2016 4th International Conference on Future Internet of Things and Cloud Workshops

Mobile Health (m-health) System in the context of IoT

Sultan H. AlMotiri
Department of Computer Science
Umm Al-Qura University
Saudi Arabia
Email: shmotiri@uqu.edu.sa

Murtaza A. Khan
Department of Computer Science
Umm Al-Qura University
Saudi Arabia
Email: makkhan@uqu.edu.sa

Mohammed A. AlGhamdi
Department of Computer Science
Umm Al-Qura University
Saudi Arabia
Email: maeghamdi@uqu.edu.sa

***Abstract*—In this paper we describe the mobile health (m-health) system in the context of Internet of Things (IoT). We describe the fundamental characteristics of m-health devices such as compactness, IP connectivity, low-power consumption and security. We discuss acquisition of mobile health data via medical gadgets and wearables and application of this data in monitoring various health conditions such as blood sugar level, ECG, blood-pressure, asthma, etc. Security is very critical for IoT based m-health system. We address the issues of confidentiality, privacy, and security in the context of secure m-health system. We listed several measures to protect the information of patients and m-health system. The m-health system will benefit the patients in many ways such as quick diagnosis, remote monitoring and home rehabilitation. Overall m-health system will significantly reduces healthcare cost and unnecessary hospitalizations.**

I. Introduction

Mobile health (m-health) refers to the use of mobile devices in collecting health data in real-time from patients, storing it to network servers connected to Internet. The data can be access by heterogeneous group of clients (e.g., hospitals, health-insurance companies, etc). The m-health data is used by doctors to monitor, diagnosed and treat patients. Availability of wearable medical devices and body sensor networks giving rise to mobile health. Integration of mobile health devices in the patient's environment provides capabilities to predict health anomalies in real time [1]. Latest developments in micro and nano technologies as well as in information processing and wireless communication offer the possibility for smart miniaturization and non-invasive biomedical measurement as well as for wearable sensing, processing and communication. Mobile health technology will be the key of personal health-care services in future.

Internet of Things (IoT) is an environment of a variety of things such as RFID tags, medical devices, mobile phones, etc. These devices connects through unique identifiers and interact with each other [2], [3]. IoT connected devices transfer data between each other, in turn leading to new derived data.

Health care is one of the most important application areas of IoT. It provides opportunities to several medical applications such as mobile and remote health monitoring. The integration of wearable devices and systems in IoT provides better m-health services. Medical devices generates data and send to designated computer servers. Pervasive medical sensing and mobile technology deployed on IoT systems lead to the accumulation of big data [4]. The data provides information about the patients in real-time which can lead to diagnosis, treatment or hospitalization in case of of medical emergency. Consequently, IoT infrastructure, smart health monitoring devices, and wireless communications provides enormous possibilities of improvement in the quality of health services. The concept of m-health in the context of Internet of Things (m-IoT) brings the promises of better health management system by efficient scheduling of limited resources by ensuring their best use and service of more patients. IoT based m-health services will benefit the people by saving their time and money of visiting hospitals unless there is real need of it.

The essential parts of m-health and IoT are medical devices equipped with sensors and communication devices. These medical devices are infact smart devices that can be used to monitor various parameters such as sugar-level, blood-pressure, heart-rate, etc. Intelligence algorithms analyze the m-health data in real-time to identify certain patterns and raise different alert levels such as normal, cautious, emergency, etc., depending upon the condition of the observed patients. The volume of data at IoT servers is very large as it is collected from million of individual users or patients. This medical data can be access by various organizations such health-insurance companies, hospitals, government, etc. Different level of privacy control mechanism is applied depending upon who access the data and what is permissible? Nationwide health records of patients are maintained via centralized medical server and database to access the information anytime and anywhere.

II. Related Work

In the last few years, IoT based m-health system attracted attention of several researchers to investigate the potential benefits and challenges of future of health-care system. The deployment of IoT technology in the medical field is very much dependent on information and communication technologies (ICT).

