Cloud Computing for Enhanced Mobile Health Applications

M.T Nkosi, F. Mekuria SM IEEE
CSIR Modelling and Digital Sciences
Mobile Computing & Security Unit
Meiring Naude Road, Pretoria 0001, South Africa
mnkosi@csir.co.za, fmekuria@csir.co.za

Abstract

Mobile devices are being considered as service platforms for mobile health information delivery, access and communication. However mobiles face challenges with regard to delivering secure multimedia based health services due to limitations in computation and power supply. Since mobile devices have limited computational capacity and run on small batteries; they are unable to run heavy multimedia & security algorithms. In this paper a cloud computing framework to relieve mobile devices from executing heavier multimedia and security algorithms in delivering mobile health services is described. The proposed framework uses a Cloud Computing protocol management model which intends to provide multimedia sensor signal processing & security as a service to mobile devices. Our approach suggests that multimedia and security operations can be performed in the cloud, allowing mobile health service providers to subscribe and extend the capabilities of their mobile health applications beyond the existing mobile device limitations.

Keywords **–**Multimedia DSP, Security, cloud computing, Mobile health application.

1. Introduction

Mobile phones as service platforms can provide several societal, business and governmental services. Hence, serious applications, like bank transactions, can now be performed on a mobile device, constituents can send SMS requests to their representatives in parliament, and people can access health information through text enquiries. Further developments will allow mobile devices with unique features that can sense the environment and physiological parameters to enhance quality of life and remote monitoring of patients [1]. However, mobile devices as compared to desktops computers have limitations in computational capacity and power consumption[2]. These limitations must be acknowledged when developing mobile applications and hinders them from functioning in a more or less acceptable capability and reliability like desktop computers. Users of desktop PC based online applications have become comfortable with accessing more sensitive health applications via the Internet.

Securing mobile health applications running on a mobile device is therefore an important area, if we want the applications to be trustworthy and reliable. In this article a frame work and protocol based on cloud computing is proposed to enhance the capability of mobile devices for use in advanced sensor based health care and monitoring applications.

The emergence of cloud computing in the research space promises to solve some of the concerns facing mobile computing platforms. The following definition is used: Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), so we use that term. The data-center hardware and software is what we will call a Cloud.

Hence, cloud computing could be regarded as an unlimited resource that can be accessed anytime and anywhere in the world. This is in direct contrast to having servers inside organisation's premises to run applications. Irrespective of several concerns against cloud computing, it is envisaged as an answer to questions about capability of mobile devices to function equally as desktop computers [4]. Mobile health services are one of the applications that can benefit from the combination of mobile & cloud computing technologies. Building a converged and trusted network infrastructure and mechanism for mobile cloud computing is undertaken in this paper, to promote mobile health monitoring services.

There are a number of computationally intensive operations that can be offloaded onto the cloud, when considering multimedia services using ubiquitous mobile devices. Among these are multimedia sensor signal processing and security management operations which have not been given much attention in mobile cloud computing research field. In this paper a proposal is presented to use cloud computing for mobile health management which also addresses security concerns in mobile cloud computing.

2. Related Work

A number of cloud based mechanisms are being suggested to protect mobile devices and improve the capacity & reliability of mobile devices. The offloading approach is proposed in [7] which address the outsourcing of execution of heavy application to the surrounding systems called surrogates. In this approach, when a mobile device has to run a heavy application, it sends that application to a close by surrogate system that will execute it and sends the output to the mobile device. Byung-Gon and Petros [4] proposed a cloud based architecture that present a technique to combat problem of smartphones limitations in terms of computation, memory, and energy reserves. In their architecture, a smartphone is cloned and its execution offloaded to a computational infrastructure hosting a cloud of clones. In that way, a mobile device is relieved from running heavier applications. From both offloading approaches mentioned above, security concern is not addressed.

