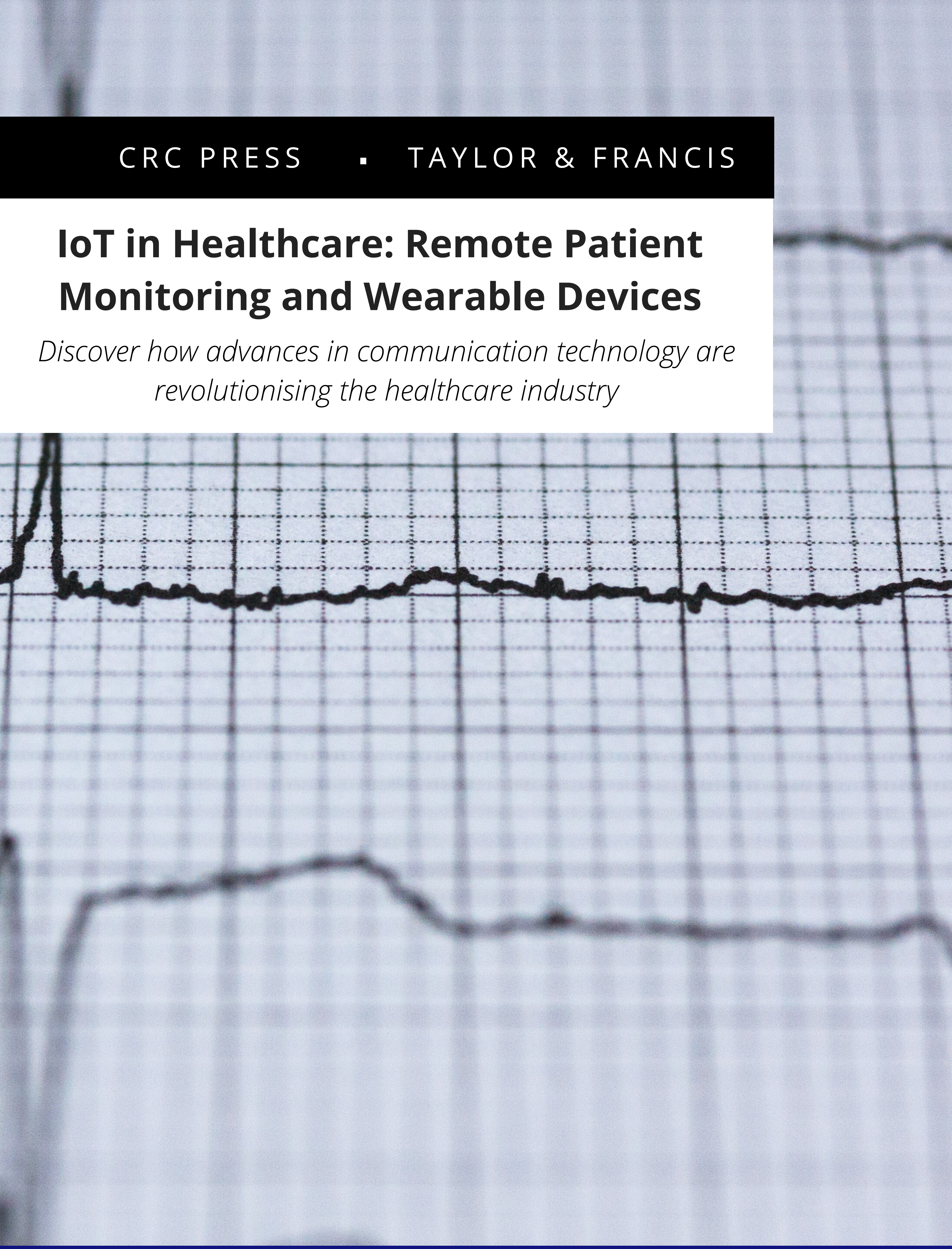
CRC PRESS ▪ TAYLOR & FRANCIS

IoT in Healthcare: Remote Patient Monitoring and Wearable Devices

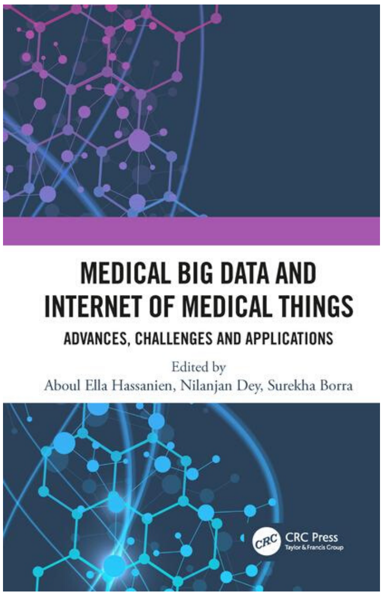
Discover how advances in communication technology are revolutionising the healthcare industry



CRC Press
Taylor & Francis Group

www.crcpress.com

Contents

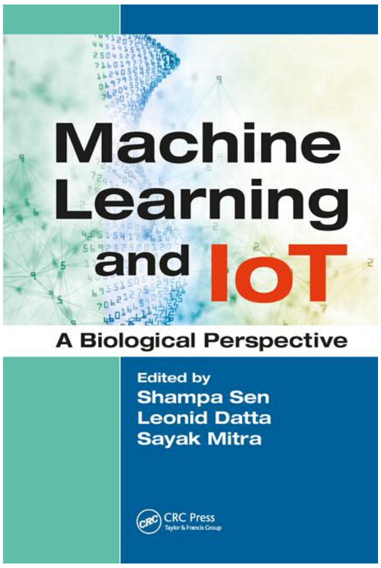


MEDICAL BIG DATA AND INTERNET OF MEDICAL THINGS

ADVANCES, CHALLENGES AND APPLICATIONS

Edited by
Aboul Ella Hassanien, Nilanjan Dey, Surekha Borra

CRC Press
Taylor & Francis Group

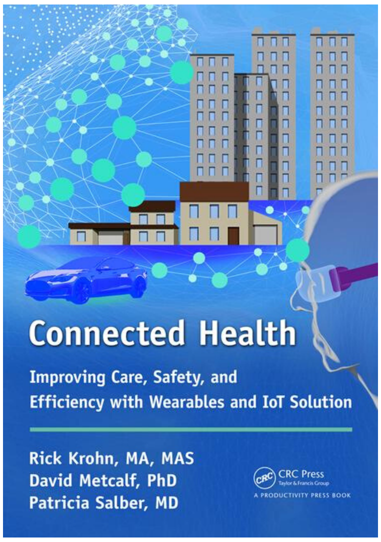


Machine Learning and IoT

A Biological Perspective

Edited by
Shampa Sen
Leonid Datta
Sayak Mitra

CRC Press
Taylor & Francis Group

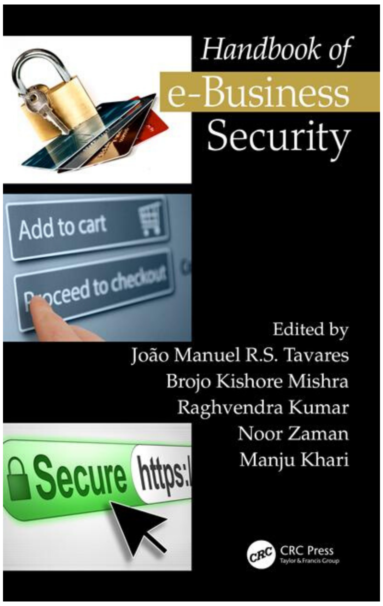


Connected Health

Improving Care, Safety, and Efficiency with Wearables and IoT Solution

Rick Krohn, MA, MAS
David Metcalf, PhD
Patricia Salber, MD

CRC Press
Taylor & Francis Group
A PRODUCTIVITY PRESS BOOK



4. Internet of Things (IoT) Deployment in Wearable Healthcare

From *Handbook of e-Business Security Edited by* João Manuel R.S Tavares, Brojo Kishore Mishra, Raghvendra Kumar, Noor Azaman and Manju Khari

WI-FI
ENABLED HEALTHCARE
Ali Youssef • Douglas McDonald II
Jon Linton • Bob Zemke • Aaron Earle
CRC Press
AN AUERBACH BOOK

5. Mobile Medical Devices

From *Wifi Enabled Healthcare* by Ali Youssef, Douglas McDonald, Jon Linton, Bob Zemke and Aaron Earle.

11 Internet of Medical Things

Remote Healthcare and Health Monitoring Perspective

Sitaramanjaneya Reddy Guntur,
Rajani Reddy Gorrepati, and Vijaya R. Dirisala

11.1 INTRODUCTION

The latest emerging trends and advances in communication technology continue to sweep the global healthcare industry. Recent advances in innovative design and development of medical devices enhance the quality of patient care. New technological trends, from physical devices to smart systems, are transmitting essential information in real time enabling specialists, healthcare providers and patients to interface in new ways and recognize life-threatening situations [1]. The vision of medical services at 'anytime, anywhere and anything' is changing to reach the patient expectations and is motivating the next generation of innovations [2]. Presently, advances in smartphone frameworks are helpful and comfortable enough to enable specialists or doctors with consultations for medical assistance. IoT regions interfaces with frameworks related to enormous information, security and protection, which possess a serious challenge. In addition, it allows people to upload, retrieve, store and collect information, which ultimately forms big data. IT enables individuals to transfer, recover, store and accumulate the data.

In addition to this, it examines the investigation of continuous large flows of information to infer significant knowledge in big data applications in a few areas. It investigates conceivable computerized arrangements in everyday life including structures and mechanized frameworks of IoT innovation, and additionally medicinal services frameworks that oversee a lot of information to enhance clinical decisions [3,4]. In this chapter, we highlight the innovative technological advances with major implications in the field of IoMT and remote medical services.

11.1.1 Overview of Internet of Medical Things (IoMT)

The IoMT is playing a pivotal role in remote healthcare and monitoring to increase the efficacy of medical devices, and the speed and accessibility of medical services. The IoMT can be used to collect remote patient health data utilizing wearable sensors and devices connected to Internet-based health monitoring systems. IoMT is processed by connecting and communicating machine-to-machine (M to M) through medical devices equipped with Wi-Fi. The received healthcare data from the IoMT devices are stored in the cloud server database, which is linked to cloud platforms and then analysed.

Remote health monitoring (RHM) refers to a continuous process of monitoring a person's health by closely following the course of exercises and contrast to ascertain what is going on and what is relied upon to happen. Clinical services are not particularly incorporated into RHM, in spite of that it may certainly lead to the provision of such services. It may include monitoring physiological parameters such as the heart rate, pulse rate, blood pressure and temperature in addition to other parameters such as medication and diet monitoring to help patients. Remote healthcare is a process that periodically collects and reviews health data on program implementation and provides elementary analysis so as to enable progress of expectations. RHM may be used in conjunction with healthcare, which allows a patient to use a smartphone or wearable device to perform a routine test and send the test data to a healthcare professional in real time. RHM and healthcare services have improved the physicians ability to monitor and manage patients in non-traditional healthcare settings. RHM utilizes advanced methods to gather the health information from people in a single area, such as a patient's home, and transmit the data to healthcare providers in a different area for analysis and recommendations by home nurses, or disease management programs.

The concept of IoMT is the integration of healthcare devices with computer networks through the web, which receives information in real time, and also allows interaction with patients [5–7]. Basically, IoMT associates living and non-living things through the web [8]. Another concept of IoMT is 'things oriented', particularly day-to-day objects via smart systems utilizing smart interfaces such as ZigBee, Bluetooth, RFID, LAN, Wi-Fi or by other working frameworks to interface and communicate in social, natural and client contexts [9–11]. The object-oriented IoMT module considers a smart physiological thing that allows communicate through the internet technologies virtually [12]. IoMT collects and communicates the patient's physical parameters at any time, any location, about anything by using the ideal service in any path or network, as shown in Figure 11.1. The IoMT is able to remotely connect people about chronic diseases by using the patients' and hospitals' locations and tracking medication orders and wearable health devices [13]. The large amount of health data generated by health devices or sensors, including blood pressure, heart rate, body temperature, respiratory rate, pulse rate and so on is sent to the healthcare providers [14]. At present, hospital beds and analytics, dashboards are being connected with

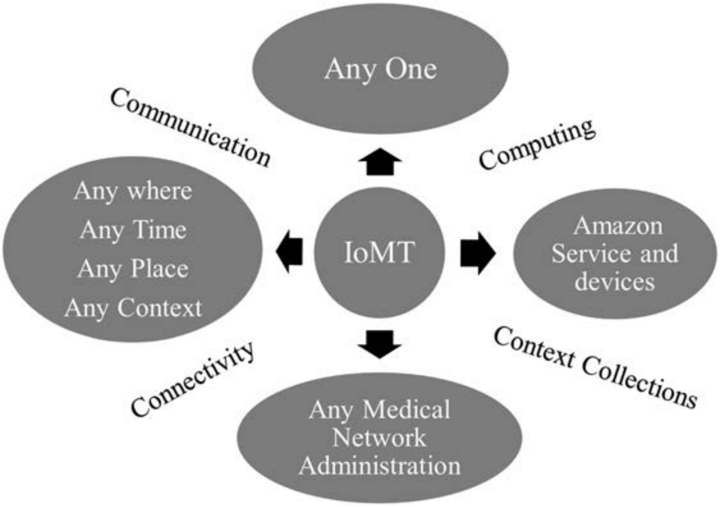


FIGURE 11.1 IoMT in various environments.

a good number of wearable sensors for measurement of a patient's physiological parameters in real-time, and the medical devices convert or deploy the data with the IoMT technology [15].

A large volume of generated data (often called big data) is received from sensors, actuators and embedded systems; however, these are unable to process it readily by utilizing conventional data processing methods and applications. Besides this, numerous database groups and additional resources are required to store the data [16]. However, storage and recovery is not the only problem but it is also of paramount importance to obtain a meaningful pattern relevant to patient diagnostic information [17]. IoMT enables faster diagnosis of disease and decision-making by compiling numerous medical data (i.e., big data) on time coupled with wise investigation [18]. IoMT includes in-depth analysis of patient monitoring with network and communication technology. A novel health monitoring healthcare framework and computational models that handles large volume of data driven by patient information such as big data and along with the available tools, mechanisms and algorithms to deal with those problems as well as a case study was presented and addressed the security and privacy issues as well as the big data challenges [19–21].

11.1.2 The Requirements of the IoMT Systems

The requirements for remote healthcare and health monitoring capture the data required to build IoMT functionalities by a framework. These practical prerequisites of IoMT requirements are classified into two categories: functional and non-functional, as shown in Figure 11.2.

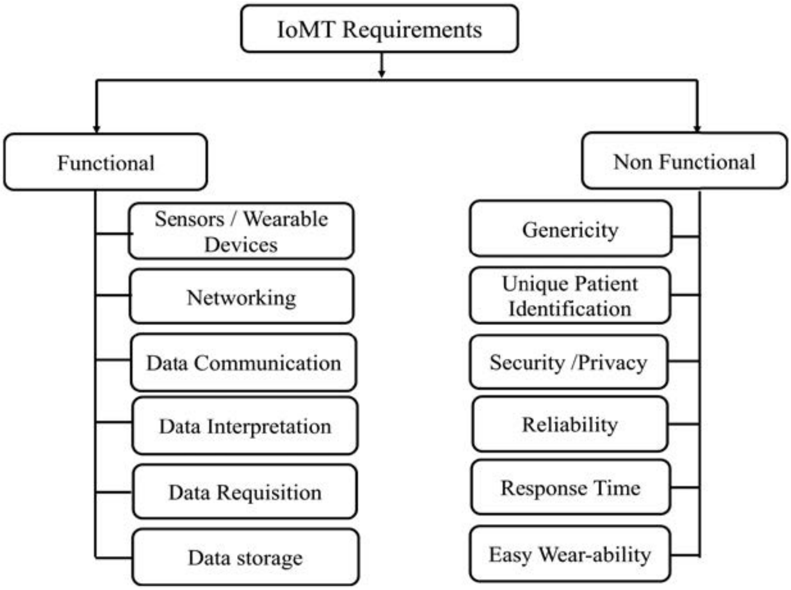


FIGURE 11.2 Requirement of IoMT.