A review about the contemporary status of research and future challenges on smart wearable health applications is presented by [5]. The authors conclude that the scope of telemedicine will continue to broaden in future due to latest developments in nano-technologies, information processing and wireless communication. The work of [1] presents a knowledge acquisition and management platform for personalized health based on the Internet of Things (IoT). The potential benefits of using m-IoT in non-invasive glucose level

978-1-5090-3946-3/16 $31.00 © 2016 IEEE
DOI 10.1109/W-FiCloud.2016.24

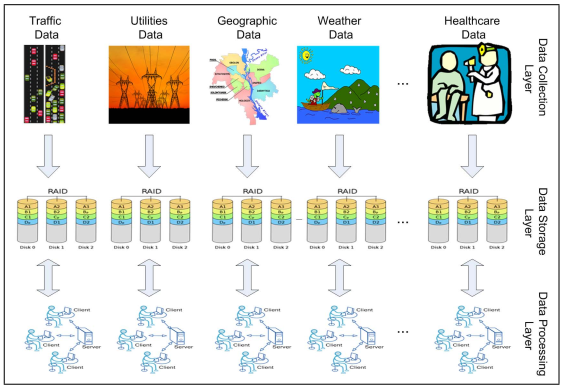

Fig. 1. Multi-layer architecture of IoT system

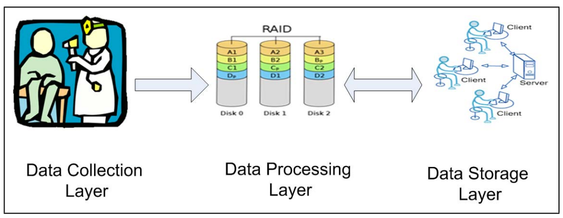

Fig. 2. Mobile health (m-health) architecture, a part of IoT.

sensing and the potential m-IoT based architecture for diabetes management is described by [6]. An intelligent Augmented Quick Health (AQH) health monitoring system is proposed by [7]. The system uses multiple sensors to read heartbeat, body temperature, etc., and transmits the monitored data to a cloud-based infrastructure via smartphone. [8] analyzes IoT security and privacy issues from the health care perspective and proposes an intelligent collaborative security model to minimize security risk. A security architecture for mobile e-health system to manage medication prescription service via electronic Personal Health Records is presented by [9]. The architecture supports mobile e-health application (m-health) through a RFID technology.

III. Architecture

The information technology architecture of a m-health system is a part of IoT architecture which is multi-layer and consists of data collection, data storage, and data processing layers. Each layer is itself based on distributed components (servers) located at different locations. Data storage layer is capable to store Big-data (health, traffic, weather, date etc.) collected from heterogeneous resources. Data processing layer is responsible for intelligent data analysis, report generation and visualization services. The over all architecture of a IoT system is shown in Fig. 1 where as m-health part is shown in Fig. 2.

Patients medical data is stored on the IoT servers. The data can be access by any permissible healthcare facility e.g., hospital, medical insurance, etc., via Internet. It means data is available anytime and anywhere.

IV. Characteristics m-health devices

A vast amount of Mobile health (m-health) data is generated via compact and easy to use mobile health devices. These m-health devices are wirelessly connected to IoT servers and can store, transmit and receive data. In this section we identify and describe the following main characteristics m-health devices:

A. Compact and easy-to-wear

For m-health devices size, mobility and comfortableness is very important. The are many m-health devices in the market with varying size and functionalities. Here we briefly discuss few of the latest m-health devices:

TICKR© is heart rate monitor by Wahoo Fitness. This device can simply easily straps across the chest to take the heart rate measurements.

FitBit Surge© is a convenient smartwatch with abilities to get notifications from smartphone. It can track heart rate, sleep patterns, and amount of calories burned during a workout. The FitBit Surge supports Bluetooth wireless connectivity and is compatible with iOS and Android operating systems.