3. Model Security Layer

Application development on its own is a challenge; it gets even more complicated when one has to think about the limitations of mobile devices and securing the applications. Running secure multimedia signal processing algorithms in mobile applications turns to be a burden for developers as mobile devices have limited computational capacity. With the current business model, organisations spend a lot of money in buying or developing software applications to provide or access services. Furthermore, security of applications must be built in inside the infrastructure so as to protect data flowing through the various nodes. And when security has been added it must be well managed from time to time to keep it up to date to fight new security threats.

The concept of cloud computing seeks to come up with a new business model whereby companies can outsource IT infrastructure (data storage, computation, etc) and other services to the cloud. It promises to benefit companies, more especially small businesses, by minimising costs as they will not have to buy expensive hardware to store data in their premises. But one may wonder how can organisations, that have already invested a lot of money to build IT infrastructure, benefit from the concept of cloud computing? The continuous growth in technology has an impact on users, including organisations that have invested in building IT infrastructure. The rapid growth of technology comes with security challenges that can never be overlooked; hence security updates to protect existing infrastructure are a continuous necessity. Therefore, organisations that have invested in building IT infrastructure will benefit if security can be provided as services via the cloud. Furthermore, with advent of mobile technology, security concerns will not vanish anytime soon instead more innovations on security mechanisms are required to complement the technology[4,8]. A security management mechanism is therefore essential to address security issues in cloud computing. A successful security management mechanism will compel adoption of cloud computing by organisations.

In figure 1, a new security management model of mobile devices is presented. The model aims at separating applications and the management of their security, more especially in wireless or mobile computing environment. But the model can also be applicable to desktop based applications if one wishes to minimise costs of running or implementing security applications. The incapability of mobile devices to execute heavy applications due to limited computational power motivated the proposition of this model. The work done by Byung-Gon and Petros [4] and Kun and Shumao [6] suggest offloading technique of applications execution from a mobile device to a close by computer connected to Internet. This approach raises a concern as to who manages security during the whole process. Like in the case of Byung-Gon and Petros architecture, when a mobile device is cloned to a computational infrastructure how can you be sure that results of computation will not be infected by viruses when it is loaded back to the mobile device? This can be a serious concern for those who want to adopt cloud computing for mobile applications. Consequently, in our proposed model we argue that a security can be provided as a service to protect mobile applications while a mobile device is cloned to an untrusted computational infrastructure. In so doing, there would be a security provider or vendor organisation that offers security to mobile devices. Mobile health application providers and users will not have to worry about security as it will be taken care of by security vendor.

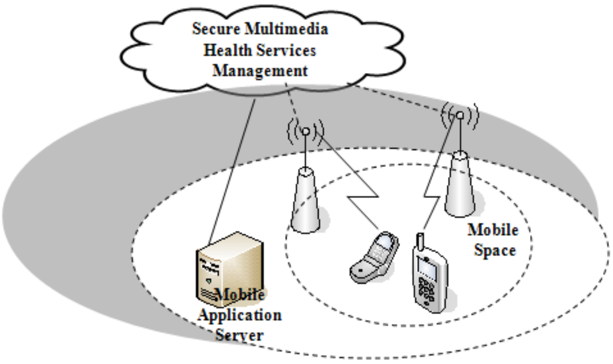


Figure 1: Cloud-Based Mobile Health Security Management

The concept of Security as a Service (SaaS) has been implemented in desktop systems to support small businesses [9] but not to mobile based technology services. SaaS means, security management is offered as a service to organisations that runs applications which must be protected against unauthorised access. For example, in our proposed model, when mobile devices request to access a particular application, security verification is performed in the cloud.

The proposed model intends to address or answer to security concerns in mobile devices. Some of security concerns to be addressed by this model are briefly discussed below:

- ***Secure Software Execution Environment***: viruses from malicious software can cause a serious negative impact to the functioning of a mobile device, therefore threat detection and prevention mechanism is required to avoid this impact.
- ***Secure Data Communication***: communication channel must retain privacy and integrity of data communicated to and from mobile applications.
- ***User Identification***: unauthorized access to mobile applications must be prevented.