Sensors/wearable devices: Sensors and wearable devices are prerequisites for obtaining patient health data. Non-invasive, non-intrusive sensors are prime components of mobile and long-term health check-up frameworks. Wearable sensors are more comfortable and less obstructive, while suitable for checking a person's health without intruding on their day-by-day activities. The sensors, placed on various locations of the body, can measure physiological parameters as well as the activity and movement of a person. Different sensors have been developed for an assorted scope of health information specific for healthcare services. Such sensors are prospective enough to transfer the data to similar service through the IoT. On the other hand, wearable devices can accompany an arrangement of highlights for proper the IoT design along these lines, the joining of previously mentioned sensors into wearable items is obvious. Such sensors are sufficiently imminent to exchange the information comparative administrations through the IoT. Then again, wearable gadgets can go with a game plan of features for appropriate the IoT outline. Thusly, the joining of beforehand specified sensors into wearable things is self-evident.

Network: The framework should allow for an interface between the patient and specialist. The IoMT refers to both the network and the computing platform, and the service layer focuses on patient healthcare. This structure demonstrates that an efficient and precise hierarchical model of caregivers or operators can access various databases from the application layer with the assistance of a supporting layer.

Data communication: Data communication is the process of transferring the received health information from wearable sensors. First, the acquired health data is transferred to the IoMT in real time. The correspondence between the sensor and health monitoring system is called intra-correspondence, and data should to be transferred to the cloud server.

Data interpretation/differentiation: The system should be able to analyse the basic health parameters from the sensors. Biosignals must be effectively deciphered by remote patient monitoring systems and cloud servers. RPHM establishes the connections between various physiological parameters and life styles.

Data requisition: In order to analyse the patient's health condition, clinicians require the current heath information together with the past records from the database. The data-storing servers are able to provide relevant data on request.

Data storage: IoMT-based remote health monitoring systems consist of a large volume of information from various patients or patient groups. The data storage severs should have enough space and memory and be able to accommodate large data quantities.

Non-Functional Requirements:

Genericity: The IoMT system is able to adjust with the patients' monitoring requirements and should not be concise with a particular disease, group or group of individuals.

Patient identification: Patients must be furnished with a unique patient ID.

Security/privacy: The connection between the biometric sensor layer, IoMT base unit and server should be secure and verified.

Reliability: IoMT systems play a vital role in the healthcare industry for increasing the accuracy, reliability and productivity of electronic devices. They should be able to perform consistently and produce health information precisely.

Response time: IoMT systems are always fast enough to provide services for emergencies and also fast enough to provide patient information during crisis situations to avoid unnecessary confusions and provide quick assistance to patients.

Easy wear-capacity: The sensors used to measure on the body area network are portable and sensitive, so that the sensors are simple, easy to use and convenient for the patient.

11.1.3 Remote Patient Healthcare and Health Monitoring System

Currently, people are busy with their work schedules and have limited time to visit specialists for routine health examinations. Because of this, medical problems continue to increase and people suffer from various avoidable diseases. Likewise, a majority of elderly people suffer from various health ailments and are unable to visit hospitals routinely. People are not prepared to wait for a long time for consultations and medical examinations. Once in a while, the treatment may not be accessible immediately nearby even when a person is suffering from a major health problem, and the patient needs to travel a long way for the treatment. Based on the assistance of the RHM framework, health parameters can be self-assessed by sitting at home and the information can be shared with a qualified doctor who is far away. If the patient is suffering from a major medical ailment, and the specialist treating the patient is unable to help, these parameters can be remotely sent to a doctor who can help him/her from any location. In the worst case, even if the treatment isn't accessible in his/her country, he/she can communicate and continue the treatment with a specialist from a technically advanced country. Thus, mortality rates can be decreased and the quality of care can be enhanced using RHM with IoMT [22]. The RHM is a small and compact system and can be carried by the patient whenever and wherever it is needed; these devices are available at very low cost and provide long-term service [23].

Remote patient monitoring is also called self-testing or monitoring of health parameters. This enables remote monitoring of patient's physiological parameters using different medical equipment by the physician. This method is useful for monitoring the patient's physiological status as well as diagnosing diseases and prescribing medications according to data analysis feedback [24]. In remote monitoring, the wearable sensors capture data pertaining to body temperature, heartbeat, pulse rate and so on and transmit the data to a specialist either in real time, or it is stored and then forwarded. RHM includes home-based surveillance of ECGs [25], wireless gastrointestinal capsules [26], dialysis, multi-parameter ICUs, telehealth and diseases [27]. Hence, the RHM system is used to continuously monitor the physiological parameters of a patient with the help of sensors. These parameters are tracked and sent to the physician and in case of any abnormality, the problem can be rectified. The existing patient monitoring systems are fixed monitoring systems, which are only available in hospital ICUs, as shown in Figure 11.3. These systems are huge in size and useful to monitor patients in hospital beds only. No automatic system exists able to regularly provide important data about the patient when he or she is mobile [28]. Medical assistance, health monitoring, and rehabilitation for the older and disabled people is an imminent challenge, as it requires an ideal network between people, medical equipment and health service providers. For this reason,

FIGURE 11.3 Existing patient monitoring system.

reliable and cost-effective wearable devices with low-power are needed to enhance their quality of life. The IoMT framework offers promising innovative advances to accomplish before the specified patient care services, and enhance further the health service systems [29].

The IoMT platform is useful to collect important health information form clients and wirelessly communicate the information to the cloud server for evaluating the previous record of the client [30]. Such a network with this equipment and these processes will assist in preventive measures, or for providing immediate care. Recently, a few IoMT frameworks have been created for remote medical care services and assisted living applications. An excellent IoT system, with capable medical devices and standard communication, was produced by Xu et al. [31]. A resource-based data receiving method is better suited for medical care intensive data applications [32]. A medical support system based on IoT was proposed and implemented by Kolici et al. Moreover, several experiments were performed to evaluate the system [33]. Ang et al. developed a smart guide portable system with a handheld device which helps visually impaired and low vision individuals to move around using a camera sensor system to improve observing capacities for an additional level of security and reliability with mobile association innovation [34]. IoMT-based remote patient monitoring data sets consist of large volumes of information from various groups, which is difficult to separate the data sets between groups and within the groups. In order to arrange datasets, a Fisher's discrimination criterion was applied to clean the raw datasets in row, columns and time stamps [35,36]. This chapter is mainly focused on proposing a new remote patient healthcare monitoring system, and starts with a review of the related work, monitoring and examines the proposed architecture, available advantages, limitations, and the challenges addressed to enhance the practice of medicine.

11.2 NETWORK ARCHITECTURE OF INTERNET OF MEDICAL THINGS (IoMT)

The proposed architecture is based on communication between client and server, as shown in Figure 11.4, which depicts the main layers of the remote health monitoring system. The first biometric sensor layer is data sensing and collecting information from smart wearable sensors from the whole network. Local and intelligent computing and processing units are connected between the hardware devices and the patients' skin surface [37]. The collected data is processed and transferred to the service layer, which consists of data storage, data organization devices and wire/wireless protocols such as Bluetooth, Zigbee, RFID, WiFi, Ethernet and 3G/4G networks; these are linked to the IoMT layer for communicating the measured parameters to facilities such as hospitals, emergency centres, ambulances, care takers and medical centres.

The physicians have easy access to the medical histories of patients or large groups of patients as well as their physiological status, and the analyses of suspicious data (blood pressure, respiration, ECG, etc). The overall health testing for a group of patients is performed by doctors using efficient hardware and software devices, which analyse the variations in the parameters of each patient automatically and identify their physical status over a period of time. In this layer, cloud computing and data protection as well as patient privacy services are provided. The fourth application layer uses the interface between doctors and remote patients to easily provide information status on demand or on a regular basis. The second layer has a significant importance for processing the sensor data online. A cloud-based information storage framework is used for arranging and recovering lots of information and provides highly stable, high speed, and cheap storage. S_3 serves as a raw sensor data storage and sorting server for image, audio, and video data in IoMT systems. Amazon offers commercial web services that permit designing MySQL, Oracle or Microsoft SQL servers on the cloud.

Amazon Kinesis is a web service that permits real-time processing of information, and it deals with automatically scaling large amounts of streaming data originating from a large number of sources. Amazon SQS offers an exceptionally adaptable and predictable hosted queue for stores, storing and release messages in a scalable manner between distinct components of applications. Amazon EMR is a web service that utilizes the Hadoop framework and permits processing large-scale data, consequential, and is suitable for IoMT applications that produce large amounts of data that need to be analysed. Matallah et al. [38] addressed the service metadata improvement by proposing a blended arrangement amongst centralization and circulation of metadata to upgrade the execution and versatility of the model utilizing Hadoop Distributed file (HDFS) framework.

The IoMT can be seen in three patterns based on sensors oriented acquisition things, internet-oriented middleware monitoring, and knowledge-oriented action systems (Figure 11.4). However, the IoMT is useful for the development of applications based on the three patterns. As the purpose of the hardware layer is to interconnect sensors and the device components such as storage, processing, and internal parts. Physiological parameters such as temperature, ECG, blood pressure and so on are measured using wearable sensors, which must be very precise and small in size.

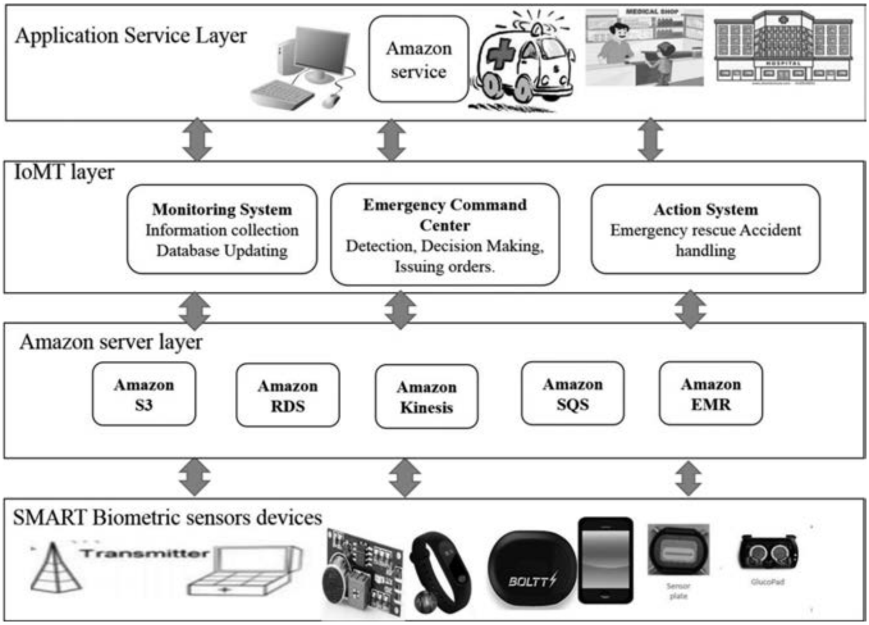


FIGURE 11.4 Architecture of remote healthcare monitoring system.

The communication layer is useful to connect many devices to the network and transmit the information to the application layer. The application layer presents the required services such as hospital, ambulance, emergence, medication to the remote patient by receiving the information from the IoMT layer. Moreover, it allows the possibility of obtaining, processing and recommending valuable information to patients and improving their way of life. Moreover, it is necessary to exploit the advantages of innovative technologies such as IoT for communicating medical data from machine-to-machine (M2M), and person-to-person (P2P) to improve healthcare.

11.3 REAL-TIME ANALYSIS REMOTE PATIENT HEALTH MONITORING

A remote patient monitoring system based on wearable sensors with IoMT for obtaining chronic patient conditions is shown in Figure 11.5. Patients purchase biosensors from commercial vendors and install network services on their mobiles. These services can be connected with the help of GPS and BPO services for location-tracking of patients at low cost. The patients' physiological parameters and patients' health status can be monitored with a smartphone and the information can be transferred to the IoMT through Zigbee, Bluetooth or Wi Fi. IoMT can be used to store and process the data received from the sensors in a cloud server and provide required medical assistance on the basis of sending application service to the hospital, physician, medication centre, home and so on in real time. IoMT technology is implemented using biometric sensors in hospital settings or smartwatches that enables the patients to self-monitor

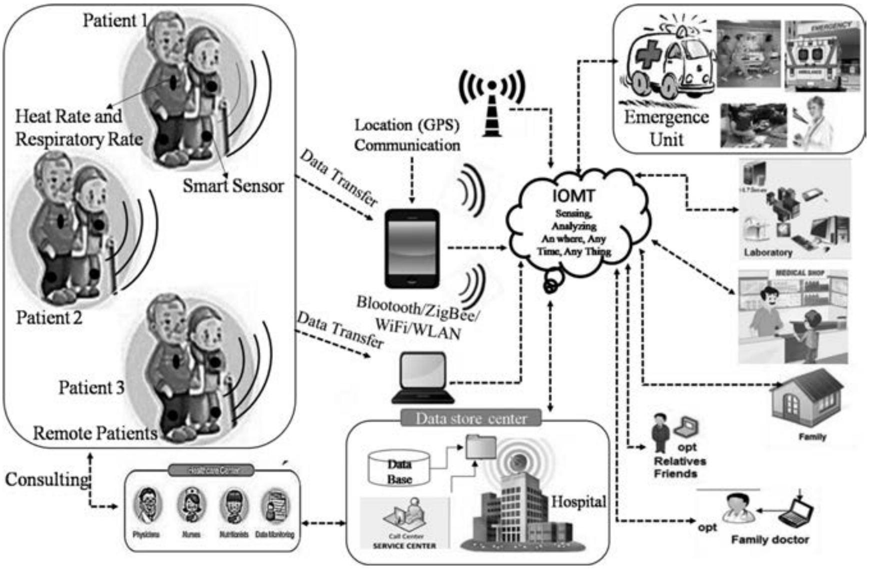


FIGURE 11.5 Remote patient health monitoring system based on wearable sensors.

and collect sensory information. Built-in smartwatch sensors are able to monitor heartbeat, pulse rate, blood pressure, temperature or respiration and even interface with remotely located medical devices. In case of medical emergencies, these smart devices can be used to contact the physician at any time, or an opened pharmacy in order to save a life. Blood pressure measurements help in explaining patterns of blood stream variations. IoMT-based blood pressure sensing is done in real-time by sensors attached to patients and connected to relevant medical services. An IoMT network collects specific information about blood pressure using communication devices, which includes a blood pressure sensors, smartphones and processors.

11.4 METHODOLOGY AND ANALYSIS

Patient physiological information is collected by wearable sensors for body temperature, pulse, respiration, and ECG [39]. The sensors are connected to the network through data accumulators in the region of the patient [40]. The patients' physiological data are recorded and transmitted in real time (by using the components of the system from any remote location) to the data centre with assured security and privacy [41].

Typically, data acquired from wearable sensors is transferred to the accumulator through Zigbee or Bluetooth. Collected information is further transmitted to a cloud using web connectivity on the accumulator, typically via a cellular phone data connection or Wi-Fi [42]. Each sensors' data can be accessed through the Internet via the accumulator based on the IoMT architecture. Most often, data storage and processing devices are a mobile client, or local cloud storage, and a processing unit (PC), which are directly accessible by the accumulator through Wi-Fi [43,44].

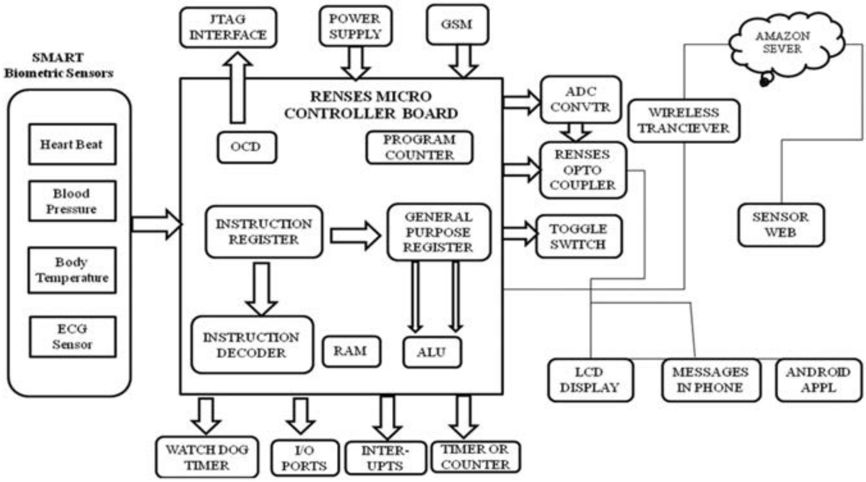


FIGURE 11.6 Master block diagram of a remote health monitoring and healthcare system.

