Challenges in Wireless Bio-Sensor Based mHealth Development

Mzomuhle T. Nkosi, Fisseha Mekuria
Council for Scientific & Industrial Research,
CSIR-MDS, Mobile Computing & Security Unit
Meiring Naude Road, Pretoria 0001, South Africa
mnkosi@csir.co.za, fmekuria@csir.co.za

Samson H Gejibo
Dept. of Informatics, Centre for International Health,
University of Bergen, 5020 Bergen
P.O.Box 7800 Norway
Samson.Gejibo@cih.uib.no

Abstract

Healthcare providers are facing growing challenges in patient diagnostics and information gathering due to in-adequate infrastructure and insufficient number of health-care professionals to perform such operations. The traditional way of patient information gathering is largely based on text and dependent on self-report surveys and infrequent doctor consultations. The proposed bio-sensor based frame work can improve remote diagnostics and healthcare information gathering using mobile device based bio-sensor systems. Bio-sensor based systems can be used to gather relevant multimedia health information and improve the quality of remote diagnostic both for ambulatory and continuous monitoring of chronic diseases. The paper addresses bio-sensor signal processing and secure communication of sensor signals based on next generation mobile technology and bio sensors, with the aim to facilitate the development of secure and innovative mobile health services.

1. Introduction

Bio-sensors are typical example of sensor technology which is used to measure and track particular bio-medical conditions such as temperature, heart rate, blood pressure, weight, breathing, blood sugar, brain waves[18]. The research carried out at Roviera i Virgili University on bio-sensor development has shown that biosensors can detect bacteria at levels as low as 1 cell per 5 ml of water, allowing water to be tested for typhoid fever bacteria in only a few seconds [25]. Effort is being made to build-in sensors in mobile device platforms, sothat sensor data can be captured, processed and sent to a central location to improve existing healthcare services[2,3,8].

Mobile phone manufacturers have also understood the potential impact of sensors and are embedding different types of sensors in their smart-phone platform strategies. Some sensors already appearing in mobile platforms are accelerometers, digital compass, proximity sensor, gyroscope, GPS, microphone, and camera [2,19]. Based on the growing research and development in this area, there is strong indication that bio-sensors will be an integral part of ordinary cell phone and smart phone platforms [2,8]. The introduction of embedded sensors in mobile phone can benefit from better computing power, speed and memory as compared to standalone sensors. However, limitations due to mobile radio access infrastructure, security, low bandwidth and computing power still exist. Mobile bio-sensor data must meet the standards for fundamental elements of data quality that are expected by medical or other instrumental records and must comply with all applicable statutory and regulatory requirements [16,17]. In the exiting GSM/GPRS network, data is encrypted only between the Mobile station and Base transceiver Station (BTS). Providing a reliable end-to-end security for healthcare applications over next generation wireless networks is an active research area which this paper tries to contribute. Compromising patient related data damages the trusted relationship between the patient and healthcare care providers, and can result in legal consequences. The aim of this research is therefore to develop cost effective bio-sensor based health data capture, secure wireless transmission and storage of mobile bio-sensor data in a central location. The system is designed to be compliant with the Health Insurance Portability And Accountability Act (HIPAA) security standards and requirements[16]. HIPAA has well documented security and privacy requirements for electronic health data system. Compliance of mHealth with standards and regulatory requirements is a major driving force of this research. It is strongly believed that security and privacy guidelines, policies and standards are crucial components in healthcare service establishment. Therefore, participatory design where all stakeholders are involved is followed during the design and growth of the bio-sensor based mHealth application.

2. Impact of bio-sensors in m-Health

Bio-sensor enabled mobile phones have the potential to improve health information gathering both for ambulatory and continuous chronic disease monitoring applications. Increasing number of mobile subscribers and wide coverage of cellular networks create opportunities to support the health sector by reaching out to inaccessible society due to limited number of medical professionals, healthcare facilities and transportation. The first stage of mHealth revolutionized the way health data is collected from traditional paper based to electronic text data

capturing system using a mobile form agent[9]. It improved productivity, fast decision making process and fast response to the community who needs emergency help. UNICEF RAPID SMS implementation for supplies and logistics can be an example for emergency diagnostics in remote communities [15]. The UNICEF mHealth project significantly reduced the time needed to reach the information from the villages to the decision makers. Children under the age of five were saved from preventable diseases such as malaria & malnutrition. There is a strong indication that existing health care systems can benefit more from mobile phone and sensor integrated devices. The existence of GPS, location information and time tags can make mobile devices smarter and useful for healthcare services, through bio-sensor integration [2,18,19]. Mobile bio-sensor technology is expected to expand the boundaries of mHealth system by making possible personalized healthcare services. Sensor enabled mobile phone devices are going to revolutionize personal and social network based sensor data collection leading into the next generation of innovative and secure mHealth services [2,3, 19].