- ***Secure Network Access***: only subscribers must be able to connect to network and access services.
- ***Content Security***: the content downloaded and stored in the mobile device must be utilised as per the terms set by the content provider.
- ***Secure Storage***: private and sensitive information must be protected from unauthorized access.

The above mentioned security concerns pose even more research questions in accordance with our proposed model. In this paper, we will address some of these concerns with respect to the proposed model. The following section will discuss the dimensions of security and show how the proposed model can address security issues at different levels.

4. Role of Cloud Computing

Research developments towards cloud computing will have a direct impact to a number of issues in existing technologies. Different approaches are necessary to successfully address those issues. Research efforts in cloud computing has identified services that can be delivered via the cloud. Below we list some of those services:

- Software as a Service (SaaS).
- Data storage.
- Sales force automation.
- Supply chain management.
- Hosted infrastructure (services, network capability).
- Hosted services (fully operational IT environment).

Services delivered via the cloud are dependent on other factors that affect cloud computing. More research will have to be undertaken to find ways to deal with these factors. Some of the aspects that will be affected by cloud computing are listed below:

- ***The volume of traffic in the network***: increased bandwidth will be required to allow fast connection to the Internet.
- ***Security Aspects***: a secure way to access services through Internet must be ensured.
- ***Business Models***: the way business is conducted will have to change to suit the cloud computing paradigm.
- ***Accessibility***: a reliable IT infrastructure must be in place to enable access to services.

Each of these aspects is an inevitable challenge that requires innovative approaches to address it. Our proposed model tackles security aspect and business model.

5. Cloud & Mobile Health

Today's mobile applications run in different platforms and serve diverse purposes. Future possibilities are that mobile networks will operate in an open model as the Internet [4,11]. Whereby applications developed and managed by different companies can run with cloud support. Mobile services require different levels of security to run on the cloud, depending on several factors. A service that transmits or stores sensitive health information will require a secure mechanism to protect applications as opposed to non-security-critical applications. Therefore, a varied layered security model is imperative to meet security needs of applications for running on cloud resources. Figure 2 illustrates a framework for a sensor based remote mobile health monitoring services. The framework focuses on mobile health applications and their limitations.

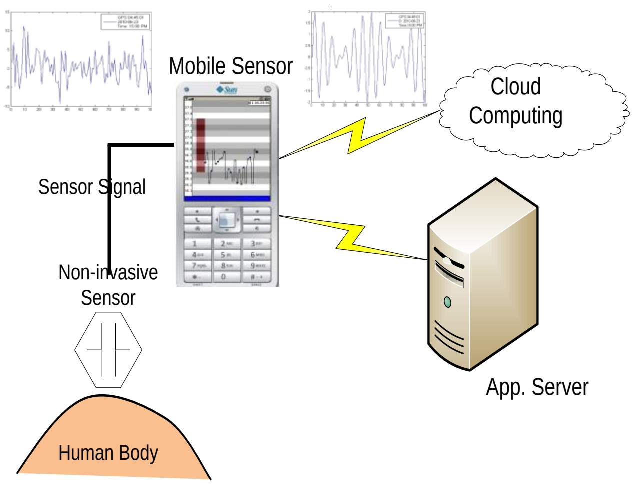


Figure 2: Sensor based Mobile Health Service

A basic idea of this framework is that a multimedia sensor signal processing will require increased power consumption for it to execute in a mobile device. To prevent this power drainage, the proposed model uploads complex computational algorithms to be executed in the cloud and final output is then uploaded back to the mobile device and the application server (AS). The model framework, therefore, classifies the required computational service request as weak and strong classes. The weak class requires low security and computation, and strong class complex multimedia processing and security. It is assumed that weak class offload request consumes less power and will be entirely performed in a mobile device and strong class is performed in the cloud with varied conditions. Furthermore, we innovatively propose a transitional performance of strong class multimedia and security verification. Transitional offloading where, part of (eg., 85%) a complex multimedia operation is performed in the cloud and the other remaining part (15%) is transferred to mobile device for completion. Mobile device is therefore expected to execute the remaining 15% and send a completion acknowledgement feedback to the mechanism in the cloud.