Forerunner 920XT© is a Bluetooth compatible smartwatch. Some of the features of Forerunner 920XT are heart rate monitoring, calorie computation, step counter, swimming stroke counter and tracking elevation (via barometric altimeter).

iBGStar© is a blood sugar meter. It is about the size of a USB memory stick and very easy to carry. It is compatible with the iPhone and iPod. The iBGStar automatically synchronizes data with the iBGStar Diabetes Manager on the iPhone to track glucose and insulin. It supports to tag meals and exercise, graph data and share data via email with health care providers.

B. IP enabled and wireless connectivity

Each m-health device has a unique identifiers called IP address. The IP address enables the device to transmit/receive data over the network. The IoT infrastructure provides ubiquitous connectivity to m-health devices in a heterogeneous network environment.

Mobile health devices use wireless technology for connection and transmission of data. Connected devices streamline the process of monitoring, diagnostic, treatment, admission, billing, etc [10]. There are many standard for wireless connectivity but for mobile health devices decisive factors are low power, low cost, physical size and ease of use. Table I summaries the various wireless standards [11]. Here we briefly describe the selected standards suitable for mobile health devices:

The Infrared Data Association (IrDA) is an ultra-high-speed connectivity version, yielding throughput of 1 Gbps. However, it only works over a distance of less than 10 cm.

Nike+ is a proprietary wireless technology developed by Apple and Nike mainly to monitor the activity levels of users while exercising.

Bluetooth Low Energy (BLE), the main aim of this wireless technology is to enable power sensitive devices to be permanently connected to the network for long period of time. BLE sensor devices may operate for many years without need to replace the battery.

ANT is a low-power proprietary wireless technology which operates in the 2.4 GHz bandwidth spectrum. Its primary goal is to allow medical and sports sensors to communicate with a display unit, for example, a watch or cycle computer. It typically operates from a coin cell.

ZigBee is a low-power wireless specification based on the Institute of Electrical and Electronics Engineers (IEEE) Standard 802.15.4-2003 and was established in 2002 by a group of 16 companies. It introduces mesh networking to the low-power wireless space.

Near field communication (NFC) is significantly different from the other low-power wireless technologies. It only works up to a range of approximately 1 - 5 cm and consumes relatively more power.

Wi-Fi is a very efficient wireless technology, it is optimized for large data transfer using high-speed throughput. Wi-Fi is the most power efficient technology and would be ideally suited to large file medical data.

TABLE I. COMPARISON OF WIRELESS CONNECTIVITY STANDARDS

Wireless Technology	Peak power consumption	Throughput ≈	Range ≈
IrDA	10mA	1Gbps	5cm
Nike+	12.3mA	272bps	10m
BLE	12-16mA	305kbps	50m
ANT	17mA	20kbps	10m
ZigBee	30-40mA	100 - 250kbps	100-300m
NFC	30-40mA	424kbps	10cm-1m
Wi-Fi	116mA	6Mbps	150-500 ft

C. Low-power consumption

Mobile health devices are suppose to work for long period of time. This requires low power consumption and thermal efficiency. The sensors, circuits and processors of m-health devices are specifically designed to perform a given task at optimal power, i.e., delivering longer battery life. There is tight integration of software to the hardware in the m-health devices to take advantage of power saving hardware features and to make intelligent power management decisions. For power hungry components such as the display and power amplifiers frame buffer compression (FBC) and content adaptive backlight (CABL) are used to save power. A general mobile health and IoT architecture based on IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) is described by [12].

V. ACQUISITION AND APPLICATIONS OF M-HEALTH DATA

In this section, we describe acquisition of m-health data via medical gadgets and wearables and application of this data in monitoring various health conditions.

A. Blood sugar level monitoring

Diabetes is a serious chronic disease with major economic and social impact. Blood sugar testing is an important part of diabetes care. A self-testing mobile device that can measure blood sugar level on the go is important for treatment plan and preventing long-term complications of diabetes. Google, in partner with Swiss based pharmaceutical company Novartis, has developed smart contact lenses for people who suffer from diabetes. Smart contact lenses take the tears in a persons eye and measure the glucose levels [13].