Cloud servers are used to partially store the data before communication and are also used to concentrate the patient's data when mobile devices have some limitations [45]. A block diagram of the proposed remote health monitoring and healthcare system is shown in Figure 11.6; the design consists of a Renses microcontroller, smart biometric sensors, GSM/GPRS, power supply, and so on. Biosensors such as heartbeat, temperature, respiration, pulse and ECG sensors are connected to the microcontroller though port pins and the output signals are analogue; thus, the output pins are connected to the analogue digital converter pins of the microcontroller. Microcontrollers read and process the data and transfer it to the next level through a Wi-Fi. The measured sensor data is sent to the commercial cloud server and then sent to a web page through Wi-Fi, and messages are sent to smartphone and simultaneously displayed in LCD. However, the sensed ECG information is fed into an android application. Embedded C, Renesas flash programmer and Cube suite programmer were used to feed the values to the pins, so they can be stored in the web page.

11.4.1 Data Sensing and Acquisition

Physiological parameters are measured using various device platforms such as wearable sensors, minor pre-processing hardware and communication software for transmission of measured physiological parameters. The measuring sensors must be light, small, and operate in a wearable package with energy efficiency and also should not block the patient's movements and mobility. Sensors should provide continuous operation without replacing the extended durations. Recently designed biosensors for medical applications are flexible and easy to place on various body parts in contact with the skin. The sensors receive the bio-signals with greater accuracy [46].

11.4.2 Sensor Interface Circuits

The sensor interfacing circuit is used to connect different sensors (e.g., body temperature, pulse, blood pressure, etc.) are then adapted to be prepared for input to the microcontroller. This is accomplished using sensor interfacing hardware that changes over the signals from analogue to digital and further processes the signal to ensure the functionality and compatibility with the microcontroller.

11.5 MICROCONTROLLER

A microcontroller contains memory and a processor, and is embedded with machinery in the computer system including phones, peripherals, and household appliances. Nowadays, most programmable microcontrollers are called ‘embedded controllers’. Most of the embedded systems are available with minimum memory and are complex. Input and output devices are connected to the microcontroller, including wearable sensors, relays, displays, and other hardware. Microcontrollers are used to automatically control the connected devices and concentrate the data of the different sensors and communicate such information to the cloud server for additional processing and are used for tracking of the area information.

Our proposed method uses a Reneses microcontroller RL78/G13 single-board device with 20 pins and 128 pins with a flash memory of 16 KB and 512 KB, respectively. The RL78/G13 microcontroller includes the following: on-chip oscillator, real-time clock, power on reset, low voltage detection, watch dog timer, 26 channels of 10 bit, analogue digital converter, 32/32 divider, universal asynchronous receiver/transmitter, LIN, timer array and IEC 60730 hardware. The Reneses microcontroller is a board transmission module that controls the data stream between the distinctive sensors and the microcontroller. The sensor data communicated to the network can be accessed for monitoring the physiological parameters by the doctors. The controller alerts the doctor, nurses and caretaker about the variation output of the parameters. However, the major objective in remote healthcare and monitoring systems is data security and privacy.

11.6 PHYSICAL SENSORS

A sensor is used to detect the change in the parameters or the objects and sends the information to the processor. The sensor is a sub-system which is as basic as light or as complex as a computer. In order to collect patient action and health information, multiple sensors are needed. These sensors should be insignificant to be wearable and used for receiving the data for the proposed system was shown in Figure 11.7.

11.6.1 Temperature Sensor

A temperature sensor is used to measure body temperature. The LM35 series sensor contained an integrated circuit and converts the output voltage in terms of centigrade temperature. Various types of temperature sensors such as thermistors, RTDs, thermocouples and IC sensors are available, however, the proposed system focuses on the LM35 sensor due to its sealed sensor circuitry. The LM35 sensor can

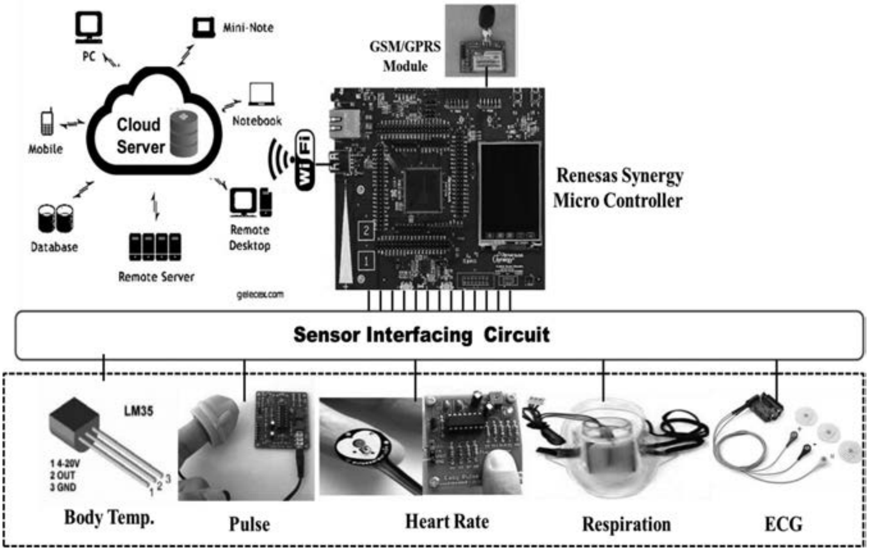


FIGURE 11.7 Proposed IoMT wearable sensor system for patient healthcare monitoring.

measure more accurately than a thermostat. The working temperature range is from −55 ± 0.1°C to 150 ± 0.1°C, with a scale factor of 0.01 V/°C.

11.6.2 Pulse Rate Sensor

The pulse rate is measured using Infra-Red (IR) light absorption of oxygenated and deoxygenated (or reduced) haemoglobin passing though the finger, which shows the difference in light absorption. Hemoglobin with oxygen (or reduced) absorbs more IR and allows more red light to pass through the finger, and hemoglobin without oxygen absorbs more red light and allows more infrared light to pass through the finger. The wavelength of red and infrared are 600–750 nm and 850–1000 nm, respectively. The pulse rate is measured by using a fingertip sensor, which emits light and receives it with a photo detector placed on the other side of the fingertip.

11.6.3 Heart Rate Sensor

The heart rate sensor is comprised of an amplifier circuit and fingertip sensor, as shown in Figure 11.7. The heartbeat sensor comprises an infrared (IR) light emitting diode transmitter and a photodetector receiver. The IR light is transmitted through the fingertip to measure the changes in blood volume in the blood vessel by using a fingertip sensor which is reflected in the light received by photodiode detector. The fluctuation in the blood volume is detected with respect to the pulse and the heartbeat is produced at the output of the photodiode. The signal received from the photodiode is not detected by the Reneses microcontroller directly because of the small amplitude of the signal, which requires amplification. The signal is amplified using an LM324 operational amplifier and the output is sent to the microcontroller analogue pin A_1 for additional processing.

11.6.4 Respiratory Sensor

A respiratory rate sensor is used to monitor the periodicity and non-periodicity of breathing, and controlling highly prevalent diseases such as coughs with sputum production or sleep apnoea. The respiratory rate is frequently used as an alternative to pulse and heart rate parameter variables. The main detection technique used is plethysmography. However, the long and laborious procedure for the detection of respiration of patients requires skilled health professionals, and is a costly and unpleasant process for the patients. Respiratory polygraph is another less complex alternative technique employed for respiration rate measurements; it reduces waiting time and cost, but it is an invasive technique. A smart respiration sensor is connected to a microcontroller, as shown in Figure 11.7, which overcomes the difficulties associated with the existing respiratory system in terms of complexity.

11.6.5 ECG Sensor

An ECG sensor is utilized to monitor the electrical activity of the heart, which includes the measurement of cardiovascular information such as the heartbeat and the basic rhythm of the heart, and prolonged PR and QT intervals. Besides, the ECG sensor gives confirmation of damages that occur in various parts of the heart muscle, and indicates the expanded thickness of the heart muscle. The electrical activity of the heart is measured by using the cost-effective board and the output of biopotential signals from the heart muscles is read as an analogue waveform. IoMT has the potential to monitor the ECG waveforms remotely and can be used to its fullest extent when based on a cloud server [47]. A number of studies have reported on ECG monitoring using IoT [43–53]. ECG signals are measured using three leads AD8232 monitor, which acts as an operation amp to obtain a clear signal from the PR and QT intervals. The AD8232 measures the biopotential signals from the skin surface using an integrated signal conditioner, which is designed to extract, amplify and filter the small biopotential signals in the presence of noisy conditions. The ECG sensor records the biopotential signals of the heart with time, using leads arranged on specific locations of the body. The signals obtained from electrodes placed on the patient are amplified by using an operational amplifier circuit LM324. To begin with, the LM324 has been utilized in the pre- and post-amplifier stages. The output of the amplified signal is specifically sent to the Reneses 2560 pin A_2 for additionally processing. The altium designer and multisim software were used in designing and testing the circuit.

11.6.6 Global System for Mobile Communications (GSM)

A GSM modem is used for connecting the PC to the mobile network, which is operated by using a SIM card to the subscribed mobile operator, just like for a cellular phone. The GSM modem operates over the network to send and receive messages. The GSM communication module acts as a gateway for the receiving module. The receiving module such as GPRS modem, mobile phone or any device sending and receiving SMS is connected with the computer and microcontroller through a USB or serial cable [54]. GSM uses AT (Attention) commands in order to control modems and computers to send, receive, write or delete messages. The IoMT agent will receive the SMS and process the command.

11.6.7 General Packet Radio Service (GPRS)

General packet radio service (GPRS) is a wireless data communication service available as a packet-based that delivers data rates from 56 to 114 Kbps, and is intended to replace the present circuit-exchanged administrations for GSM that associates with cell phone connections and send the Short Message Service (SMS). GPRS disseminates packets of information from several different terminals in the framework over different channels, making a significantly more proficient utilization of the transmission capacity applications such as Internet access. These higher data rates will enable clients to access applications utilizing a portable handset or PC. The cloud server actualizes a wide arrangement of information administrations including sensor and actuator, information handling, information investigation, database stockpiling and information perception.

The received client information is imparted to a cloud server, which is important for the accessibility of information anywhere on the Internet. The cloud server implements a wide set of information management services including sensor and actuator, data processing, data analysis, database storage and data resolution. The data analysis incorporates the stage with the system framework and application, in addition to providing an application program interface (API) and software tools through which the information can be accessed and manipulated. The design and development of the cloud server is shown in Figure 11.8. The cloud server stores the huge database that has enough space to furnish huge amount of data from various sensors for long times and also track the historical backdrop of the user. The database is interfaced to a wide set of data analysis algorithms and APIs for estimation and evaluation. The IoMT client-side computer can easily access the data through the Internet, as shown in Figure 11.8.

11.7 SOFTWARE DESCRIPTION

11.7.1 Embedded C Programming

Embedded C is a language programming expansion of C programming to address the communication between different embedded systems. A large portion of the syntax and semantics of embedded C, for example, main function, variable, data type, loops, functions, arrays and strings, structures and so on resemble standard C programming. In short, embedded C deals with microcontrollers, input/output ports (RAM, ROM), whereas C deals with only memory and operating systems. C is a desktop programming language used for embedding a piece of software code into the hardware to make it function. Here, the program on the wearable sensor operation was written using embedded C.

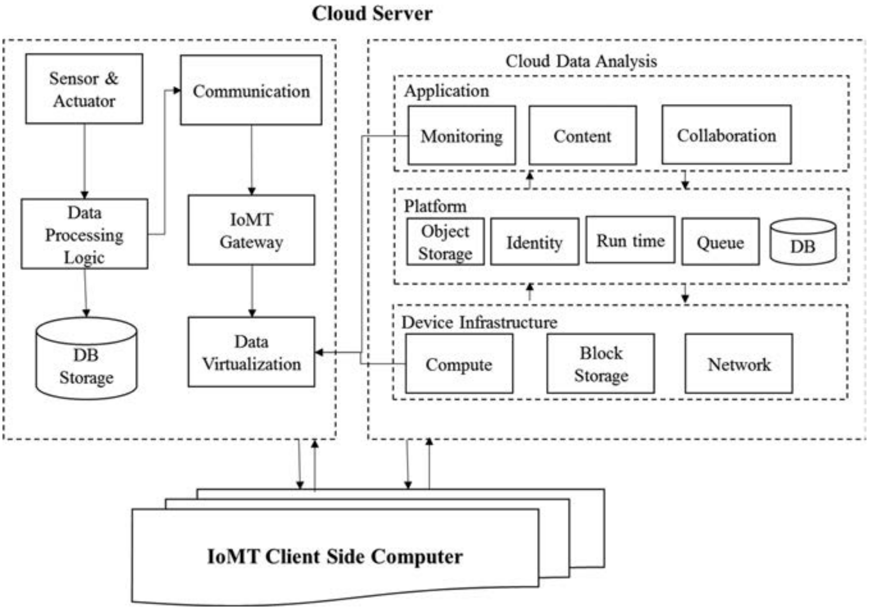


FIGURE 11.8 Cloud server architecture.

11.7.2 Renesas Flash Programmer

Renesas Flash Programmer (RFP) is used to write, erase, and verify the programs with on-chip flash memory mounted onto the target system or program adapter on which a Renesas single-chip microcontroller, E20 emulator, or the on-chip debug emulator with programming function, QB-MINI2 (INICUBE2), or a serial interface is set.

11.7.3 MySQL

It is the most prevalent open source relational SQL database administration framework. It has a perfect convenient database server and is valuable for applications. Also, the SQL supports standard compilation on various stages and has multi-reading capacities on UNIX servers, which enables excellent execution. For non-Unix individuals, MySQL can keep running as an administrator on Windows NT, and as an ordinary procedure in Windows 95/98 machines.

11.8 EXPERIMENTAL EVALUATION

11.8.1 Flow Diagram

A proposed algorithm based on the healthcare of patients shown in Figure 11.9. The parameters can be obtained from the present status of patients. In the case critical condition patients, the system can collect data continuously. The parameters collected

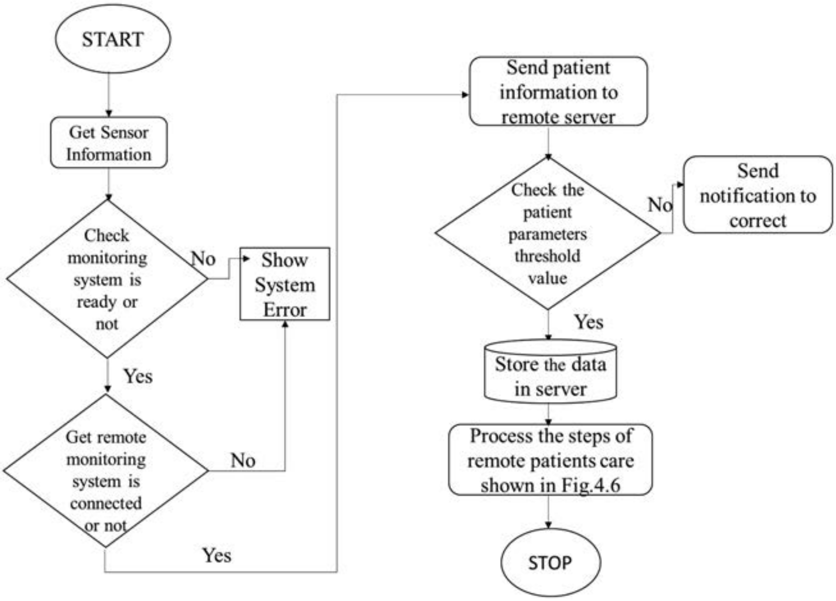

START
Get Sensor Information
Check monitoring system is ready or not
No
Show System Error
Yes
Get remote monitoring system is connected or not
No
Yes
Send patient information to remote server
Check the patient parameters threshold value
No
Send notification to correct
Yes
Store the data in server
Process the steps of remote patients care shown in Fig.4.6
STOP

FIGURE 11.9 Flowchart of the remote health monitoring and healthcare system.

are temperature, heat rate, blood pressure, respiration rate, ECG and so on. The proposed system contains an alarm system which generates beeps to notify the concerned doctor/nurse/care taker in case of an emergency. When the data deviates from a preset threshold value, a message is generated to notify the users.

The proposed algorithm is a generalized health-monitoring model that works on the principle of threshold limits, and is customized for individual remote monitoring. It will be designed in a way where the algorithm accepts various threshold limits for each parameter, and estimations of the threshold values can be defined on the basis of the essential parameters of the individuals. The customized algorithm for monitoring aids keep on changing threshold limits throughout the monitoring phase and analyses the health parameters such as heart rate after every 10 minutes and compares it with previous values to find out if any change occurred. A robust scanning mechanism has been applied in alarming module. In this module, the data from heart rate, blood pressure and body temperature are collected through sensors.