6. Sensor Signal Processing

Sensor signal are captured with environmental noise signals which makes the sensor signal unusable without signal enhancement and extraction to remove the unwanted additive noise signal. The signal-to-noise ratio (SNR) of the sensed signal can typically be in the region of 0 dB SNR, for many real world applications. Hence digital signal enhancement and extraction are crucial components of a mobile sensor based health monitoring system. Since the physiological or important information parameters are embedded in the waveform of the sensor signal, accurate and non-distortive sensor signal waveform extraction requires digital filter models which give a high magnitude attenuation for out-of-band frequencies and unwanted additive noise signal while preserving the linear phase characteristic of the filter to avoid distortion in the important sensor signal waveform. Such a digital filter transfer function characteristic is defined by:

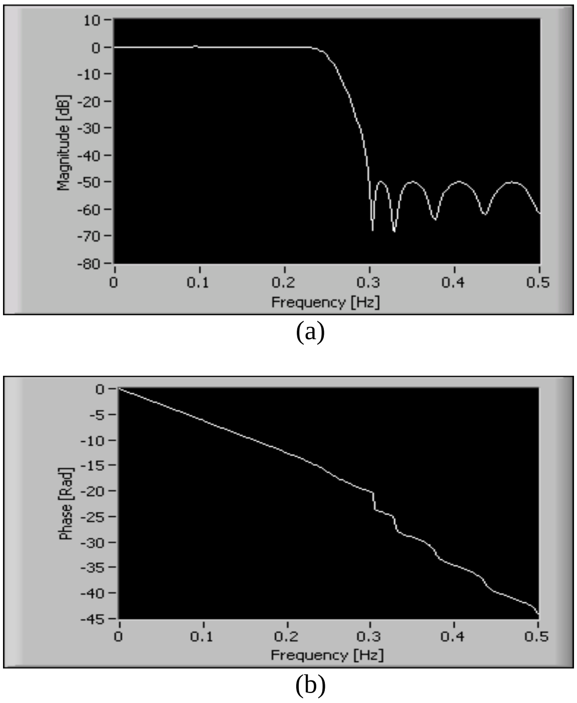
$$H(f) = |H(f)|e^{-j\varphi(f)} \quad \text{.............................} \ (1)$$

Where, |H(f)| is the magnitude or attenuation function of the filter, and $\varphi(f)$ is the phase function with respect to frequency. An ideal transfer function plot of a low-pass filter, with a normalized cut-off frequency of 0.3 Hz is shown in figures 6a-b. The filter characteristic depicts a 60 dB attenuation of out-of-band frequencies, while the phase characteristic is maintained linear within the pass-band (0-0.3 Hz). Such a signal enhancement filter characteristic for 1D sensor signals can be obtained using one of the two digital filter design methods, namely the Infinite Impulse Response (IIR) architecture described by equation (2), or Finite Impulse Response (FIR) model as given in equation (3).

$$\mathrm{y(n)} = \sum_{k=0}^{N} a^k x^{n-k} - \sum_{k=1}^{M} b^k y^{n-k} \ \text{........}(2)$$

$$\mathrm{y(n)} = \sum_{k=0}^{N} a^k x^{n-k} \quad \text{..............................}(3)$$

Where $a_k$and b_k are the filter coefficients, x(n) is the input and y(n) is the output of the filter, M & N are the sizes of the recursive and non-recursive parts of the filter. Figure 3, shows and ideal digital filter characteristics for sensor signal enhancement. We assume that such 1D or 2D signal enhancement digital filters can run either in the mobile sensor device in the case of smart phones, or the operation is offloaded to the cloud for processing in the case of limited capacity client mobile devices[6,14].