B. ECG monitoring

An electrocardiogram (ECG) is a simple test that records the heart's electrical activity. A regular heart's activity monitoring by a handheld ECG device is both effective and provides longterm cost savings for cardiac patients. Existing electrocardiogram (ECG) monitoring devices such as Holter are inconvenient for long-term use due to their size and twisted wires. Wireless ECG monitoring devices that can connect to remove IoT server are emerging into market. A wearable ECG monitoring and alerting system "iHeart" that continuously monitors ECG is developed by [14]. The iHeart monitors patient's ECG and issues an alert to the patient if it detects abnormal heart behaviour. The device uses a wireless ECG sensor and a smartphone.

C. Blood pressure monitoring

High blood pressure or hypertension is a serious risk factor that may leads to heart attacks, strokes, etc. Therefore, its diagnoses and monitoring is critically important. Blood pressure can vary from minute to minute, therefore continuous monitoring helps to better understand the cardiovascular health of the patient. Wearable blood pressure monitors can be worn on a belt and are connected to a cuff on the upper arm. These devices are automatic and can record blood pressure for 24/7, while patients can do their normal daily activities. A photoplethysmographic (PPG) based approach to monitor blood pressure using wearable sensor is presented by [15]. A noninvasive pulse transit time (PTT) based approach to continuous measurement of BP is described by [16].

D. Asthma monitoring

Observation is the key to asthma management. When, where and what triggers an attack is very critical to maintain an adequate environment and alleviating symptoms. Peak flow meter is a simple hand-held device for asthma monitoring. A wearable stethoscope to continuously monitor the patients with asthma or other pulmonary diseases is described by [17]. The system transmitting the signals via a wireless sensor attach to the skin. A wearable sensor system consisting of a wristband and chest patch for understanding impacts of ozone on chronic asthma conditions is described by [18]. The data from the device is streamed and transferred to a server for cloud storage. The battery life of wristband is around 15 hours and the chest patch is around 36 hours.

VI. SECURITY OF M-HEALTH SYSTEM

It is patient's right to control the access of his/her personal health data. Therefore, it is very critical that mobile health devices and system are secure. There are three aspects of this issue namely confidentiality, privacy, and security. **Confidentiality** refers to the obligation of professionals who have access to patient records or information to hold that information in confidence. **Privacy** is the right of the individual patient to make decisions about how personal information is shared. **Security** refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure. Confidentiality, privacy, and security are important. However, it is important to balance system security with availability. A non-authorized access may be harmful to the system or patient. But in case of emergency, if the patient's data can't be access at right time, it can be dangerous to the life of patient.

In a mobile health system data is stored and access electronically via Internet. The personal health data is available to any intruder unless protected. It is highly recommended that m-health data and devices are HIPAA-compliant. The HIPAA (Health Insurance Portability and Accountability Act), defines the standard for protecting sensitive patient data. Any company that deals with protected health information must ensure that all the required physical, network, and process security measures are followed. Following measures are recommended to ensure confidentiality, privacy, and security and m-health system:

1) **Physical safeguards** mean only authorized physical access to data-center. All HIPAA compliant facilities must have policies about use and access to workstations and electronic media. This includes transferring, removing, disposing and re-using electronic media and electronic protected health information (ePHI).
2) **Technical safeguards** require only authorized user to access electronic protected health data. Access control includes using unique user ID, strong password, automatic log off, encrypted storage and transmission of data.
3) **Audit reports** are used to keep records of activities, e.g., user login/logout, who accessed what data, system messages, etc. Audits are very useful to determine the source of any security breach.
4) **Technical policies** should also cover integrity controls, or measures put in place to confirm that ePHI has not been altered or destroyed. IT disaster recovery and offsite backup are key to ensure that any electronic media errors or failures can be quickly remedied and patient health information can be recovered accurately and intact.
5) **Network security** is an important measure to protect against unauthorized public access of ePHI. Network security refers to the policies and procedures implemented by a network administrator to prevent unauthorized access, exploitation, modification, or denial of the network and network resources. It is concerned with all the methods of transmitting and receiving data such as email, web, etc.