The basic technology in Figure 1 incorporates

- Noninvasive Bio-Sensor
- Mobile phone processing of sensor signal and Secure Radio Transceiver design.
- Web server and database for data storage, management and analysis

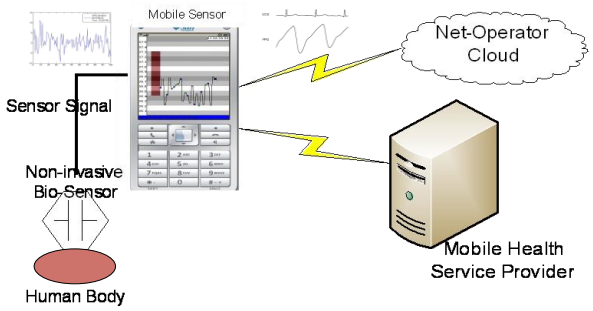


Figure 1. Bio-Sensor based mHealth system.

The design will also bring best practices from experiences such as the interactive tools on mobile phones which have been launched for the self-management of chronic diseases: (http://www.tplusmedical.co.uk/)

3. Bio-sensor signal processing

Bio-sensor signals are captured with embedded 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 a sensor 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 φ(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).

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

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

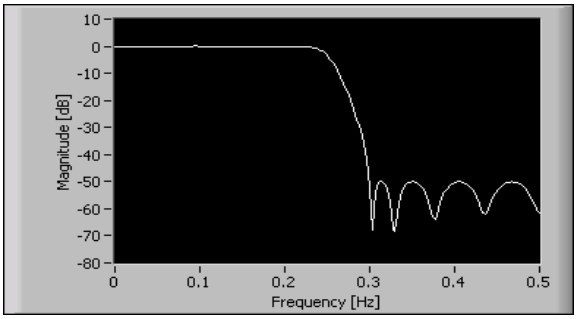
Where and are the filter coefficients, x^n is the input and y^n is the output of the filter, M & N are the sizes of the recursive and non-recursive parts of the filter. Figure 2, shows and ideal digital filter characteristics for sensor signal enhancement. We assume that such 1D or 2D signal enhancement 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 [3,19].

4. Cloud support for m-Health services

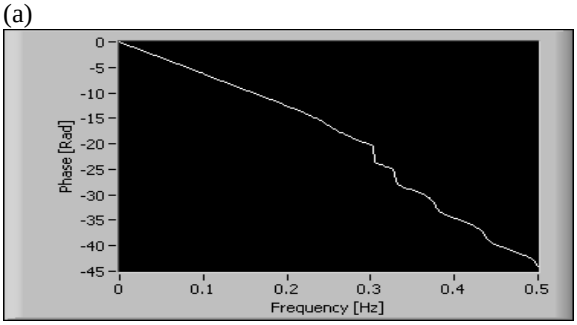
4.1 NGN & Cloud Concept

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 [7,26]. The convergence of IP, fixed and

mobile networks in the NGN-IMS architecture can be used as an important development to combine mobile and cloud computing [3,19].



(a)



(b)

Figure 2. (a)(b). Ideal sensor signal filter characteristics

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 [3,6]. 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[3,5,6]. 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 signaling (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 signaling and session control functions. The database management system (XDMS), controls and organizes data created by the health monitoring services. The health service provider (HSP) server contains the ongoing mobile service and supports the transceiving of data to-and-from the IMS client through the IMS system monitor. The HSP 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 HSP server system acts as the recipient and interpreter of the sensed physiological information, and communicates back to remote locations the necessary decision and action to be taken.

The system described in figure 3, 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, HSP and core network nodes [26].