(a)

(b)

Figure 3. Ideal sensor signal filter characteristics

7. NGN & Health Services

The all-IP network vision of next generation networks (NGN) allows support for authentication, and offloading of mobile services based on the IP multimedia subsystem (IMS) standard [13,14]. The convergence of IP, fixed and mobile networks in the NGN-IMS architecture raises an important issue to combine mobile and cloud computing [10,16]. How can the SIM (subscriber identity module) based authentication and mobile computing defined in the 3GPP-IMS standard is suitable for:

1- Easy service creation, and integration of convergent services.
2- The definition and allocation of authentication keys for the various mobile services, a subscriber wants to access with a single device.

Although the 3GPP Generic bootstrap authentication (GBA) architecture allows for different kinds of authentication based on service requirements [4,5], service oriented scalable security architecture will be required, for this to be effective. The question: who should be responsible to define the level of authentication needed for health services, is crucial. Should health service providers who develop the content and services do the job or the network operator, who owns the network? This is a contentious issue which requires regulatory intervention and the setting up of a general guideline for promoting successful launch of the myriad of innovative mobile services services expected to appear in the near future [8,12].

In the meantime, NGN based services such as circuit/packet switched voice services and web based health monitoring services can be improved with a flexible cloud computing architecture [4,7,11]. At the same time Next Generation mobile broadband services require multimedia content and the involvement of service providers to set the required level of security. The use of cloud computing architectures is expected to complement the 3GPP-IMS standards in improving the execution of multimedia health and security mechanisms for increased reliability and efficient provision of next generation innovative mobile health services. Mobile network operators and mobile based health service providers are gearing up to provide next generation ubiquitous health monitoring systems based on the integration of IMS and the cloud computing paradigms[11,13]. Figure 4 shows a block diagram of a health monitoring system that uses mobile device as an IMS client. In figure 4, a non-invasive (NI) sensor is used to obtain the necessary sensor signal which is fed to a digital signal processor (DSP) embedded in the IMS client. The DSP is used to extract the physiological information necessary for health monitoring and decision support. In case of limited capability IMS client device, the IMS client can also offload the signal processing into a cloud resource, which could be operated by either the network operator or a service provider. The session initiation protocol signalling (SIPS), the SIP event packet (SIP-EP) connect the IMS client to the call session control functions (CSCF). The CSCFs are essentially SIP proxy servers, supporting IMS signalling and session control functions. The database management system (XDMS), controls and organizes data created by the health monitoring services. The application server (AS) contains the ongoing mobile service and the transcieves data to-and-from the IMS client. The AS also acts as a subset (for health related data) of the home subscriber server (HSS), which is the central repository of mobile user-related information. At the other end, the IMS system monitor acts as the recipient and interpreter of the sensed physiological information, and communicate back the necessary decision and action to be taken.

The system described in figure 4, is simulated using the IMS based service development API and Testbed. It further uses J2ME (Java mobile edition) libraries to exploit the IMS functionality for the client and core network nodes [11,12].