VII. Conclusion

Mobile health (m-health) system build upon IoT infrastructure is revolutionizing how clinical research is conducted and disease therapies are delivered. Real-time data is recorded and transferred via wearable gadgets and sophisticated implantable medical devices. The patients information access via doctors supports quick diagnosis, remote monitoring and home rehabilitation. Further m-health significantly reduces overall healthcare cost and unnecessary hospitalizations.

References

[1] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, "Knowledge acquisition and management architecture for mobile and personal health environments based on the internet of things," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, June 2012, pp. 1811–1818.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[3] D. Giusto, A. Iera, G. Morabito, and L. Atzori, *The Internet of Things*, 1st ed. Springer New York, 2010.

[4] C. Kan, Y. Chen, F. Leonelli, and H. Yang, "Mobile sensing and network analytics for realizing smart automated systems towards health internet of things," in *2015 IEEE International Conference on Automation Science and Engineering (CASE)*, Aug 2015, pp. 1072–1077.

[5] A. Lymberis, "Smart wearables for remote health monitoring, from prevention to rehabilitation: current r d, future challenges," in *Information Technology Applications in Biomedicine, 2003. 4th International IEEE EMBS Special Topic Conference on*, April 2003, pp. 272–275.

[6] R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, "The potential of internet of m-health things m-iot for non-invasive glucose level sensing," in *Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE*, Aug 2011, pp. 5264–5266.

[7] S. Sharif, I. Mobin, and N. Mohammed, "Augmented quick health," *International Journal of Computer Applications*, vol. 134, no. 11, pp. 1–6, January 2016, published by Foundation of Computer Science (FCS), NY, USA.

[8] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[9] F. Gonalves, J. Macedo, M. J. Nicolau, and A. Santos, "Security architecture for mobile e-health applications in medication control," in *Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on*, Sept 2013, pp. 1–8.

[10] S. Hengstl, "Wireless health: Making your devices talk - a review, solution, and outlook for wireless health connectivity," *IARIA International Journal on Advances in Life Sciences (LIFSCI)*, vol. 6, no. 3 & 4, pp. 147 – 156, 2014.

[11] M. Habbal, "Bluetooth low energy-assessment within a competing wireless world," in *In Proc. Of Wireless Congress 2012-Systems & Applications*, 2012.

[12] R. S. H. Istepanian, A. Sungoor, A. Faisal, and N. Philip, "Internet of m-health things "m-iot"," in *Assisted Living 2011, IET Seminar on*, April 2011, pp. 1–3.

[13] https://www.wearable-technologies.com/2015/04/wearables-in-healthcare/.

[14] W. Hyuma, M. Kawarasaki, A. Sato, and K. Yoshida, "Wearable ecg monitoring and alerting system associated with smartphone: iheart," *International Journal of E-Health and Medical Communications (IJEHMC)*, vol. 4, no. 4, pp. 1 – 6, 2013.

[15] P. A. Shaltis, A. Reisner, and H. H. Asada, "Wearable, cuff-less ppg-based blood pressure monitor with novel height sensor," in *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE*, Aug 2006, pp. 908–911.

[16] C. C. Y. Poon, Y. M. Wong, and Y. t. Zhang, "M-health: The development of cuff-less and wearable blood pressure meters for use in body sensor networks," in *Life Science Systems and Applications Workshop, 2006. IEEE/NLM*, July 2006, pp. 1–2.

[17] K. J. Cho and H. H. Asada, "Wireless, battery-less stethoscope for wearable health monitoring," in *Bioengineering Conference, 2002. Proceedings of the IEEE 28th Annual Northeast*, 2002, pp. 187–188.

[18] J. P. Dieffenderfer, H. Goodell, B. Bent, E. Beppler, R. Jayakumar, M. Yokus, J. S. Jur, A. Bozkurt, and D. Peden, "Wearable wireless sensors for chronic respiratory disease monitoring," in *Wearable and Implantable Body Sensor Networks (BSN), 2015 IEEE 12th International Conference on*, June 2015, pp. 1–6.