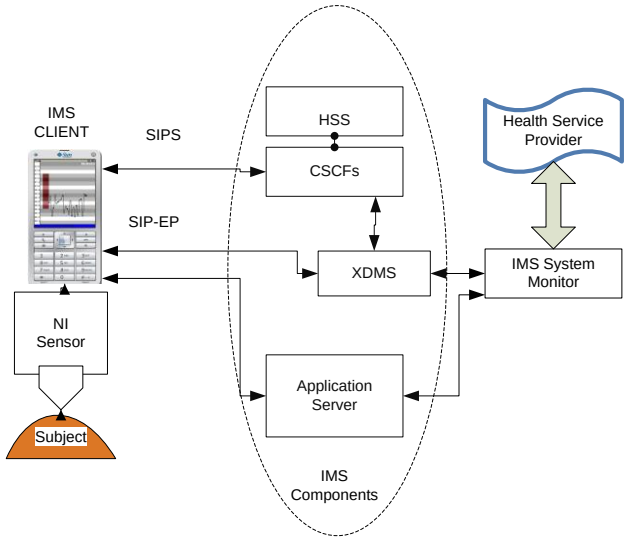


Figure 3. IMS-based Mobile Health Monitoring with Cloud Support

5. Security of bio-sensor based m-Health application

How can the SIM (subscriber identity module) based authentication and mobile service platform defined in the 3GPP-IMS standard become suitable for:

1- Easy service creation, and integration of convergent services.
2- The definition and allocation of authentication keys for the various mhealth 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 [7], 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 expected to appear in the near future [3,11].

In bio-sensor based mHealth systems, security will be a major challenge. Researchers have been proposing different security solution for standalone sensor network and few research has been done to address security issues of mHealth system [10,13]. Lack of mHealth standards, regulatory body and policy, and business model of mHealth system have contributed less efforts on securing mHealth. However, there have been several mHealth implementation in all corners of world and most of them are supported by Non-governmental organizations (NGOs), government, operators, vendors and manufacturers. Sustainability and Scalability of mHealth systems are determined by several factors and cost is one of the major factor. It is well understood that adding good security will increases the cost the system, therefore it needs considerable effort to address security issues in cost-effective manner. At the same time, the system security should be compliant with HIPAA or Food and Drug Association (FDA) [17] security requirements. We will consider built-in bio-sensors in smart phone and externally connected bio-sensors with feature phones. Our aim is to secure the entire mHeakth system.

6. Mobile terminals and security issues

There are about six major market leading mobile device platform. These are, Symbian, BlackBerry, Windows Mobile, Android, iPhone, and Java FX or Java 2 Mobile Edition (J2ME). The former five platforms are designed for smartphones and J2ME handles low end phones or feature phones. Smartphone shipments only make up 20% of total handset shipments, as of the first half of 2010 [2]. The rest 80% goes to less expensive feature phones. According to Gartner [27] Symbian leads the smart-phone market by 37% and followed by Android 25% and Apple iPhone with 17%. J2ME platform leads the feature phones market and most phone manufacturers such as Nokia, Sony Ericsson, Motorolla, LG, and samsung have it.

Security model differs from platform to platform and the security solution is dependent on the chosen platform. Smart-phones have access to advanced programming APIs which help to implement good security mechanisms rather than feature phones. The lack of secure application programming interfaces (APIs) in the feature phone forces secruity experts and developers to use external light weight security APIs such as BouncyCastle [22].

Authenticating user, pre-signal processing, keeping secure sensor data in the device storage, data access for authorized user, key management, and secure data upload are some of the day to day duties of mobile device. This can be easily achieved through smart phones but the challenge remains with feature phones. For instance, J2ME has record management store (RMS) to store data continuously. RMS stores data only as byte array and signal per-processing is a relevant step to digitized electrical signals of sensors output. The lack of J2ME security APIs for RMS data storage protection is one of the major challenges. External APIs can provide light weight cryptographic operations but increases the size of the application. Mobile Information Device Profile (MIDP) 3.0 [24] specification has been released and includes password based encryption (PBE) mechanism for data storage protection. However, there is no MIDP 3.0 supporting phone in the market and will take some years to see those phones in the market .

Key generation and management in resource constrained feature phones are the other challenges. In symmetric encryption algorithms, secret key generation and distribution determine the level of security. Key generation rely on the randomness the key generator. Th key generator depend on the random sources. Radioactive source and thermal noise are an example of unguesable random sources. In J2ME, the pseudorandom generator uses current time in milliseconds with 16 static bytes. Weak random source of J2ME leads the researcher to be able recover the symmetric keys and plaintext from Secure Socket Layer (SSL) session [14]. This is a critical issue and must be resolved.