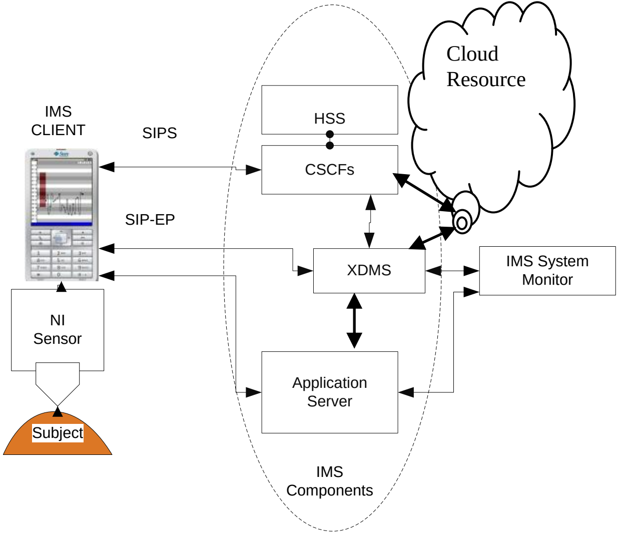


Figure 4. IMS-based Mobile Health Monitoring with Cloud Support

8. Conclusion and Future Work

Cloud computing technology and sciences can be used to alleviate limitations of ubiquitous mobile devices for use as service platforms in a number of societal applications. Mobile health monitoring and management is one example shown in this paper. The system described in this paper uses an NGN/IMS system with cloud computing to reduce the burden of organizing and improving the functions of existing mobile health monitoring systems. This will improve the utilization of the ubiquitous mobile device for societal services and promote health service delivery to marginalized rural communities. However, necessary functional testing of the IMS protocols, for secure transportation of sensor signals to-and-from the supporting cloud computing resources should be made with care. The interaction between health service provider, IMS network operator and cloud computing service providers should be regulated so as identity management and security verification is performed in accordance with accepted standards. The transitional execution and synchronization necessary for cloud offloading of computationally heavy algorithms will require more research with regard to IMS client capability, to look at which part of applications must be performed in the mobile device and the computationally intensive part that could be executed by the cloud. Involvement of medical professionals and users in the design of the health monitoring system is crucial for the usability and sustainability of such mobile health services.

9. References

[1] Y. Lin and I Chlamtac, *Wireless and Mobile Network Architecture* (Book Style).Robert Ipsen, USA: John Wiley & Sons, 2001, pp.15–37.

[2] F. Koushanfar, M. Potkonjak, V. Prabhu, J. Rabaey, “Processors for Mobile Applications”, in *IEEE International Conference on Computer Design (ICCD’00)*, pp.603, September 2000.

[3] A. Agarwal, D. Gupta, “Security Requirements Elicitation Using View Points for Online System”, *First International Conference on Emerging Trends in Engineering and Technology*, pp.1238-1243, July 2008.

[4] B. Chun, P. Maniatis, “Augmented Smartphone Applications Through Clone Cloud Execution”, *12th Workshop on Hot Topics in Operating Systems*, Monte Verita, Switzerland, May 2009

[5] 3GPP TS 33.220; “Generic Authentication Architecture (GAA). Generic Bootstrapping Architecture (GBA)” ; December 2006.

[6] K. Yang, S. Ou., “On Effective Offloading Services for Resource-Constrained Mobile Devices Running Heavier Mobile Internet Applications.” IEEE Communication Magazine, pp.53 – 63, January 2008.

[7] S. Beji, N. E. Kadhi, “An Overview of Mobile Applications Architecture and the Associated Technologies”, *The 4th Intern. Conference on Wireless and Mobile Communications*, pp. 77 – 83, July 2008.

[8] F. Mekuria, “Issues in Mobile Broadband Networks & Services.” Proc. of the IEEE Mobile for Development, M4D2008, 10-12, Dec. 2008, Karlstad, Sweden.

[9] Armbrust et.al.,“Above the clouds: A Berkeley View of cloud compuring.” http://radlab.cs.berkeley.edu/. February 10, 2009.

[10] K. Rikitaki,et.al Ubiquitous Health Monitoring System, in Proc. of the 6th Annual IEEE Consumer Communications & Networking Conference (CCNC 2009), Las Vegas, Nevada, USA, Jan.2009.

[11] The open IMS core project: http://www.openimscore.org.

[12] S.Loreto, et.al. “IMS service development API and Test-bed” IEEE Communications Magazine, April 2010. Pp. 26-31.

[13] M. Weitzel, et. Al, “A web 2.0 model for patient centered health informatics applications.” IEEE Computer Magazine, July 2010.

[14] M.T. Nkosi, F. Mekuria, ”Mobile Government for Improved Service Delivery.”, Proceedings of IST-Africa 2010, 19-21 May, 2010, Durban, South Africa.