure tunnel) is suggested to reduce the possibility for inside or outside adversaries (both on the private and

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.61 e-ISSN: 2251-7545

public clouds) to have any chance to have access to the private information or alter/delete. For this issue, strong VPN/IPSec tunnels are suggested.

- SECURE STORAGE – Multi-redundant storage databases are required to store MHRs. This should be accompanied with very strong encryption techniques.
- ACCESS CONTROL – In particular, Role-based Access Control (RBAC) techniques would be ideal for cloud-computing environments, including [20]: context-aware approaches (dynamic and fine-grained mechanisms), identity protection, and data provenance incorporation. RBAC techniques are simple, flexible, support least privilege, and privilege management.
- AUTHENTICATION – An important security measure is to securely exam who accesses the resources and at the same time, the legitimacy of the resources accessed by authenticated user. A number of methods can be used in relevant APIs (Application Programming Interface) including [20]: Kerberos (ticket-based authentication protocol), LDAP (Lightweight Directory Access Protocol), Active Directory, NTLM (NT LAN Manager), RSA (Rivest, Shamir, and Adleman) public-key cryptography, X.509 (public key infrastructure "PKI" certificate system), and SAML (Security Assertion Markup Language, an XML-based open standard data format for authorization and exchanging authentication).
- PRIVACY-BY-DESIGN (PBD) – One of the most effective strategies for mitigating privacy risks is through a concept called Privacy-by-Design (PbD). PbD is based on the fact that privacy needs to be considered from early stages of the design of a system. This is to ensure that the possibilities for privacy breaches are dealt with throughout various levels and layers of the system design and not just through providing preventive patches. PbD is built on top of the following seven principles (adapted from [21, 22]): "proactive not reactive; preventative not remedial, privacy as the default, privacy embedded into design, full functionality: positive-sum, not zero-sum, end-to-end lifecycle protection, visibility and transparency, and respect for user privacy.

B. INTEROPERABILITY FOR VARIOUS CCMH PLATFORMS

As mentioned, there are many platforms on the network and not all of them are interoperable. Open Source approaches, such as Android platform are required or a translator medium to translate between various platforms and formats are required.

Figure 4. Logical view of Network-Cetric Healthcare Operations (NCHO) (adapted from [23-25])

C. SCALABLE QOS SCHEMES FOR CCMH

Scalable QoS approach for CCmH can become a tricky issue when too many clients are trying to access heavy loads of mHealth data with multimedia contents. For this matter, load sharing techniques are required to balance the data delivery according to the location, application, and user mandates.

D. BIG DATA ISSUE FOR CCMH

Aggregation and management of medical information and its efficient transmission across networks and cloud are very challenging. The current approach to managing large amount of health-related data (i.e., Big Data) requires non-SQL data storage/access schemes, such as those used in Hadoop, which are based on efficient data aggregating methods, data classification and characterization (e.g., deep-packet inspection) techniques [26].

E. PRIORITY DEPLOYMENT OF CCMH IN THE M-INDUSTRY SPACE

The number of cloud-based applications that smartphones will cover is expected to grow exponentially, including [27]: m-banking, m-education, and m-education. Providing scalable priority to mHealth applications is a challenging task, especially when the number of mobile-based applications is not bounded. For this, guaranteed classes of priority need to be established for extremely high priority applications, such as health, which may call for self-organizing classes of priority.

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.61 e-ISSN: 2251-7545

VI. Discussion

With the advances in cloud computing, there is clearly a benefit to healthcare delivery by embracing mHealth in the cloud space. However the ultimate and far reaching benefit lies in the ability to support a NCHO (Network-Centric Healthcare Operations Approach (Figure 4).

Network-centric healthcare operations have been discussed in detail [24, 25, 26]. In particular what von Lubitz and Wickramasinghe have established is that if healthcare is ever going to meet its objectives of delivering effective and efficient quality care, it is imperative that a network-centric perspective is adopted. What we have presented in this paper is the necessary steps to design and deploy successful mHealth solutions in the cloud space. By so doing, it will then only be possible to truly design appropriate and successful network-centric healthcare initiatives.

VII. Conclusion

The deployment of mHealth in the cloud space (Cloud Computing Mobile Health "mHealth" or CCmH) has a number of benefits and challenges, which have been discussed in this paper. We presented an introductory summary to cloud computing and summarized the advantages and challenges concerning cloud computing. Then we discussed the idea of mHealth deployed in cloud computing. We concluded a set of recommendation regarding the security and privacy of CCmH, interoperability issues, scalable Quality of Service (QoS), and medical data aggregation for CCmH. We believe providing supports for the security and privacy for smartphone is going to be challenging and vital, in particular to mHealth. This includes supporting local, distributed, centralized data as well as data on the move.

Cloud Computing Mobile Health is still in its infancy with promising potentials and the set of recommendations provided in this paper should draw the community's attention to the current issues and challenges, which should be addressed before cloud computing can be fully exploited.