Public-key cryptography key exchange protocol such as Deffie Hellman and widely used Rivest, Shamir and Adleman (RSA) are suitable protocol for advanced computer system. These protocols require computing resources and implementing them in low-end phones will have an impact on the performance of the devices.

The other key challenge in resource-costrained feature phones are insecure storage for public key ,symmetric key, and other authentication credetials. Subscriber Identity Module (SIM) card can be a protential solution for key and credentail storage. However, unlike the computers and laptops vendors, phone manufacturers and operators have control over the usage and access of SIM

card resources and they require signed midlet by right permission domain i.e., operator, manufacturer or third-party trusted domain. Choosing the right domain by itself is a challenge. For instance, if we choose operator domain, we will be limited to the cellular covage of the operators, and these days, in most countries, we can find more than one operators. Multi-phone manufacturers requires multi-signing if we pick manufaturer domain. The root certificate of third party such as Versign does not exist in some models and vendor phones. Furthermore, signing midlet require cost for code signing certificate for the domain.

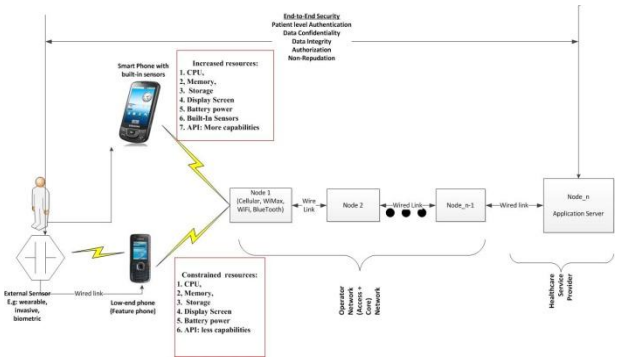


Figure 4. Sensor based mHealth System

7. Network security issues

In mHealth system, the data originating from the handheld devices and sent to the health care provider database must be secure, reliable and encrypted. Low-end phones access web services through Hyper Tect Transfer protocol (HTTP) in TCP/IP network. The data are send in clear all the way from hanheld to the server. J2ME MIDP 1.0 provides APIs for HTTP implementation without securing it. The later version, MIDP 2.0 came up with APIs HTTP Secure (HTTPS) implementation which provides security mechanisms for data integrity, certificate based authentication and confidentiality. The security in HTTPS are achieved by running HTTP over SSL or Transport Layer Security(TLS). One of the challenge with this protocol is in place with low-data-rate connection, lower-reliability networks and intermittent or non-existent non-local connectivity, SSL session establishment is difficult. In order to build server authentication, it requires certificate Authority (CAs) signed certificate and MIDP 2.0 does not provide certificate based client authentication. To address these challenges, new security protocol has to be proposed and implemented requiring hardware or software changes in the existing mHealth system. We need to make sure all incoming data from handheld devices must be received properly without modification and get notification to the sender to show all sent data are received.

Figure 5, End-to-end security model

8. Biometric m-Health Security

Taking into consideration that mobile and smart phone devices are more ubiquitous than normal desktops, it makes sense to give the mobile devices the ability to recognise the user and in doing so, allow a third party to have confidence in the mobile device and the user. The design of an end-to-end biometric based security using the model described in figure 5, is necessary to increase the security of existing technology supported health care systems. Considering the fact that use of embedded biometric authentication on a smart-phone will be common in the near future[2,19]. It will be possible to meet the standards of authentication and speed performance, while at the same time try to minimise resources such as mobile OS CPU, memory and power consumption.

A more reliable biometric security for mHealth system can be designed, using server or cloud resources for better performance, and avoiding the limitations inherent in embedded biometric. This will allow the main biometric functionalities and processes (Feature extraction, pattern Matching, Biometric database access, ...) to be hosted on a server while a minimum of essential signal processing such as biometric identity capture, enhancement, segmentation, preprocessing and feature extraction could be computed using the smart mobile phone capabilities. Another area which should be given adequate attention for a sustainable implementation of bio-sensor based mobile health deployment is the dimensions of security for mobile devices. As shown in figure 6, due to variations in capability of mobile devices and the type of services the mobile user is requesting to access, a scalable authentication algorithm is required to meet the different demands. A strong authentication demand can also put the service unusable by ordinary citizens of society. Therefore usability studies and HCI analysis based on context of the user communities is a requirement before the final implementation of an mhealth system [13,18].