11.8.2 Experimental Analysis

In order to validate the proposed idea, a prototype model was developed and evaluated by *assess* of remote patient monitoring using IoMT and assisted living healthcare system as shown in Figure 11.10. The model has been constructed to receive data from all the listed sensors. However, the readings of the other wearable sensors have been validated in the laboratory as well. The step-by-step process of the hardware is connected to the power supply. The proposed system was detected by the SIM and was configured by Wi-Fi, which was indicated on the LCD display as 'OK' message after

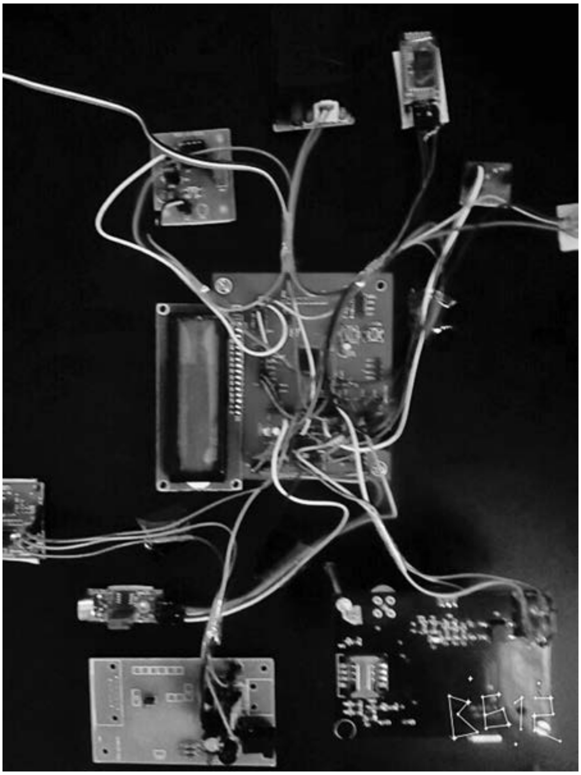


FIGURE 11.10 Prototype of the proposed remote patient monitoring system.

the configuration process was completed and the system was put online. Temperature, pulse rate and heart rate were measured by the sensors and the values were indicated on the LCD display, and simultaneous messages were sent to the doctor, caretaker, and physician through the Wi-Fi cloud. The sent data was viewed on an html webpage with a unique ID and messages were sent to the nurse, caretaker and doctor's mobile phone. The measured ECG waveform was indicated and displayed on the mobile. The wearable sensors with IoMT recorded the physiological parameters of the patients at home and at work. The recorded data was processed and communicated to the doctor, caretaker and nurse or physicians via a mobile phone data connection or Wi-Fi.

Most of the patient-monitoring systems are intended for a particular group or group of individuals suffering from different diseases [55] such as distressing sickness [56], dementia [57], hypertension [58] and diabetes [59], while some other patient monitoring systems are committed to the more established age group patients [60]. Only a few models are displayed for onexclusive portable patient monitoring systems [61,62]. A real-time signal detection algorithm is implemented to measure physical health data such as blood pressure, heart rate, pulse rate, and respiration including ECG signals monitoring in the proposed system. The proposed remote health-monitoring system sends numerous messages during irregular patterns detected in the ECG signal. The Proposed RHM empowers a patient to choose the health data analysis locally or on a centralized server. The local analysis of the received health data from the sensors can alert the clinicians through an alarm, allowing them to cross-examine a patient about his/her health condition. The remote patient monitoring system tends to be secure and safe by sending the monitoring information intermittently to the clinical database, which is typically deployed in mobile base units. The RHM system automatically contacts the healthcare provider or specialist about any irregularity in the measured signals.

As the remote health monitoring and healthcare services are rapidly progressing towards development, current emphasis is on introducing skill into the model for the autonomous decision. Intelligent health monitoring systems can assist doctors in translating the therapeutic medical information, directing and automating the heath monitoring process through intelligent expert systems, and a data management system can successfully encapsulate, extract and interpret real-world context aware information, ensuring doctors get the right information each time [63,64]. The data responds contrastingly relying upon the medicinal information and constant recording of the patients in various conditions. To help these kinds of frameworks, a few methods like data mining (for the presumed present medical condition of a patient), or applying a group algorithm to both current and historic data have been proposed [65,66]. Another approach for simple data mining is introduced as object oriented database system for server and customer [67].

The IoMT is addressing several challenges in sensing, analysing, and visualizing the data before designing the systems for integration into clinical practice. Visualization is integrated with several objects such as sensing, communicating and sharing the information over networks. The data received from the interconnected sensors at regular intervals is processed and the feedback action is provided by a network for analysing, planning and decision-making. The IoMT is a connecting object to the Internet and facilitates remote patient monitoring.

11.8.3 Security and Privacy Concerns of IoMT

The realization of the IoT requires changes in frameworks, architectures and communications that correspond to adaptable, versatile, secure, and unavoidable without being meddlesome [68]. The specialists expect that the technological advancements of the IoMT will present basic improvements in the areas of ethics, information insurance, specialized design, distinguishing proof of organized articles and administration. As more smart systems are connected to the Internet, potential security is required and good connection with feedback administration and information is needed. The security issues (assurance of information protection) may emerge amid data accumulation, transmission and sharing and consequently speaks to a basic segment for empowering across the board appropriation of IoMT technologies advancements and applications. The rapid developments of IoMT healthcare contains risks for security and privacy. Therefore, there is need to develop and integrate viable universal detection systems for healthcare security and privacy, as critical objectives are taken into account. To decrease and understand the risk of security and privacy in healthcare applications, a number of articles have been published [69–75]. The unauthorized use of such private information could present undesirable security risks to the patients [76].

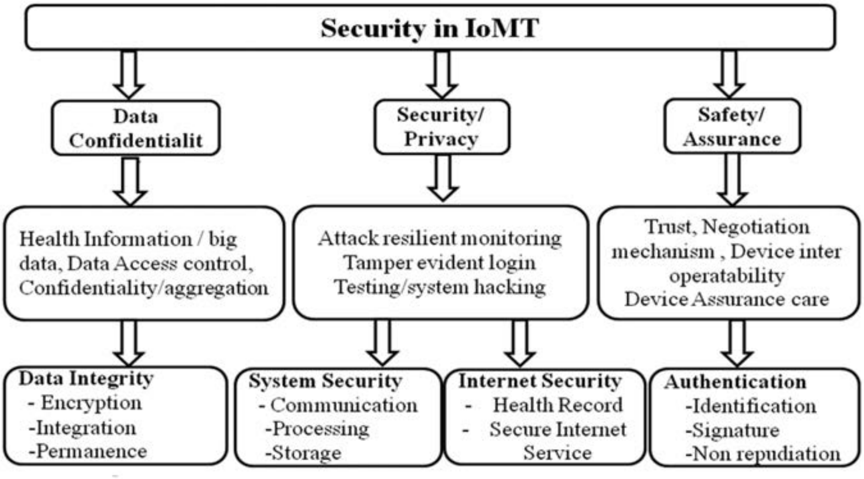

Security in IoMT
Data Confidentialit
Security/ Privacy
Safety/ Assurance
Health Information / big data, Data Access control, Confidentiality/aggregation
Attack resilient monitoring Tamper evident login Testing/system hacking
Trust, Negotiation mechanism , Device inter operatability Device Assurance care
Data Integrity - Encryption -Integration -Permanence
System Security - Communication -Processing -Storage
Internet Security - Health Record - Secure Internet Service
Authentication -Identification -Signature -Non repudiation

FIGURE 11.11 Security and privacy concerns of IoMT.

Subsequently, compact smart sensors to record, store, and transmit to understand information to a focal server, require secure approaches to transmit recorded information at rapid speed to guarantee that anytime. Ensuring privacy must not be constrained to specialized arrangements such as encryption, ID administration and security upgrading advancements. The prerequisites of IoMT communication systems in healthcare applications could be interoperability is expected to empower diverse things to cooperate in order to give the desired benefit. Bounded idleness and reliability should be conceded when managing emergency circumstances in order for the intercession to be powerful. Authentication, security, privacy and respectability are compulsory when sensitive information is exchanged over the effective (Figure 11.11).

Client verification is imperative in healthcare databases, as it is the initial phase in the whole health data access method. Confirmation systems are expected to check the client's character like: secret key, PIN, unique finger impression, signature, voice design, card, token, and so forth. Using these techniques we can be sure beyond any doubt that the data is sent by the confided in sender. By understanding of information respectability, the transmission of therapeutic reports from the patient to the medical staff can't be changed by any outside or unapproved source. Likewise, the patient's records can't be interpreted by anybody other than the authorized medical staff. Subsequently, confidentiality ensures that the patient's medical documents are protected from uninvolved assaults [77].

The data being produced, accumulated and shared through network devices must be protected with solid and usable verification techniques. As some of the received information might be confidential, and patients would prefer not to share it with others – sometimes even with family doctors – the revealing of such confidential information could lead to prejudice [76]. Subsequently, smart devices can record, store and transmit patient information to a cloud server; therefore, this requires secure approaches to transmit recorded data at rapid rates to ensure individual records can't be compromised at any time. It is imperative that data security, privacy and assurance be deliberately addressed at the planning stage. In summary, security should be fully incorporated into healthcare, from the device to the system, all the way to the server farm.

A solid security system incorporates verification advancements and procedures, confirming patient and supplier identification to guarantee devices are utilized by approved clients. The interchanges channels between the devices inside the IoT should likewise be secure to guarantee the validity of the data going through them. As healthcare frameworks store and process exceptionally delicate information, they ought to have appropriate security and protection structures and systems. Securing privacy must not only be confined to technical solutions such as encryption, ID administration and privacy enhancing measures, but should also include regular activities such as shopper assent, accumulation constraint, transparency, responsibility based self-direction, security accreditation, customer instruction and socio-ethical based customer rights, open mindfulness, divulgence, purchaser support [78]. However, data security, protection and information assurances should be deliberately addressed during the outline stage.

11.9 ADVANTAGE OF REMOTE PATIENT MONITORING

At present, only 10% of the patients are familiar with remote patient health monitoring (RPHM) systems, leaving 90% unaware of this opportunity. Currently, RPHM continues to gain acceptance in hospitals and healthcare centres, and many specialists are expressing interest in the next generation platforms to address the challenges and inefficiencies of the current patient monitoring platforms. Research surveys are stating that the RPHM market is growing rapidly, and in this context the advantage of RPHM for patients, care providers, public health authorities and insurance payers are reported in Table 11.1. IoMT is able to monitor, record and track the changes in

TABLE 11.1
Advantages of Remote Patient Healthcare Monitoring for Patients, Care Providers, Public Authorities and Insurance Payers

	Benefits for Patients	Benefits for Care Providers/ Public Health Authorities	Benefits for Insurance Payers
1	Better outcomes and quality in treatment	Enhance the access of patient health data in real time	Better visibility on patient compliance practices
2	Real-time support and interventions improve the disease management and reduce errors	Continuous monitoring of patient health parameters, regardless of patients location	Better acceptability and accountability from patients and care providers
3	Prevent emergencies and re-admissions	The accuracy, reliability and relevance in reading data enhanced, which would provide better precision in treatment	Reduced costs of care and monitoring
4	Reduced hospital stays	Cost reduction from re-admissions and hospital stays	Real-time processing of patient documents

parameters over a specific time period. Doctors can prescribe the medication and suggest treatment methods based on the recorded changes or the history of the patient. Normal routine check-ups and hospital stays can be minimized. Digital records of patient health parameters on the clouds are becoming reliable, and storing data in a computer or memory device has benefits over printing on paper such as minimal chances of data loss.

11.10 APPLICATIONS OF REMOTE PATIENT HEALTH MONITORING AND HEALTHCARE PARADIGM

- The RPHM system mainly focuses on measuring, evaluating and communicating the sensor data of vital parameters, for example, temperature, heart rate, ECG, pulse rate etc;
- RPHM system enables to diagnose and evaluate the obtained data at specific circumstances such as medial practice and facilitate projection for a framework of diseases at an initial stage, prevention, diagnosis, and treatment with overall management;
- RPHM system is able to record long-term clinical data and access the patient's physiological information, which can be sent to the physicians/doctors/caretakers when needed;
- The sensory data of remote patients are easy to analyse and can be presented to physicians in a prescribed format, and are eventually easy to start using their clinical practice.

11.11 LIMITATIONS AND CHALLENGES

The successful implementation of IoMT-based remote patient monitoring systems are facing certain limitations and challenges in terms of technology and networking such as accurate data acquisition, inter-operability between hardware and software, bandwidth, quality of health services, limitation of battery life, sensor biocompatibility and so on. The emerging technology and advances in the field of Internet communication bring many challenges coupled with contribution in the growth of the medical field. The significant challenges in the domain of IoMT are design in hardware and software implementation, design optimization of wearable sensors and real-time processing with low power consumption sensors. Network performance is likely to be constrained in the memory of the system, which influences the performance and management of network-like devices, as well as bandwidth and flexibility of data volume, data security and data privacy. In addition to the network and technological challenges, the most common and general challenges are user attitudes, technological acceptance and barriers, confidentiality, legal issues, ethical and administrative barriers, implementation costs, maintenance of the system and sufficient investments. Overcoming these difficulties in the area of IoMT will enhance the standard of remote healthcare. IoMT provides better and reliable healthcare and health monitoring services, as it bridges the gap between doctors, patient and healthcare services. IoMT enables the doctors and hospital staff to work more precisely and actively with less effort.

11.12 CONCLUSIONS AND FUTURE ENHANCEMENTS

In this chapter, we reviewed the current state of remote patient monitoring using IoMT-related services and technologies in remote healthcare and monitoring. In addition, future perspectives for RPM technologies in clinical practice have also been discussed. A significant number of research challenges have been highlighted, which are expected to be major research areas in the future. In the present work, an IoMT-based smart healthcare system has been designed using a microcontroller. Wearable sensors are used to measure the physiological parameters and the data is transmitted to the embedded controller and sent to the server through a Wi-Fi protocol. The measured physiological parameters are processed and displayed on an LCD so the patient can also monitor his/her health status. The health status of a patient is also sent via an SMS to the doctor/nurse/caretakers' mobile phone through a connected GSM modem where an alarm alerts the caretaker. The real-time data is monitored by the physician/caretakers after logging on to an html web page using a unique IP.

Future undertakings can be designed on the basis of the major challenges in terms of network and technology advances. For instance, there is a need for designing and developing hardware and software modules for better transmission of large and critical data with advanced communication networks. The real-time measurement of physiological parameters of the patient needs to be enhanced. Implementing Li-Fi (Light Fidelity) modules for uploading data may result in faster uploading of data into databases, which could also enhance the functionality of android applications. Future work should perhaps investigate the challenges that are constantly faced by mobile-based systems such as accuracy of critical signals, bandwidth, quality of health services, adaptable wireless technologies, inter-operability between different systems, data encryption and security. However, one shouldn't forget legal and ethical aspects, and to focus on developing user-friendly systems.

REFERENCES

1. Thimbleby H. Technology and Healthcare in future. *Journal of Public Health Research*. 2013;2(3):160–167.
2. White Paper. Internet of Things Strategic Research Roadmap, Antoine de Saint-Exupery, September 15, 2009.
3. Dey N, Hassanien AE, Bhatt C, Ashour A, Satapathy SC. *Book: Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*. Springer, 2018:3–20.
4. Dey N, Ashour AS, Borra S (Eds.). *Classification in BioApps: Automation of Decision Making*. Springer, 2017;26.
5. Tan L, Wang N. Future internet: The internet of things. *3rd International Conference on Advanced Computer Theory and Engineering*. 2010;5:376–380.
6. Wu M, Lu TJ, Ling FY, Sun J, Du HY. Research on the architecture of Internet of Things. *3rd International Conference on Advanced Computer Theory and Engineering*. 2010;5:484–487.
7. Pandikumar S, Vetrivel RS. Internet of things based architecture of web and smart home interface using GSM. *International Journal of Innovative Research in Science, Engineering and Technology*. 2014;3(3):1721–1727.
8. Gómez J, Huete JF, Hoyos O, Perez L, Grigori D. Interaction system based on internet of things as support for education. *Procedia Computer Science*. 2013;21:132–139.