REFERENCES

[1] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches",Wireless Communicatios and Mobile Computing, Wiley Online Library, Oct. 11, 2011, DOI: 10.1002/wcm.1203

[2] Charalampos Doukas, Thomas Pliakas, Ilias Maglogiannis, "Mobile Healthcare Information Management utilizing Cloud Computing and Android OS", 32nd Annual International Conference of the IEEE EMBS, Buenos Aires, Argentina, August 31 - September 4, 2010

[3] "Cloud Computing", Wikipedia, Retrieved on June 09, 2012, http://en.wikipedia.org/wiki/Cloud_computing

[4] Keith Combs, "What is Infrastructure as a Service (IaaS)?", April 4, 2012, http://blogs.technet.com/b/privatecloud/archive/2012/04/04/what-is-infrastructure-as-a-service-iaas.aspx

[5] An Overview of the Amazon PaaS, Platform-as-a-Service, Transcend Computing, 2012, http://www.transcendcomputing.com/wp-content/uploads/2012/04/An-Overview-of-the-Amazon-PaaS.pdf

[6] Gonzalo Fernandez, Isabel de la Torre-Diez, Joel J. P. C. Rodrigues, "Analysis of the cloud computing paradigm on Mobile Health Records Systems", International Workshop on Extending Seamlessly to the Internet of Things (esIoT-2012) - IMIS-2012, Palermo, Italy, July 4-6, 2012

[7] Leslie Willcocks, Will Venters, Edgar A. Whitley, "Meeting the challenges of cloud computing", Accenture, May 2011, http://www.accenture.com/us-en/outlook/Pages/outlook-online-2011-challenges-cloud-computing.aspx

[8] Kim-Kwang Raymond Choo, "Cloud computing: Challenges and future directions", Australian Government, Australian Institute of Criminology, No. 400, October 2010

[9] Jian Zhen, "Five Key Challenges of Enterprise Cloud Computing", Cloud Computing Journal, Nov. 16, 2008, http://cloudcomputing.sys-con.com/node/659288

[10] S. Adibi, A. Mobasher, T. Tofigh, "LTE Networking: Extending the Reach for Sensors in mHealth Applications", Transactions on Emerging Telecommunications Technologies (ETT), Wiley, Published on January 10, 2013

[11] Sasan Adibi, "Link Technologies and BlackBerry Mobile Health (mHealth) Solutions: A Review", IEEE Transactions on Information Technology in Biomedicine, July 2012

[12] Abderrahim BOUROUIS,Mohamed FEHAM, Abdelhamid BOUCHACHIA, "A New Architecture of a Ubiquitous Health Monitoring System: A Prototype of Cloud Mobile Health Monitoring System", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012

[13] Suraj Pandey, William Voorsluys, Sheng Niu, Ahsan Khandoker, Rajkumar Buyya, "An Autonomic Cloud Environment for Hosting ECG Data Analysis Services", Future Generation Computer Systems, Volume 28, No. 1, Pages: 147-154, ISSN: 0167-739X, Elsevier Science, Amsterdam, The Netherlands, January 2012

[14] Sasan Adibi, Gordon B. Agnew, "On the diversity of eHealth security systems and mechanisms", Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC'08), pp. 1478-1481, Vancouver, Canada, August 2008

[15] S. Adibi, "An application layer non-repudiation wireless system: A cross-layer approach", PhD thesis, Electrical and Computer Engineering Dept., University of Waterloo, September 27, 2010

[16] S. Adibi, "An Application Layer Non-Repudiation Wireless System: A Cross-Layer Approach", published and presented at the Ph.D. Forum at the Eleventh IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '10), Montreal, Quebec, Canada, June 14-17, 2010

[17] S. Adibi, Tony Sahama, "Information Accountability for eHealth Infrastructures through Quality of Service (QoS) Support", published and presented at the Advances in Health Informatics Conference (AHIC '10), Kitchener, Ontario, Canada, April 28-30, 2010

[18] S. Adibi, C. Labrador, "Suite-B Elliptic Curve Cryptographic Scheme for eHealth-based Networks" published and presented at the Security and Trust group (WG7), 24th Wireless World Research Forum (WWRF-24), Penang Malaysia, April 12-14, 2010

[19] S. Adibi, C. Labrador, "BlackBerry mHealth Solution", published and presented at the Short-range Radio Communication Systems group (WG5), 24th Wireless World Research Forum (WWRF-24), Penang Malaysia, April 12-14, 2010

[20] H. Takabi, J. B. D. Joshi, G. Ahn, "Security and PrivacyChallenges in CloudComputing Environments", IEEE Journal of Security and Privacy, Vol. 8, Issue 6, Pages: 24-31, Nov-Dec 2010

Doi: 10.7321/jscse.v3.n3.61 e-ISSN: 2251-7545

[21] Ann Cavoukian, "Privacy-By-Design Principles", adapted from http://privacybydesign.ca, Retrieved on Novmber 20, 2012
[22] S. Adibi, R. Dara, N. Wickramasinghe, C. Chan, S. Varadarajan (2012) Privacy-Enabled Mobile-Health (mHealth)-based Diabetic Solution, Accepted at SpringerSmart Data Proceedings on August 24, 2012
[23] D. V. Lubitz, N. Wickramasinghe, and G. Yanovsky (2006) Networkcentric Healthcare Operations: The Telecommuniucations Structure, International Journal of Networking and Virtual Organizations (IJNVO) , Vol. 3, No. 1 pp. 60-85
[24] D. V. Lubitz, N. Wickramasinghe (2006) Network-centric healthcare: applying the tools, techniques and strategies of knowledge management to create superior healthcare operations, Int. Journal of Electronic Healthcare, Vol. 2, No. 4, pp.415–429
[25] D. V. Lubitz, N. Wickramasinghe (2006) Healthcare and technology: the doctrine of networkcentric healthcare, International Journal of Electronic Healthcare, Inderscience, Vol. 2, No. 4/2006, pp. 322-344
[26] S Kaisler, F Armour, JA Espinosa, W. Money, "Big Data: Issues and Challenges Moving Forward", The 46th Hawaii International Conference on System Sciences (HICSS), pp. 995 - 1004, Big Island, Hawaii, January 7-10, 2013
[27] S. Goundar, Fiji, "Cloud computing: Opportunities and issues for developing countries", DiPLO, Diplomacy, 2011, http://www.diplomacy.edu/sites/default/files/IGCBP2010_2011_Goundar.pdf