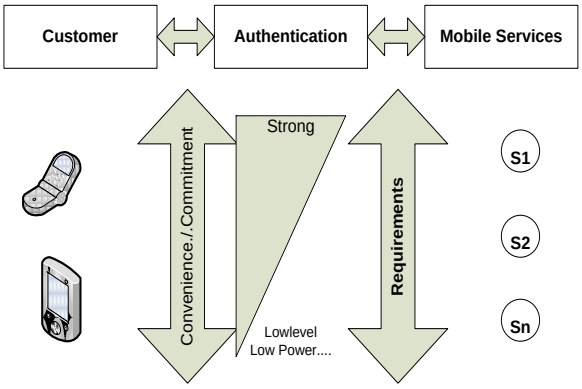


Figure 6, Dimensions of Mobile Health Security

9. A Case of m-Health

mHealth is one of the emerging innovative system of technology that promises to improve and build capacity in health care systems and community sectors in low income countries. Implementation of mHealth has been done in several countries. Most of these are based on text exchange using the openstandards openxdata, rapidSMS, javarosa, and Motech [9].

One of the Millennium Development goals (MDG) is to improve health and education sector by utilizing existing mobile technology and network infrastructure[23]. One such implementation was the Mellinium Village Project in Sauri Area, Nyanza province, in Kenya. The project was planned to run pilot on mHealth project for malaria and malnutrition prevention using mobile phones[20]. The project was aimed for reducing mortality rate of 11,000 children under the age of five due to malaria and malnutrition. In collaboration with medical professionals, training of 108 community health workers was done on site. The trainees were provided with mobile phone equipped with text and SMS capturing program, tools for malaria testing, and other necessary materials. The project pilot ran 3 months, managing the system technologically and coordinating community health workers, team managers, and health care professionals. The project used the Rapid Diagnostic Tests (RDT) for malaria testing which costed $1 per RDT and mobile texting to a health centre, resulting in saving lives and was described in a NYTimes article as "Shower of Aid Brings Flood of Progress"[1].

Development of a specialised camera enabled mobile phones for malaria testing was carried recently. This has the potential to substitute the use and throw RDT testing samples and the expensive instrument needed for testing at the health centres[2,8].

The project has shown that mhealth systems can improve existing community-based health care. Coordination and remote data-collection to health centers and professional decision support is communicated, reducing the time needed to process data from the ground to the decision makers. At the end of the project a wealth of health data information was collected which was used for statistical analysis and inference.

Figure 7. Rapid diagnosis tests tool (RDT)[24]

Combining such mobile health initiatives with advanced bio-sensors integrated with smart-phone platforms, is a next step. Innovative mHealth services and schemes can be designed to perform remote patient diagnostic. Accurate data (time and geographically tagged) can be captured, processed and securely transmitted to health centres. A number of initiatives by the mobile industry and health care providers are already underway to achieve this and improve existing text-based mHealth-care systems [1,2,3,8,11,19]. This paper is a contribution towards achieving that goal.

10. Conclusion

Advanced technology supported health provision is a must if countries are to overcome the limitations in the number of health professionals, increasing aging population, and reduce the spread of chronic diseases. Mobile technology and bio-sensor integration is one promising development that is expected to improve existing health care systems and lead into the next generation of personal health care systems. The paper has addressed issues pertaining to mobile health systems using bio-sensors. The ubiquity of the mobile device is taken as advantage to design ambulatory and continuous remote health monitoring, using existing mobile technology & networks. Sensor signal processing for secure transmission and storage is presented with a view to enhance bio-sensor signals and improve the quality of remote diagnostics. Finally security analysis pertaining to next generation mobile networks and terminals has shown that usability and collaborative design are important factors that determine the design and successful deployment of an innovative mHealth-care system.

11. References

[1] Arto Holopainen, A (2006) "Use Of Modern Mobile Technologies To Enhance Remote Healthcare Services", 6th Nordic Conference On Ehealth And Telemedicine, Helsinki, 31 August 2006

[2] Lane, D.L.et. al., " A survey of Mobile Phone Sensing." IEEE Communications Magazine. Sept. 2010, pp. 140-146.