9. Botterman M. Internet of Things: An early reality of the future Internet. In: *Meeting at EU*, Prague, 2009.
10. Sharma M, Siddiqui A. RFID based mobiles: Next generation applications. In: *Inf. Manag. Eng., 2nd IEEE Int. Conf.*, Chengdu, China, 2010;523–526.
11. Ziegler J, Urbas L. Advanced interaction metaphors for RFID-tagged physical artefacts. In: *RFID-Technologies Appl. IEEE Int. Conf.*, Sitges, Spain, 2011;73–80.
12. Pandikumar S, Vetrivel RS. Internet of things based architecture of web and smart home interface using GSM. *International Journal of Advanced Computer Science and Technology*. 2014;3(3):1721–1727.
13. Dimitrov DV. Medical internet of things and big data in healthcare. *Healthcare Informatics Research*. 2016;22(3):156–163.
14. Patel S, Park H, Bonato P, Chan L, Rodgers M. A review of wearable sensors and systems with application in rehabilitation. *Journal of Neuroengineering and Rehabilitation*. 2012;9:21.
15. Yu L, Lu Y, Zhu X. Smart hospital based on internet of things. *Journal of Networks*. 2012;7(10):1654–1667.
16. Yao Q, Tian Y, Li PF, Tian LL, Qian YM, Li JS. Design and development of a medical big data processing system based on Hadoop. *Journal of Medical Systems*. 2015;39(3):23.
17. Lee CH, Yoon HJ. Medical big data: Promise and challenges. *Kidney Research and Clinical Practice*. 2017;36(1):3–11.
18. Kruse CS, Goswamy R, Raval Y, Marawi S. Challenges and opportunities of big data in health care: A systematic review. *JMIR Medical Informatics*. 2016;4(4):e38.
19. Bhatt C, Dey N, Amira A. *Book: Internet of Things and Big Data Technologies for Next Generation Healthcare*. 2016:3–33.
20. Elhayatmy G, Dey N, Ashour AS. Internet of things based wireless body area network in healthcare. In *Internet of Things and Big Data Analytics toward Next-Generation Intelligence*. Springer, Cham, 2018:3–20.
21. Aminian M, Reza Naji H. A hospital healthcare monitoring system using wireless sensor networks. *International Journal of Medical Informatics*. 2013;4:121.
22. Prashob B, Vegnesh N, Sandesh W. Remote health monitoring using IOT. *International Journal of Advance Research, Ideas and Innovations in Technology*. 2017;3(2):23–24.
23. Yadav D, Agrawal M, Bhatnagar U, Gupta S. Real time health monitoring using GPRS technology. *International Journal on Recent and Innovation Trends in Computing and Communication*. 2013;1(4):368–372.
24. Dey N, Ashour AS, Shi F, Fong SJ, Sherratt RS. Developing residential wireless sensor networks for ECG healthcare monitoring. *IEEE Transactions on Consumer Electronics*. 2017;63(4):442–449.
25. Dey N, Ashour AS, Shi F, Sherratt RS. Wireless capsule gastrointestinal endoscopy: Direction-of-arrival estimation based localization survey. *IEEE Reviews in Biomedical Engineering*. 2017;10:2–11.
26. Kakria P, Tripathi NK, Kitipawang P. A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors. *International Journal of Telemedicine and Applications*. 2015;2015:1–11.
27. Mohammadzadeh N, Safdari R. Patient monitoring in mobile health: Opportunities and challenges. *Medical Archives*. 2014;68(1):57–60.
28. Yin Y, Zeng Y, Chen X, Fan Y. The internet of things in healthcare: An overview. *Journal of Industrial Information Integration*. 2016;1:3–13.
29. Sullivan HT, Sahasrabudhe S. Envisioning inclusive futures: Technology-based assistive sensory and action substitution. *Futures Journal*. 2017;87:140–148.
30. Wang X, Wang JT, Zhang X, Song J. A multiple communication standards compatible IoT system for medical usage. In: *IEEE Faible Tension Faible Consommation*, Paris, France, 2013;1–4.

31. Xu B, Xu LD, Cai H, Xie C, Hu J, Bu F. Ubiquitous data accessing method in IoT-based information system for emergency medical services. *IEEE Transactions on Industrial Informatics*. 2014;10(2):1578–1586.
32. Kolici V, Spaho E, Matsuo K, Caballe S, Barolli L, Xhafa F. Implementation of a medical support system considering P2P and IoT technologies. In: *8th Int. Conf. on Complex, Intelligent and Software Intensive Systems*, Birmingham, UK, 2014;101–106.
33. Sandholm T, Magnusson B, Johnsson BA. An on-demand WebRTC and IoT device tunneling service for hospitals. In: *International Conference on Future Internet of Things and Cloud*, Barcelona, 2014;53–60.
34. Ang LM, Seng KP, Heng TZ. Information communication assistive technologies for visually impaired people. *International Journal of Ambient Computing and Intelligence*. 2016;7(1):45–68.
35. Kamal S, Dey N, Ashour AS, Ripon S, Balas VE, Kaysar MS. Fbmapping: An automated system for monitoring Face book data. *Neural Network World*. 2017;1:27–57.
36. Acharjya D, Anitha A. A comparative study of statistical and rough computing models in predictive data analysis. *International Journal of Ambient Computing and Intelligence*. 2017;8(2):32–51.
37. Chakraborty S, Chatterjee S, Ashour AS, Mali K, Dey N. Intelligent computing in medical imaging: A study. In: *Advancements in Applied Metaheuristic Computing*. 2017;143.
38. Matallah H, Belalem G, Bouamrane K. Towards a new model of storage and access to data in big data and cloud computing. *International Journal of Ambient Computing and Intelligence*. 2017;8(4):31–44.
39. Yilmaz T, Foster R, Hao Y. Detecting vital signs with weable wireless sensors. *Advances in Biosensors*. 2010;10(12):10837–10862.
40. Mane A, Dighe V, Gawali R, Sabale S, Gudadhe S. Location based service and health monitoring system for heart patient using IoT. *International Journal of Innovative Research in Computer and Communication Engineering*. 2017;5(11):11543–116548.
41. Daga N, Prasad S. Smart healthcare system using IoT. *International Journal of Professional Engineering Studies*. 2017;9(4):316–320.
42. Rizal Islam SM, Kwan D, Humaun KM, Mahmud H, Kwacha K-S. The internet of things for health care: A comprehensive survey. *IEEE Access*. 2015;3:678–708.
43. Hu F, Xie D, Shen S. On the application of the internet of things in the field of medical and healthcare. In: *IEEE Int. Conf. on Physical and Social Computing Green Computing and Communications*, Beijing, China, 2013:2053–2058.
44. Soyata T, Muraleedharan R, Funai C, Kwon M, Heinzelman W. Cloud-vision: Real-time face recognition using a mobile-cloudlet cloud acceleration architecture. In: *Proceedings of the IEEE Symposium on Computers and Communications*, Cappadocia, Turkey, 2012:59–66.
45. Hassanalieragh M, Page A, Soyata T, Sharma G, Aktas M, Mateos G, Kantarci B, Andreescu S. Health monitoring and management using internet of things (IoT) sensing with cloud-based processing: Opportunities and challenges. In: *IEEE International Conference on Services Computing*, New York, USA, 2015:285–292.
46. Majumder S, Mondal T, Jamal Deen M. Wearable sensors for remote health monitoring. *Advances in Biosensors*. 2017;17:130.
47. Chavan P, More P, Thorat N, Yewale S, Dhade P. ECG remote patient monitoring using cloud computing. *Imperial Journal of Interdisciplinary Research*. 2016;2(2):368–372.
48. Page A, Kocabas O, Soyata T, Aktas M, Couderc JP. Cloud based privacy-preserving remote ECG monitoring and surveillance. *Annals of Noninvasive Electrocardiology*. 2014;20(4):328–337.
49. Yang G, Xie L, Zheng LR. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. *IEEE Transactions on Industrial Informatics*. 2014;10(4):2180–2191.

50. Jara AJ, Zamora-Izquierdo MA, Skarmeta AF. Interconnection framework for mHealth and remote monitoring based on the Internet of Things. *IEEE Journal on Selected Areas in Communications*. 2013;31(9):47–65.
51. Rasid MFA, Musa WMW, Kadir NAA. Embedded gateway services for internet of things applications in ubiquitous healthcare. In: *2nd Int. Conf. Inf. Commun. Technol.*, Bandung, Indonesia, 2014:145–148.
52. Yang L, Ge Y, Li W, Rao W, Shen W. A home mobile healthcare system for wheel chair users. In: *IEEE Int. Conf. Comput. Supported Cooperat.*, Hsinchu, Taiwan, 2014:609–614.
53. Castillejo P, Martinez JF, Rodriguez-Molina J, Cuerva A. Integration of wearable devices in a wireless sensor network for an e-health application. *IEEE Wireless Communications*. 2013;20(4):38–49.
54. Pandikumar SA. Model for GSM based intelligence PC monitoring system. *International Journal of Advanced Computer Science and Technology*. 2012;2(2):85–88.
55. Fortier P, Viall B. Development of a mobile cardiac wellness application and integrated wearable sensor suite. In: *SENSORCOMM. 5th IC on Sensor Technologies and Applications*, Nice/Saint Laurent du Var, France, 2011:301–306.
56. Dickerson RF, Gorlin EI, Stankovic JA. Empath: A continuous remote emotional health monitoring system for depressive illness. *Proceedings of the 2nd Conference on Wireless Health*. 2011;5:1–10.
57. Wai A, Fook F, Jayachandran M, Song Z, Biswas J, Nugent C, Mulvenna M, Lee J, Yap L. Smart wireless continence management system for elderly with dementia. In: *IEEE 10th IC on e-Health Networking, Applications and Services, Health Com.*, Singapore, 2008:33–34.
58. Miao F, Miao X, Shangguan W, Li Y. Mobi healthcare system: Body sensor network based m-health system for healthcare application. *e-Health Telecommunication Systems and Networks*. 2012;1(1):12–18.
59. Logan AG, McIsaac WJ, Tisler A, Irvine MJ, Saunders A, Dunai A, Rizo CA et al. Mobile phone based remote patient monitoring system for management of hypertension in diabetic patients. *American Journal of Hypertension*. 2007;20(9):942–948.
60. Bourouis A, Feham M, Bouchachia A. Ubiquitous mobile health monitoring system for elderly (UMHMSE). *International Journal of Computer Science & Information Technology (IJCSIT)*. 2011;3(3), arXiv preprint arXiv: 2011;1107.3695:74–82.
61. Jones V, Gay V, Leijdekkers P. Body sensor networks for mobile health monitoring: Experience in Europe and Australia. In: *4th IC on Digital Society, IEEE Computer Society*, Sint Maarten, Netherlands Antilles, 2010:204–209.
62. Pawar P, Jones V, van Beijnum BJF, Hermens H. A framework for the comparison of mobile patient monitoring systems. *Journal of Biomedical Informatics*. 2012;45(3):544–556.
63. Fotiadis D, Likas A, Protopappas V. *Intelligent Patient Monitoring*. Wiley Encyclopedia of Biomedical Engineering, 2006.
64. Donoghue OJ, Herbert J. Data management system: A context aware architecture for pervasive patient monitoring. In: *Proceedings of the 3rd IC on Smart Homes and Health Telematic*, Nagasaki, Japan, 2005:159–166.
65. Patil D, Andhalkar S, Gund M, Agrawal B, Biyani R, Wadhai V. An adaptive parameter free data mining approach for healthcare application. *International Journal of Advanced Computer Science and Applications*. 2012;3(1):55–59.
66. Kamal MS, Dey N, Ashour AS. Large scale medical data mining for accurate diagnosis: A blueprint. In: *Handbook of Large-Scale Distributed Computing in Smart Healthcare*. Springer, Cham, 2017:157–176.
67. Ranjan R, Varma S. Object-oriented design for wireless sensor network assisted global patient care monitoring system. *International Journal of Computer Applications*. 2012;45(3):8–15.

68. Yan L, Zhang Y, Yang LT, Ning H. *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*. CRC Press, 2008.
69. Shih F, Zhang M. Towards supporting contextual privacy in body sensor networks for health. Monitoring service. In: *W3C Workshop on Privacy and Data Usage Control*, Cambridge, MA, 2010.
70. Appari A, Johnson ME. Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management*. 2010;6(4):279–314.
71. Löhr H, Sadeghi AR, Winandy M. Securing the e-health cloud. In: *Proceedings of the 1st ACM International Health Informatics Symposium*, Arlington, Virginia, USA, 2010:220–229.
72. Tsai FS. Security issues in e-healthcare. *Journal of Medical and Biological Engineering*. 2010;30(4):209–214.
73. Wilkowska W, Ziefle M. Privacy and data security in E-health: Requirements from the user's perspective. *Journal of Health Informatics*. 2012;18(3):191–201.
74. Agrawal V. Security and privacy issues in wireless sensor networks for healthcare. In: *Internet of Things User Centric IoT*, Rome, Italy, 2014:223–228.
75. Kim JT. Privacy and security issues for healthcare system with embedded RFID system on internet of things. *Advanced Science and Technology Letters*. 2014;7(2):109–112.
76. Lake D, Milito R, Morrow M, Vargheese R. Internet of things: Architectural framework for eHealth security. *Journal of ICT Standardization*. 2014, River Publishing, vol 1, 301–328.
77. Divi K, Kanjee MR, Liu H. Secure architecture for healthcare Wireless Sensor Networks. In: *IEEE 6th International Conference on Information Assurance and Security*, Atlanta, GA, USA, 2010:131–136.
78. Hasić H, Vujović V. Civil law protection of the elements comprising the "Internet of Things" from the perspective of the legal owner of the property in question. *Infoteh-Jahorina*. 2014;13:1005–1011.

17 IoT-Based Wearable Medical Devices

Avitaj Mitra, Abanish Roy, Harshit Nanda, Riddhi Srivastava, and Gayathri M.

17.1 INTRODUCTION

In the current day and age, with increasing usage of technology, the majority of people in urban areas work white-collar jobs. These jobs, although well paid, involve working in front of a screen for extended periods of time. The lifestyle of these people is becoming increasingly sedentary. This, combined with a propensity for consuming large quantities of junk food, leaves them susceptible to various diseases like diabetes, hypertension, cholesterol, heart disorders, and many more.

The Internet of things (IoT) is a concept, which in simple terms is the interconnectivity of sensors, actuators, and microcontrollers, etc. along with smart devices and Internet connectivity to exchange and modify large sets of data. A subset of IoT is wearable medical devices (WMDs). As the name suggests, these are small contraptions like a band or a small microchip, which can be worn on any part of the body and can help to monitor certain parameters and send warning signals if necessary. The basic components of a WMD are the chip/band, a sensor, a detector, a Bluetooth system for data transmission, and an alarm detector system. Since the simplest method to treat diseases is to detect the symptoms as early as possible, WMD's can prove to be hugely beneficial in this aspect.

Apart from the usual problems faced in the initial concept design formulation, obtaining funds for components, etc. possibly the biggest challenge preventing the large-scale commercialization of medical devices is the time taken for FDA approval. A probable reason for this is that these devices target the core physiological functions of the body. Any kind of operational failure can, in the worst possible scenario, lead to the death of the patient.

There is no doubt about the fact that WMDs, though currently at a nascent stage in their development, is the technology for the future. With the advent of smartphone technology and with increasing and widespread access to Internet services for the common people, health care professionals will come to depend upon wearable devices as a means to improve health care and reduce patient mortality rates.

17.1.1 The History of Medical Devices

WMDs are a classification of devices generally attached to the surface of the skin of an individual. They usually assist in monitoring certain parameters such as heartbeat, blood pressure, and oxygenation levels. An example of this is a heartbeat monitor or an SpO2 sensor. The other major function of a WMD is to improve the efficiency of any kind of cognitive function, which has degenerated in the human body. An example of this kind of medical device is a hearing aid/implant. The earliest examples of medical devices can be considered to be stethoscopes, sphygmomanometers, earlier forms of CT and MRI scanners, etc. However, the shift in medical device manufacturing received a big boost with the advent of the IC, semiconductors, and BioMEMS or biological microelectromechanical systems technology in the 1970s and 1980s. This led to devices small in size, increasing their portability and overall utility. The major impact has been on cardiovascular devices with a number of heart valves and stents coming up in the market. All this has increased not only the lifespan of patients but also provided comfort and improved their daily lives.

17.1.2 The Advent of IoT

The IoT is a global system facilitating the exchange of information in a secure manner. The primary architecture is based on data communication, facilitated by the use of RFID (Radio Frequency Identification) tags (Weber and Weber 2010). In the current industrial scenario, the most popular method is that of an EPC (Electronic Product Code). In simple terms, this means that a unique code is given to any object with an RFID tag, which helps to track the object remotely, without causing any discomfort to the individual carrying the object. The entire data is not saved within the RFID tag, but the information is made available to servers on the Internet by cross-linking with the help of an ONS (Object Naming System).

The ONS is a centralized system linking both metadata and services and is operated by a private company, VeriSign. The ONS architecture is designed to be multifunctional and can be used for computation, recognition and identification of objects, and retrieval of datasets from the Internet.

The ONS is based on the more commonly used and well-known domain name system (DNS). In order to retrieve information about an object, the EPC of the object should be converted into a form the DNS can understand. This is done by using the usual format of a domain name ("dot," delimited, "domain name from left to right"). The EPC is usually encoded within the domain name and is used within the existing architecture of the DNS. ONS can be considered to be a subset of the DNS.

Thus, using IoT, the data collected by the WMDs can be transmitted to a storage device and can be accessed by a medical practitioner in real time. This has enabled the development of new age WMDs, which are aimed at improving health care delivery, with minimal effect on patient comfort and mobility.

17.1.3 The Age of WMDs

The recent advances in wireless sensor technology and information technology have resulted in an unprecedented number of technological advancements in the field of WMDs based on IoT (IoT). The use of WMDs for both monitoring and diagnostic purposes is rapidly becoming popular. With an increasing number of people owning smartphones enabled with Bluetooth, global positioning system (GPS), and Internet service it has become much easier to link WMDs, which measure physiological parameters for a software. This has opened up new avenues in medical devices currently being explored.

Round-the-clock monitoring of certain physiological parameters are of paramount importance in the detection and control of cardiovascular diseases. With the development of advanced wireless sensors, we no longer need to confine a patient in a hospital bed to monitor his/her vitals; it can be done remotely as the patients carry on with their daily lives. The power of remotely monitoring the vitals of a patient can go a long way in exponentially increasing the reach of proper health care facilities to semirural and rural locations. With the advent of IoT, these physiological data can be stored and transferred to the desktop of a physician for monitoring in real time.

17.2 MECHANISM OF WMDs

The heart of any WMD is data. In this case, data refers to patient history of the vital signs such as core body temperature, heart rate, and blood pressure. The functioning of any WMD can be broken down into the following: collection of raw data, transmitting the raw data using Ethernet, Bluetooth, or wireless technology, uploading the data into a secure server linked to a research facility and/or a hospital, postprocessing of the data using mathematical algorithms and statistical analysis, and finally displaying and storing the processed data using encrypted files, which can then be sent to individual patients.

The detection, diagnosis, and treatment of diseases using WMDs depends upon various factors such as the type of bio signal extracted, previous patient history, any genetic aspects which may interfere with electronic signals from the wearable device, the age of the person, work history (for a working professional, round-the-clock remote monitoring may not be a feasible option), and any kind of lifestyle changes, which need to be incorporated, etc. In short, it can be said there is no perfect wearable device, or no ideal form of treatment existing for an individual, and the diagnosis and treatment need to be carried out on a case-by-case basis.

17.3 DETECTION, DIAGNOSIS, AND TREATMENT

17.3.1 Hypertension

With the rise in the percentage of the population suffering from obesity, the number of people suffering from hypertension is on the rise. High blood pressure is often asymptomatic, and thus hypertension goes on unnoticed in many patients before it is too late. Recent studies have shown that blood pressure variability, or BPV, is an important factor for determining the cardiovascular health of an individual. Traditionally, blood pressure was measured in a clinic by a trained technician, nurse, or a doctor. In that scenario, constant monitoring of blood pressure was not possible. To tackle this problem, medical researchers and engineers have come up with a few types of WMD (Yilmaz et al. 2010).

The first type of medical device designed for home use by nontrained personnel was based on the oscillometric method. It consists of an armband, much like the one used in clinics attached to a monitoring device with a display. This device could measure the blood pressure with respect to the brachial artery. A similar type of device was later designed able to measure the blood pressure using the radial artery (Teng et al. 2008).

This new device used a wrist cuff instead of an armband. This enabled the development of smart wristwatches for blood pressure monitoring and display. The smartwatch could be connected to a smartphone to store and relay the data as per needed. The wrist cuff or smartwatch system made it easier to use the device outdoors with ease. It reduced the bulkiness of the previous devices (Yilmaz et al. 2010).

Although these devices enabled people to monitor their blood pressure without the aid of a doctor or a trained clinician, there were certain drawbacks. One of the major drawbacks was the sensitivity and data reliability. Second, these methods do not allow for a continuous monitoring of blood pressure; at best these devices could allow the monitoring of blood pressure at a regular interval of around 15–30 minutes. These methods can also lead to wrist or arm pain, sleep disturbance, and can even cause skin allergy (Bobade and Walli 2015).

Vasotrac (Medwave Inc., Arden Hills, MN) is a popular wristwatch-based ambulatory noninvasive blood pressure sensor. This medical device consists of a circular sensor placed on top of the radial artery (marked using a disposable adhesive tape) and a display unit. For reliable measurement, an external pressure needs to be applied. The data is collected from the sensor, processed by a control unit, and then displayed on the screen. Vasotrac is a good and reliable device for periodic measurement of blood pressure, but not for continuous blood pressure monitoring (Findlay et al. 2006).

17.3.2 Epilepsy

Epilepsy is a functional pathophysiology present in the cerebrum part of the brain, which arises in almost all mammalian species. It's a medical condition classified with a broader range of different types of seizures and activation from one individual to another. Different types of brain seizures in epilepsy lead to the development of brain tumors.

In epilepsy, people face different types of brain seizures. This marks the development of brain tumors. A person suffering with epilepsy has higher chances of suffering from a depression. This is due to higher exposure to chronic stress (Duyn et al. 2007). During sleep nocturnal seizures occur, which worsen the condition of the patient. These seizures mostly occur at specific sleep stages or during sleep instability (Bernhardt et al. 2015). The recent advance in the pathogenesis of epilepsy is the involvement of genetic testing. Next generation sequencing has proven to be effective for revealing epilepsy causing gene mutations (Witt et al. 2013).

Epilepsy is initially treated with medications where approximately 70% of patients get complete seizure control (French 2007). However, this is not possible for patients who have poor seizure control, and for them several other methods are used such as medical management, surgery, vagus nerve stimulation (VNS), ketogenic diets, and complementary therapies.

To detect brain abnormalities, several techniques are used such as electroencephalogram (EEG), computerized tomography (CT) scan (Duyn et al. 2007), magnetic resonance imaging (MRI) (Jewells and Shin 2014), functional MRI (Fang et al. 2017), positron emission tomography (PET) (You et al. 2012), and single photon emission computerized tomography (SPECT) (Błaszczyk and Czuczwar 2016).

There are various WMDs being developed for the timely detection of epileptic seizures. One of the latest devices is SeizeIT, which is being developed in KU Leuven (Vandecasteele et al. 2017). It is based on designing a WMD that detects the electrocardiography (ECG) and photoplethysmography (PPG) in real time. The wearable ECG device proved to be as efficient as the wired hospital ECG systems, and thus allows for greater patient mobility and comfort. The sensitivity of the wearable ECG device was 70%, whereas that of the hospital system was 57%, and it had a slightly greater false alarm rate (2.11 per hour as compared to 1.92 per hour rate of the hospital system) making it an ideal choice for people suffering from epilepsy.

The Brain Sentinel is an interventional device for the detection of tonic clonic seizures. It is based on measurement of electromyography (EMG) signals from the concerned subject and then analyzing and transmitting the data to look for identifiable patterns. The subjects were monitored for seizure-based activity for a period of 4.5 years and the test results are currently being analyzed for any favorable outcomes. However, one disadvantage is that the study excludes pregnant females from participation.

The Embrace Watch is an IoT-based device providing regular monitoring of vital signs for epilepsy-afflicted patients. It is considered to be a therapeutic rather than a diagnostic device, which transmits the dataset to a smartphone using Bluetooth technology. The data is then uploaded to Empatica servers where further analysis and processing is performed.

The neurospace responsive neurostimulator (RNS) is a recently FDA-approved device for epilepsy treatment. The principle behind this device is monitoring the brain activity and thus delivering an electrical stimulus when there is a detection of abnormal brain activity in different regions of brain (Thomas and Jobst 2015).

The RNS system is approved in the United States as a medical therapy for treatment of partial onset seizures of epilepsy. The different parts of this system include a stimulator, implanted leads, and wireless programming wands connected to a complex computer hardware and software system. The stimulator works on a design where wires connected to electrodes are implanted in the hippocampus area of the brain. The machine targets the resistant partial seizure onset zone.

The neurotransmitter monitors the ECoG (electrocorticography) activity and utilizes various methods for detection of abnormal brain activity. Measurement of changes in electrical activity and frequencies is done with this machine. The four proposed theories for mechanism of action includes:

- Depolarization blockage, which refers to changes in voltage-gated channels leading to process of inhibition in excitability (Beurrier et al. 2001).
- Synaptic inhibition refers to depolarization effects of distal axon.
- Synaptic depression, which causes the decrease in release of neurotransmitters (McIntyre et al. 2004).
- Electrical stimulation by modulating the action of pathologic networks (Durand 1986).

The RNS system does not include the allowance for external recordings and includes only limited sampling for selective ECoG. A comprehensive file of the data obtained through this system is very expensive and is difficult to track the efficacy of seizures. Further research and experiments are currently carried out for provision of better understanding and effects of this system on the human body.

17.3.3 Cancer

Cancer is among the deadliest diseases in the world, for which there is no comprehensive cure till now. Early detection of cancer can enable its treatment is most cases. However, a large percentage of the cancer cases are detected in the late stages, where nothing much can be done except to ease the pain and accept the inevitable outcome. Countless research groups across the globe are working on developing methods to enable early detection of cancers to give patients a fighting chance, and to hopefully defeat this deadly disease.

The advent of IoT and WMDs has brought about great improvements in the cancer care delivery system. Real-time data collection and analysis has undergone massive improvements in the last few years (Sledge et al. 2013). CancerLinQ, an initiative of the American Society of Clinical Oncology focuses on collecting and analyzing patient data from electronic health data to drive the process of developing better cancer care technologies.

Patient generated health data (PGHD) is an important tool in the cancer care delivery system. It includes the data collected from the patient's regular environment in form of WMD data, other local sensor data, and outcomes reported by the patients. PGHD enables us to have a holistic view on the real-time health of the patient (Chung et al. 2016). IoT technologies can be used to collect and transmit these PGHD to oncologists and other researchers in real time. Because of IoT and WMDs, it is possible to collect such health data outside the clinic in real time.

There are a few sensor-based devices having been developed to detect various types of cancer in their early stages. A majority of these devices have focused on skin cancer and breast cancer detection. One such device was developed by S. K. Attili et al., which is a lightweight, organic light-emitting diode using photo-dynamic therapy (PDT) to detect skin cancer (Attili et al. 2009). Some of the other devices for skin cancer detection include a wearable designed by D. D. Godoy et al. which has a series of smart sensors able to detect the ambient temperature, humidity, light, and UV and notifies user through bluetooth about possible UV-harm using a smartphone-based application (Ray et al. 2017). My UV Patch and Violet Plus are two more WMDs to be worn around the wrist, which detects the UV radiation of the sun on the skin—one of the primary causes of skin cancer. The former is designed as an adhesive patch, whereas the latter is designed as a clip attached module.

In case of breast cancer, A. Rahman et al. designed a compact and ultrawide band antenna placed on a flexible substrate, which was able to measure breast cancer using microwave imaging (Rahman et al. 2016). Teng et al. 2017, developed a diffusion-based optical probe working on the principle of using continuous waves to supply the hemodynamic response during neoadjuvant chemotherapy infusions (Teng et al. 2017). H. Bahrami et al. developed a lightweight, flexible, and cheap microwave array of antennas able to detect breast cancer (Bahramiabarghouei et al. 2015).

Beyond these few devices, researchers and engineers around the world are developing better wearable devices integrated with IoT to detect cancer at an early stage. Although most of the devices discussed focused on skin and breast cancer, some research is being done to develop devices to detect prostate cancer (Ray et al. 2017).

17.3.4 Migraines

Migraine is a disorder of the neural as well as the vascular systems of the body (Silberstein and Silberstein 2004; Lipton et al. 2001). It is typically considered as a form of headache, though certain migraines can occur even without any kind of definitive pain.

In the general population, migraine is more prevalent among women, and nearly three times as many women suffer from migraine compared to adult men (Durand 1986). However, the onset of migraines is earlier among boys, which implies that until puberty, boys are likely to suffer from migraines more than girls (Abel 2009). Currently, three genes have been found for migraine and it is anticipated that further genes will be discovered, providing a genetic basis for explaining the disorder.

Migraines are likely to be a major distraction from work and familial responsibilities, since they have a debilitating effect on the energy and activity levels of an individual. Roughly one-third of migraineurs say they have missed school and/or work due to migraines, while 52% to 73% of the people feel their lives are being adversely affected by migraine attacks.

There has been extensive research carried out on the pathophysiology of migraines, however a definite cause or pathway has not yet been identified. The older theory, as propounded by Wolff, was that migraines were caused by constriction and dilation of cranial blood vessels.

However, current research points to the trigeminovascular system, or more specifically, the interactions between the ophthalmic area of the trigeminal nerve with the dura mater and the cranial blood vessels. A more recent theory postulates that the sensitization of neurons, specifically peripheral sensitization, may be responsible for the throbbing pain usually associated with migraines.

Treatment for migraine mostly involves either pharmacological drugs or sustained care under a neurologist and/or optometrist. Ensuring regular sleep and having meals on time may prevent migraines. Specific techniques, which have proven to be effective, include relaxation training, biofeedback training, and cognitive behavioral therapy.

Cefaly is an FDA-approved noninvasive method of treatment for individuals affected by frequent migraines. It is an external trigeminal nerve stimulation device, wherein a self-adhesive electrode is attached to the forehead and the Cefaly device is connected with it. Microimpulses are sent to the two branches of the trigeminal nerve to either relieve the pain in the head region or to prevent future migraine attacks.

17.4 COMPUTATIONAL TESTING METHODS

17.4.1 Epilepsy

Computational analysis provides a time- and cost-effective approach for the assessment of cognitive functions in patients suffering from epilepsy. The computerized testing is advantageous for the evaluation process in attenuation and they are also easily administrable.

17.4.1.1 Computerized Cognitive Testing in Epilepsy (CCTE)

This technique comprises mainly of performing eight tasks including digit span forward and backward, focused attention, incidental recollection issues, verbal learning, and figular memory (Kurzbuch et al. 2013). The performance in various subsets of CCTE shows a match with the results obtained in paper-pencil tests and thus, validates epilepsy (Orsini et al. 2016).

17.4.1.2 Cognitive Drug Research Computerized Assessment System (CDR)

The different assessment techniques of core aspects of cognitive function sustain the ability to conduct various activities in day-to-day life. The major mechanism underlying this technique is change over time in cognitive functions. This technique is simple to administer and is applicable in the studies on psychomotor effects, which are produced by remacenide and carbamazepine in the diagnostic treatment of newly developed epilepsy (Jan 2007).

17.4.1.3 Cognitive Neurophysiological Test (CNT)

The major advantage of this technique is it incorporates the speed and precision of task performance, as well as type of neural resources and the efforts to provide levels of performance and alertness are increased by this test. The additional knowledge is therefore increased to the specific effects of drugs and their in-depth pharmacokinetics and pharmacodynamics in the human body (Tufenkjian and Lüders 2012; Packer et al. 2015). Validation of this test is in the intellectual effects of antiepileptic drugs (Stufflebeam 2011; Hasegawa 2016).

17.4.1.4 FePsy

It comprises the eleven computerized tests for neurophysiological functions and is a relative database system for storing all the obtained results. It includes various subsets of tests for the measurement of different side-effects produced by the drugs. The simultaneous EEG recording is used to assess the effects of frequency and short and epileptiform EEG discharges in the absence of seizure (Menicucci et al. 2015; Stufflebeam 2011).

17.4.1.5 Neurocog FX

The key feature of this computerized software is the assessment of patients suffering from epilepsy and neurological diseases with respective experimental setups. This specific test was designed to be used in detection of CNS diseases and monitoring neuro-oncology and neurosurgery (Helmstaedter et al. 1996). This software is available only in Germany and the reaction of the patient is monitored in real time.

17.4.2 Cancer

In recent years, there has been several developments in the field of detecting cancer in its early stages using computer programs and applications. There have been some major breakthroughs in this regard.

In 2015, a team of scientists and engineers from the Technical University of Denmark developed a set of algorithms, dubbed as TumorTracer, able to detect the exact location of cancer with a nearly 85% success rate. It enabled the proper identification of the tissue of origin of the cancer, which is crucial for designing a proper treatment plan. This was a game changer for the people who suffered from cancer, whose primary origin was difficult to locate using conventional methods (Marquard et al. 2015).