[3] M. Nkosi, F. Mekuria, , "Cloud Computing for enhanced mobile Health Applications" Proceedings of the IEEE Cloud computing and Technology conference, CloudCom2010, Nov.30 - Dec. 3, 2010, Indiana, USA.

[4] B. Blobel and F. Roger-France, "A systematic approach for analysis and design of secure health information systems," *Int. Journal of Medicical Informatics.*, vol. 62, no. 1, pp. 51–78, 2001.

[5] 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.

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

[7] 3GPP TS 33.220; "Generic Authentication Architecture (GAA). Generic Bootstrapping Architecture (GBA)" ; December 2006.

[8] Barbara G. Goode, "Sensors Help Advance Health-Care",April-1,2006
http://www.sensorsmag.com/specialty-markets/medical-devices/sensors-help-advance-health-care-856

[9] OpenXdata: ww.openxdata.org RapidSMS: www.rapidsms.org ODK: www.opendatakit.org JavaRosa:http://www.open-mobile.org/technologies/javarosa-consortium

[10] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, Dec. 2004.

[11] M. Messina, : Implementing and Validating an Environmental and Health Monitoring System, 5th Interl. Conference on Info. Technology: New Generations (ITNG 2008), April 2008

[12] S. Gritzalis, J. Iliadis, D. Gritzalis, D. Spinellis, and S. Katsikas, "Developing secure web-based medical applications," *Med. Inform. Internet Med.*, vol. 24, no. 1, pp. 75–90, 1999.

[13] Nicholas D. Lane, Emiliano Miluzzo, Hong Lu, Daniel Peebles, Tanzeem Choudhury, and Andrew T. Campbell, "A Survey of Mobile Phone Sensing", AD HOC AND SENSOR NETWORKS, Dartmouth College, IEEE Communications Magazine September 2010

[14] Kent Inge Simonsen, Vebjørn Moen, and Kjell Jørgen Hole, "Attack on Sun's MIDP Reference Implementation of SSL", University of Bergen, 2006

[15] RapidSMS, "UNICEF RAPID-SMS LESSONS LEARNT" March 2009. Last visited: October 02, 2010. [Online] Available: http://www.rapidsms.org/wp-content/uploads/2009/07/RapidSMS-Ethiopia-Lessons-Learnt.pdf

[16] The Health Insurance Portability and Accountability (HIPAA): http://www.hhs.gov/ocr/privacy/
[17] Food and Drug Administration *(*FDA*):* http://www.fda.gov/

[18] Stewart Wolpin, "How smartphones could lead the digital healthcare revolution", last visited: January 6, 2011. [Online]. Available: http://dvice.com/archives/2010/12/how-smartphones.php

[19] F. Mekuria, et.al.. "Intelligent Mobile Sensing & Analysis Systems", Proceedings of 3rd CSIR Biennial conference, August 31-Sep.2, 2010, International Convention Center, Pretoria, South Africa.

[20] Matt Berg, Dr. James Wariero, Vijay Modi, "EVERY CHILD COUNTS – THE USE OF SMS IN KENYA TO SUPPORT THE COMMUNITY BASED MANAGEMENT OF ACUTE MALNUTRITION AND MALARIA IN CHILDREN UNDER FIVE", 15 October 2009

[21] Find Foundation for new diagnositcis, last visited: Novemeber 04, 2010 [online] Available: http://www.finddiagnostics.org/programs/malaria/find_activities/quality-ensuring.html

[22] Legion of the Bouncy Castle, http://www.bouncycastle.org/

[23] Millennium Development Goals (MDG):
http://www.un.org/millenniumgoals/

[24] JSR-000271 Expert Group, Mobile Information Device Profile for Java 2 Micro Edition. Version 3 Java Community Process, 2009.

[25] R. Thusu, et. al., "Strong Growth Predicted for Biosensors Market", October 1, 2010, last visited: December 6, 2010. Available: http://www.sensorsmag.com/specialty-markets/medical/strong-growth-predicted-biosensors-7640

[26] S.Loreto, et.al. "IMS service development API and Test-bed" IEEE Comm. Magazine, April 2010. Pp. 26-31.

[27]Gartner, Inc, November 10, 2010, last visited: December 01, 2010. [Online]: http://www.gartner.com/it/page.jsp?id=1466313

[28] Jeferey Gettleman, "Shower of Aid Brings Flood of Progress", The NewYork Times, March 8, 2010
http://www.nytimes.com/2010/03/09/world/africa/09kenya.html