In March 2017, a team of researchers from the University of California, Los Angeles designed a computer program dubbed CancerLocator, which could detect the tumor's DNA and from where it was coming from using blood samples of the patients. This program works by looking for specific molecular patterns in cancer DNA. It exploits the theory that cell free DNA from cancer cells are often found in the blood stream. By comparing their sequence with a known database of tumor cell sequences it was possible to both detect the cancer and locate its origin (Kang et al. 2017).

Beyond these two, there are two important algorithms used by several research groups to diagnose cancer. One of them was random forest. Cuong Nguyen et al., in 2013, designed a system based on this algorithm able to differentiate benign breast cancer tumors from malignant ones using a random forest algorithm. It was able to do so with an accuracy rate greater than 99% (Nguyen et al. 2013). This method was obtained to solve diagnosis problems by classifying the Wisconsin Breast Cancer Diagnosis Dataset (WBCDD) and to solve prognosis problems by classifying it.

Another algorithm popularly used in cancer detection is support vector machine (Sweilam et al. 2010).

17.5 CONCLUSION

To summarize, it is clear that WMDs have certainly proven to be hugely beneficial for the health care community. Not only have they significantly improved the lives of people suffering from various disorders, they have also made the job of medical professionals easier by introducing the concept of remote monitoring. The potential drawbacks, however minor, cannot be entirely ignored. Security and confidentiality of patient data is absolutely crucial and forms the framework of wearable devices. The unreasonably high cost of certain devices can sometimes act as a deterrent, however with increasingly newer technologies being developed, it can be hoped that wearable devices will become affordable for a majority of the population in the near future.

REFERENCES

Abel, H. 2009. "Migraine Headaches: Diagnosis and Management." *Optometry* 80 (3). Mosby, Inc:138–48. https://doi.org/10.1016/j.optm.2008.06.008.

Attili, S. K., A. Lesar, A. McNeill, M. Camacho-Lopez, H. Moseley, S. Ibbotson, I. D. W. Samuel, and J. Ferguson. 2009. "An Open Pilot Study of Ambulatory Photodynamic Therapy Using a Wearable Low-Irradiance Organic Light-Emitting Diode Light Source in the Treatment of Nonmelanoma Skin Cancer." *British Journal of Dermatology* 161 (1):170–73. https://doi.org/10.1111/j.1365-2133.2009.09096.x.

Bahramiabarghouei, H., E. Porter, A. Santorelli, B. Gosselin, M. Popović, and L. A. Rusch. 2015. "Flexible 16 Antenna Array for Microwave Breast Cancer Detection." *IEEE Transactions on Biomedical Engineering* 62 (10):2516–25. https://doi.org/10.1109/TBME.2015.2434956.

Bernhardt, B. C., S.-J. Hong, A. Bernasconi, and N. Bernasconi. 2015. "Magnetic Resonance Imaging Pattern Learning in Temporal Lobe Epilepsy: Classification and Prognostics." *Annals of Neurology* 77 (3):436–46. https://doi.org/10.1002/ana.24341.

Beurrier, C., B. Bioulac, J. Audin, and C. Hammond. 2001. "High-Frequency Stimulation Produces a Transient Blockade of Voltage-Gated Currents in Subthalamic Neurons." *J Neurophysiol* 85 (4):1351–56. http://www.ncbi.nlm.nih.gov/pubmed/11287459%5Cnhttp://jn.physiology.org/content/jn/85/4/1351.full.pdf.

Błaszczyk, B., and S. J. Czuczwar. 2016. "Epilepsy Coexisting with Depression." *Pharmacological Reports* 68 (5):1084–92. https://doi.org/10.1016/j.pharep.2016.06.011.

Bobade, Y., and R. M. Walli. 2015. "A Review of Wearable Health Monitoring Systems." *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* 4 (10):8386–90. https://doi.org/10.15662/IJAREEIE.2015.0410076.

Chung, A. E., R. E. Jensen, and E. M. Basch. 2016. "Leveraging Emerging Technologies and the 'Internet of Things' to Improve the Quality of Cancer Care." *Journal of Oncology Practice* 12 (10):863–66. https://doi.org/10.1200/JOP.2016.015784.

Durand, D. 1986. "Electrical Stimulation Can Inhibit Synchronized Neuronal Activity." *Brain Research* 382 (1):139–44. https://doi.org/10.1016/0006-8993(86)90121-6.

Duyn, J. H., P. van Gelderen, T.-Q. Li, J. A. de Zwart, A. P. Koretsky, and M. Fukunaga. 2007. "High-Field MRI of Brain Cortical Substructure Based on Signal Phase." *Proceedings of the National Academy of Sciences* 104 (28):11796–801. https://doi.org/10.1073/pnas.0610821104.

Fang, Z., Y. Yang, X. Chen, W. Zhang, Y. Xie, Y. Chen, Z. Liu, and W. Yuan. 2017. "Advances in Autoimmune Epilepsy Associated with Antibodies, Their Potential Pathogenic Molecular Mechanisms, and Current Recommended Immunotherapies." *Frontiers in Immunology* 8 (APR). https://doi.org/10.3389/fimmu.2017.00395.

Findlay, J. Y., B. Gali, M. T. Keegan, C. M. Burkle, and D. J. Plevak. 2006. "Vasotrac® Arterial Blood Pressure and Direct Arterial Blood Pressure Monitoring during Liver Transplantation." *Anesthesia and Analgesia* 102 (3):690–93. https://doi.org/10.1213/01.ane.0000196512.96019.e4.

French, J. A. 2007. "Refractory Epilepsy: Clinical Overview." *Epilepsia* 48 (SUPPL. 1):3–7. https://doi.org/10.1111/j.1528-1167.2007.00992.x.

Hasegawa, D. 2016. "Diagnostic Techniques to Detect the Epileptogenic Zone: Pathophysiological and Presurgical Analysis of Epilepsy in Dogs and Cats." *Veterinary Journal* 215. Elsevier Ltd:64–75. https://doi.org/10.1016/j.tvjl.2016.03.005.

Helmstaedter, C., B. Kemper, and C. E. Elger. 1996. "Neuropsychological Aspects of Frontal Lobe Epilepsy." *Neuropsychologia* 34 (5):399–406. https://doi.org/10.1016/0028-3932(95)00121-2.

Jan, M. M. 2007. "The Value of Seizure Semiology in Lateralizing and Localizing Partially Originating Seizures." *Neurosciences (Riyadh, Saudi Arabia)* 12 (3):185–90. http://www.ncbi.nlm.nih.gov/pubmed/21857567.

Jewells, V., H. W. Shin. 2014. "Review of Epilepsy—Etiology, Diagnostic Evaluation and Treatment." *International Journal of Neurorehabilitation* 1 (3):1–8. https://doi.org/10.4172/2376-0281.1000130.

Kang, S., Q. Li, Q. Chen, Y. Zhou, S. Park, G. Lee, B. Grimes et al. 2017. "CancerLocator: Non-Invasive Cancer Diagnosis and Tissue-of-Origin Prediction Using Methylation Profiles of Cell-Free DNA." *Genome Biology* 18 (1):53. https://doi.org/10.1186/s13059-017-1191-5.

Kurzbuch, K., E. Pauli, L. Gaál, F. Kerling, B. S. Kasper, H. Stefan, H. Hamer, and W. Graf. 2013. "Computerized Cognitive Testing in Epilepsy (CCTE): A New Method for Cognitive Screening." *Seizure* 22 (6):424–32. https://doi.org/10.1016/j.seizure.2012.08.011.

Lipton, R. B., F. Stewart, S. Diamond, M. L. Diamond, and M. Reed. 2001. "Prevalence and Burden of Migraine in the United States: Data from the American Migraine Study II." *Headache* 41 (7):646–57. https://doi.org/10.1046/j.1526-4610.2001.041007646.x.

Marquard, A. M., N. J. Birkbak, C. E. Thomas, F. Favero, M. Krzystanek, C. Lefebvre, C. Ferté et al. 2015. "TumorTracer: A Method to Identify the Tissue of Origin from the Somatic Mutations of a Tumor Specimen." *BMC Medical Genomics* 8 (1):58. https://doi.org/10.1186/s12920-015-0130-0.

McIntyre, C. C., M. Savasta, L. K.-L. Goff, and J. L. Vitek. 2004. "Uncovering the Mechanism(s) of Action of Deep Brain Stimulation: Activation, Inhibition, or Both." *Clinical Neurophysiology* 115 (6):1239–48. https://doi.org/10.1016/j.clinph.2003.12.024.

Stufflebeam, S. M. 2011. "Clinical Magnetoencephalography for Neurosurgery." *Neurosurgery Clinics of North America* 22 (2):153–67. https://doi.org/http://dx.doi.org/10.1016/j.nec.2010.11.006.

Menicucci, D., A. Piarulli, P. Allegrini, R. Bedini, M. Bergamasco, M. Laurino, L. Sebastiani, and A. Gemignani. 2015. "Looking for a Precursor of Spontaneous Sleep Slow Oscillations in Human Sleep: The Role of the Sigma Activity." *International Journal of Psychophysiology* 97 (2). Elsevier B.V.:99–107. https://doi.org/10.1016/j.ijpsycho.2015.05.006.

Nguyen, C., Y. Wang, and H. N. Nguyen. 2013. "Random Forest Classifier Combined with Feature Selection for Breast Cancer Diagnosis and Prognostic." *Journal of Biomedical Science and Engineering* 6 (5):551–60. https://doi.org/10.4236/jbise.2013.65070.

Orsini, A., F. Zara, and P. Striano. 2016. "Recent Advances in Epilepsy Genetics." *Neuroscience Letters*. Elsevier Ireland Ltd. https://doi.org/10.1016/j.neulet.2017.05.014.

Packer, R., M. Berendt, S. Bhatti, M. Charalambous, S. Cizinauskas, L. D. Risio, R. Farquhar et al. 2015. "Inter-Observer Agreement of Canine and Feline Paroxysmal Event Semiology and Classification by Veterinary Neurology Specialists and Non-Specialists." *BMC Veterinary Research* 11 (1):39. https://doi.org/10.1186/s12917-015-0356-2.

Rahman, A., M. T. Islam, M. J. Singh, S. Kibria, and M. Akhtaruzzaman. 2016. "Electromagnetic Performances Analysis of an Ultra-Wideband and Flexible Material Antenna in Microwave Breast Imaging: To Implement A Wearable Medical Bra." *Scientific Reports* 6 (November). Nature Publishing Group:1–11. https://doi.org/10.1038/srep38906.

Ray, P. P., D. Dash, and D. De. 2017. "A Systematic Review of Wearable Systems for Cancer Detection: Current State and Challenges." *Journal of Medical Systems* 41 (11). https://doi.org/10.1007/s10916-017-0828-y.

Silberstein, S., and S. D. Silberstein. 2004. "Migraine Pathophysiology and Its Clinical Implications." *Blackwell Science* 24:2–7. https://doi.org/10.1111/j.1468-2982.2004.00892.x.

Sledge, G. W., C. A. Hudis, S. M. Swain, P. M. Yu, J. T. Mann, R. S. Hauser, and A. S. Lichter. 2013. "ASCO's Approach to a Learning Health Care System in Oncology." *Journal of Oncology Practice / American Society of Clinical Oncology* 9 (3):145–48. https://doi.org/10.1200/JOP.2013.000957.

Sweilam, N. H., A. A. Tharwat, and N. K. Abdel Moniem. 2010. "Support Vector Machine for Diagnosis Cancer Disease: A Comparative Study." *Egyptian Informatics Journal* 11 (2): 81–92. https://doi.org/10.1016/j.eij.2010.10.005.

Teng, F., T. Cormier, A. Sauer-Budge, R. Chaudhury, V. Pera, R. Istfan, D. Chargin, S. Brookfield, N. Y. Ko, and D M. Roblyer. 2017. "Wearable Near-Infrared Optical Probe for Continuous Monitoring During Breast Cancer Neoadjuvant Chemotherapy Infusions." *Journal of Biomedical Optics* 22 (1):14001. https://doi.org/10.1117/1.JBO.22.1.014001.

Teng, X.-F., Y.-T. Zhang, C. C. Y. Poon, and P. Bonato. 2008. "Wearable Medical Systems for P-Health." *IEEE Reviews in Biomedical Engineering* 1:62–74. https://doi.org/10.1109/RBME.2008.2008248.

Thomas, G. P., and B C. Jobst. 2015. "Critical Review of the Responsive Neurostimulator System for Epilepsy." *Medical Devices: Evidence and Research* 8:405–11. https://doi.org/10.2147/MDER.S62853.

Tufenkjian, Kr., and H. O. Lüders. 2012. "Seizure Semiology: Its Value and Limitations in Localizing the Epileptogenic Zone." *Journal of Clinical Neurology (Korea)* 8 (4): 243–50. https://doi.org/10.3988/jcn.2012.8.4.243.

Vandecasteele, K., T. D. Cooman, Y. Gu, E. Cleeren, K. Claes, W. V. Paesschen, S. V. Huffel, and B. Hunyadi. 2017. "Automated Epileptic Seizure Detection Based on Wearable ECG and PPG in a Hospital Environment." *Sensors (Switzerland)* 17 (10):1–12. https://doi.org/10.3390/s17102338.

Weber, R. H., and R. Weber. 2010. "Internet of Things." *Development*, 1–8. https://doi.org/10.1007/978-3-642-11710-7.

Witt, J. A., W. Alpherts, and C. Helmstaedter. 2013. "Computerized Neuropsychological Testing in Epilepsy: Overview of Available Tools." *Seizure* 22 (6). BEA Trading Ltd:416–23. https://doi.org/10.1016/j.seizure.2013.04.004.

Yilmaz, T., R. Foster, and Y. Hao. 2010. "Detecting Vital Signs with Wearablewireless Sensors." *Sensors* 10 (12):10837–62. https://doi.org/10.3390/s101210837.

You, G., Z. Sha, and T. Jiang. 2012. "The Pathogenesis of Tumor-Related Epilepsy and Its Implications for Clinical Treatment." *Seizure* 21 (3). BEA Trading Ltd:153–59. https://doi.org/10.1016/j.seizure.2011.12.016.

Chapter 12

The Future of Wearables and the IoT in Healthcare

Movie 7: The Future of Wearables and IoT in Healthcare by Aenor Sawyer

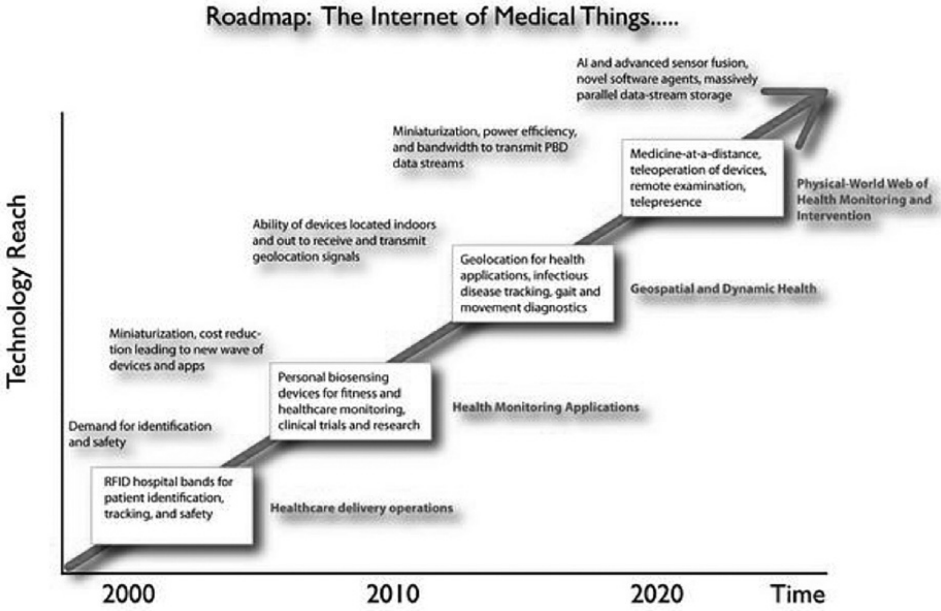
https://vimeo.com/156575723

Editor’s Note

In these pages we have championed Wearables and the IoT as headliners of Health e-Everything. But it’s impossible at this early stage to know how these technologies will unfold, or what will be there ultimate impact on the industry. And there are concerns. As the capabilities and numbers of IoT devices continue to grow, will we be over-measured and burdened by our quantified self? And can wearables truly effect behavior change across the range of healthcare issues and constituents? Will we be overwhelmed by Big Data? As the volume and complexity of wearable data grows, the technology creates challenges for service providers that are transporting the data and the firms that are collecting and analyzing that data. One the great challenges will be to curate, manage and process data, at or near real-time.

There is also an economic dimension to the growth of wearables which may bend the cost curve and usher in the personalization of healthcare. Business models based on today’s largely static information architectures will face challenges as new ways of creating value arise. When a customer’s buying preferences are sensed in real time at a specific location, dynamic pricing may increase the odds of a purchase. Wearables will likely impact our buying habits and the structure of the retail sale. From a commercial perspective, adoption of innovative wearable technology presents several challenges. The health care industry will need to find a way to successfully monetize these solutions, address consumers’ information and security concerns, recognize and respond to the fact that as mobile applications mature, they could face the scrutiny of a variety of organizations such as the Food and Drug Administration (FDA), Federal Communications Commission (FCC), Federal Trade Commission (FTC) and others.

With entrepreneurial and innovative spirit the IoT is inserting itself into healthcare in unexpected ways, and its ultimate speed and trajectory are at this point unclear. Will IoT-enabled wearables and nearables supplant traditional care delivery? Will activated health consumers alter the calculus of population health? Can the IoT truly crack the code of patient privacy and data security?


Roadmap: The Internet of Medical Things.....
Technology Reach
Time
2000
2010
2020
RFID hospital bands for patient identification, tracking, and safety
Healthcare delivery operations
Demand for identification and safety
Personal biosensing devices for fitness and healthcare monitoring, clinical trials and research
Health Monitoring Applications
Miniaturization, cost reduction leading to new wave of devices and apps
Geolocation for health applications, infectious disease tracking, gait and movement diagnostics
Geospatial and Dynamic Health
Ability of devices located indoors and out to receive and transmit geolocation signals
Medicine-at-a-distance, teleoperation of devices, remote examination, telepresence
Physical-World Web of Health Monitoring and Intervention
Miniaturization, power efficiency, and bandwidth to transmit PBD data streams
AI and advanced sensor fusion, novel software agents, massively parallel data-stream storage

What we can expect is an increasing range of innovations and interventions that leverage the convenience, efficiency, and clinical effectiveness of wearables and the IoT. This much we can predict – an infinite array of smart connected solutions designed to improve our health, environment and productivity through intelligent use of data. Whether that means empowering us to monitor and control our domestic air quality, or equipping medics with cloud-based tools that allow them to ‘consult’ with patients who aren’t even in the same room, or even the same city.

-Rick Krohn

From Wearable Sensors to Smart Implants

-J. ANDREU-PEREZ, D.R. LEFF, H.M. IP, G.Z.-. YANG

Increasing health costs and incidence of chronic diseases such as cardiovascular and cancer, senescence-related dependence and sedentary lifestyles (e.g. obesity) are major healthcare challenges. The future of healthcare delivery depends on new technological advances with emphasis on prevention, early detection and minimally invasive management of diseases. Wearable devices are common nowadays for monitoring physiological indices such as ECG, heart rate, blood pressure, blood oxygen saturation (SpO2), body temperature, posture and physical activities. This single sensing modality is defined here as "first generation" monitoring devices. Better networking capabilities of these sensors have made smart context-aware monitoring possible by fusing the information obtained from these sensors with others embedded in the environment. These developments in sensors' electronics and embodiment have given rise to a new, "second generation" of sensing technologies featured with continuous monitoring. This continuous monitoring can be essential to capture critical events such as myocardial infraction, arrhythmias and strokes.

Advances in sensor technologies have been driven by innovation in low-powered micro-electronics, micro/nano fabrication and miniaturization. These developments have been accompanied by improved bio-compatibility of materials thereby minimizing foreign body reactions and facilitating smart implantable devices and prostheses. Implantable sensors have propelled the number of benefits that sensing provides to patients. For example, a fully non-invasive blood test glucose can be implemented as a smart implant,which may sense blood glucose levels or signs of neutropenia without the need for performing a capillary test.

An important consideration is the enormous volume of data collected by continuous sensing. Extensive sensor deployments over a patient population, produce a new source of Big Data which underpins the creation of health Biobanks of longitudinal plus high frequency pervasive data.

This new informational source can be connected, processed and examined in the cloud in combination with other Big Data sources (patient health records, - omics data etc.). A timeline of technological platforms that have triggered this technological evolution is presented in Figure 1.

In the last decade, the field has evolved through progressive advancement in sensing and intelligence for pervasive health applications. More recent advances have focused on wearable/implantable devices equipped with continuous multimodal sensing capabilities, and support for data fusion deployed in a wide range of clinical applications. Advances in sensing hardware can be attributed to parallel developments in sensor embodiment technology, micro-electronics and fabrication processes, and the availability of wireless power delivery leading towards miniaturized implantable sensors.

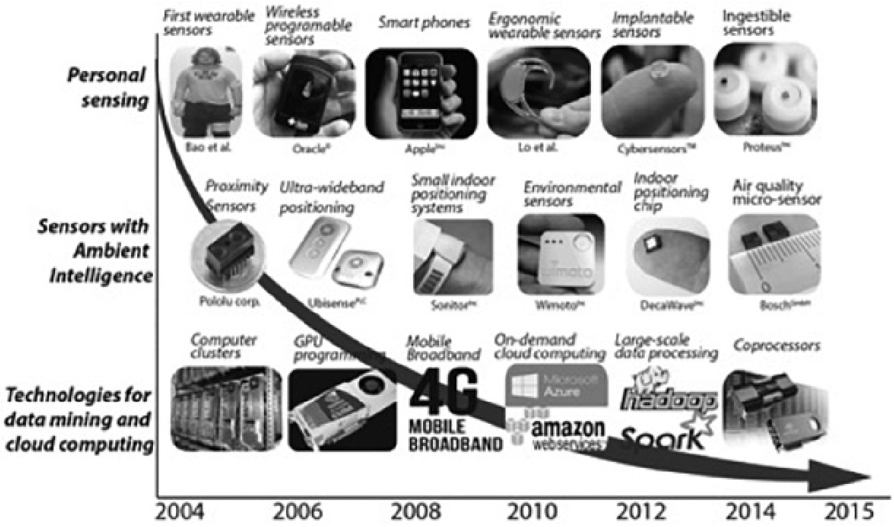


Fig. 1 Evolution of the allied technologies for pervasive healthcare in recent years.

From a clinical perspective, the evolution of each generation of pervasive health has been enabled by a sequence of technological steps towards integrated care, bridging the gap between health and disease management. From a technical standpoint, there is still a need for horizontal advances within each generation with the finality of improving device quality. However, vertical developments may bring an entirely new generation of low-powered wearable sensing devices and smart implants that are low drift, resistant to biofouling, and can be effortlessly implanted and extracted when no longer necessary.

Unique challenges towards personalized healthcare include long-term continuous sensing, intelligent interpretation and timely intervention, which in turn presents a myriad of opportunities for sensor informatics. Future research will also need to focus on integrating large data sets from heterogeneous sources including pervasive health data. If overcome, these technical challenges are set to transform our understanding of healthcare delivery. Big data mining and social network analysis provide new ways of managing global epidemics such as Ebola, accelerate warning systems, incorporating geographic location systems to track cases and systematize outbreak response. All of this can be translated into a new era for medicine, moving from a reactive to a proactive discipline.

References

1. J. Andreu-Perez, D.R. Leff, H.M. Ip, G.Z-. Yang, "From Wearable Sensors to Smart Implants – Towards Pervasive and Personalised Healthcare", IEEE Transactions in Biomedical Engineering, [In press], 2015.
2. G.Z-. Yang, "Body Sensor Networks", 2nd ed., Springer, Germany, 2014. For the full version of this article, please see: J. Andreu-Perez, D.R. Leff, H.M. Ip, G.Z-. Yang, "From Wearable Sensors to Smart Implants – Towards Pervasive and Personalised Healthcare", IEEE Transactions in Biomedical Engineering, 2015.

Connecting Implantable Devices - The Next Iteration of Wearables?

-ALISA NIKSCH

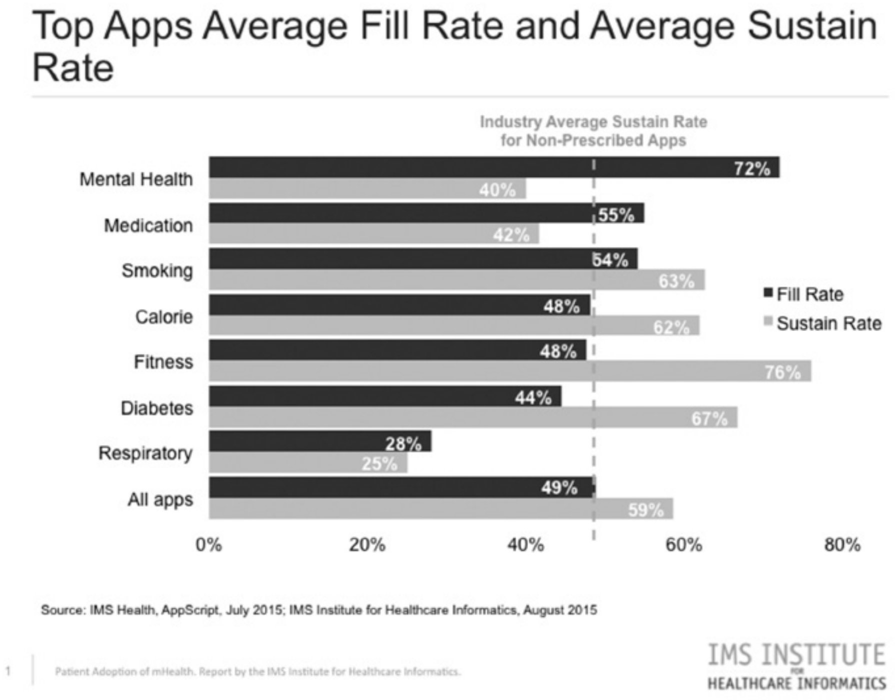
Wearable technology has highlighted the potential for medical devices to be both connected and personal. Patient generated data now plays a role in transforming disease management. However, the market has shown mixed signals for the long term adherence and success of fitness wearables. Despite a Pew research survey showing that 62% of individuals with 2 or more chronic conditions will track symptoms, a high rate of attrition in usage of fitness wearables has become a significant concern for the advancement of this model for remote patient monitoring. (http://www.pewinternet.org/files/old-media//Files/Reports/ 2013/PIP_TrackingforHealth%20with%20appendix.pdf)

Wearable devices focused on medical needs, on connecting patients to clinicians and caregiver support to optimize management strategies, are just being explored. Needs for continuous data trending and optimal compliance from the user has prompted further exploration on the form and function of wearables, including making them a permanent or semi-permanent implanted device.

Why Implantables?

Implantables are probably the extreme iteration of what we know as wearable technology today. Implantables have the potential to extract a continuous stream of data without any action required on the part of the user. As voiced by David Lee Scher, MD, Associate Professor of Medicine at Penn State College of Medicine and Director, DLS Healthcare Consulting, “The advantage of implantables addresses a fundamental desire of the user for convenience, and provides multiple accurate, real time data points for providers.”

Platforms utilizing the power of smartphones, cloud-based data storage, and machine learning can enable earlier detection of clinical changes in patients battling chronic disease states. With digitally connected implantable devices, the challenge of active compliance is obviated, and there is no requirement to incorporate a reward-for-behavior change feedback loop into a mostly passive system. However, there is debate whether taking away a feedback loop with passive data feeds erodes patient engagement in other ways. In addition to the Pew Research data from 2013, there is evidence from research done through IMS Health (IIHI_ Patient_Adoption_of_mHealth.pdf) that having a physician involved in the prescription and follow up of a mobile health tool can vastly improve retention above and beyond industry averages (Figure 1). However, there clearly remains significant uncertainty whether digital health platforms, including wearables, will have the long term stickiness needed to effect better health behaviors.



Top Apps Average Fill Rate and Average Sustain Rate

Source: IMS Health, AppScript, July 2015; IMS Institute for Healthcare Informatics, August 2015

It goes without saying that implantation of a device into a human subject for biometric tracking would imply a compelling medical indication. Implantable medical devices which deliver therapy in response to sensory data have a rich history and well established precedents, most of which have not leveraged IoT-based transmission of health data. For instance, the cochlear implant was the model of neuromodulation in its earliest implanted form. Neuromodulation has expanded its use to include chronic pain management, migraine therapy, GI motility and bladder neurostimulation. Implantables are under investigation for other clinical challenges such as diabetes control, Parkinson's Disease symptom control (http://www.ninds.nih.gov/disorders/deep_brain_stimulation/deep_brain_stimulation.htm), and elevations in intracranial pressure after traumatic brain injury. Medtronic formed a partnership with Samsung in 2015 to integrate digital health solutions into their insulin pumps and expanding to their battery of neuromodulation devices (http://www.fiercemedicaldevices.com/story/medtronic-samsungpartner-develop-neuromodulation-implants-apps-smart-devic/2015-12-11). DARPA has even invested in this space, recently receiving $78.9 million to develop a microimplant series called "ElectRx" for neuromodulation of biological functions (http://www.extremetech.com/extreme/188908-darpas-tiny-implantswill-hook-directly-into-your-nervous-system-treat-diseasesand-depression-without-medication).

Implantable devices with diagnostic and therapeutic capabilities have matured in certain fields like cardiology and neurology more rapidly than others. Areas such as orthopedics, with vast numbers of joint replacement procedures annually, are ripe for leveraging available biosensors to maximize the value of the implant to the recipient. With over 7 million Americans living with a hip or knee replacement (http://www.ncbi.nlm.nih.gov/pubmed/26333733), the prospect for making these devices digitally active is incredibly enticing.

History Of Implantable Technology For Remote Patient Monitoring

The most relevant discussion of the history of remote patient monitoring through implantable technology centers on the remote monitoring systems connected to implantable cardiac devices, including pacemakers and cardiac defibrillators. These systems, now adopted around 15 years ago by all four major cardiac device manufacturers, have produced significant changes in healthcare utilization within their patient populations. Using manufacturer specific mobile units, active or passive transmission of detailed device data can occur (Crossely GH, et al. Clinical benefits of remote versus transtelephonic monitoring of implanted pacemakers. J Am Coll Cardiol 2009; 54:2012–9). Confirming earlier studies, in 2010 the CONNECT (Clinical Evaluation of Remote Notification to Reduce Time to Clinical Decision, J Am Coll Cardiol 2011;57:1181–9) trial demonstrated that wireless remote monitoring allowed clinicians to make treatment decisions 17.4 days sooner than with in-office visits alone. There was also a statistically significant decrease in mean length of stay for cardiac related diagnoses from 4 days in the in-office group to 3.3 days in the remote monitoring group. Also in 2010, the ALTITUDE Trial was published, examining the survival rates for wirelessly connected patients with implanted devices vs. those only seen in a clinician office. For the 69,556 implantable defibrillator (ICD) patients receiving remote follow up on the network, 1 and 5 year survival rates were higher compared with those in the 116,222 patients who received device follow-up in clinics only (Saxon LA, et al. Long-term outcome after ICD and CRT implantation and influence of remote device follow-up: the ALTITUDE survival study. Circulation 2010;122:2359–67). Potentially the most important factor to physicians, in 2006 the Centers for Medicare and Medicaid Services (CMS) approved structured billing codes for these procedures, incentivizing broader adoption of wireless remote monitoring (Kalahasty G, et al. A brief history of remote cardiac monitoring. Card Electrophysiol Clin. Sept 2013; 5 (3): 275-282).

This prototypical model of remote monitoring associated with implantable device systems has vast implications for developers of other mobile health technologies, as examples of digital recording, storage, transmission, and data analysis. Simply the burden of the number of study subjects involved in validating the wirelessly connected model should give pause to developers of digital platforms. However, passive data acquisition, with evolution of continuous wireless data transmission from device to database, mitigates much of the compliance issue. Automation of alerts built around preprogrammed algorithms rounded out this system to improve provider response to patient needs. Perhaps most importantly, all of this concluded with a reimbursement strategy. What has been lacking, however, is patient access to data from implantable cardiac devices. This has been contested by patient advocates such has Hugo Campos, who recently shared his story with Slate.com (http://www.slate.com/articles/

technology/future_tense/2015/03/patients_should_be_allowed_to_access_data_generated_by_implanted_devices.html). Future implantable devices, while drawing on the precedent of cardiac devices, likely have consumer pressure to connect the user to data obtained by the device. However, the path towards this conclusion will require some intelligent and discerning steps geared towards the interests of several invested parties.

Device and Accessory Regulation

Regulation of medical devices, especially when implanted in a human subject, is a complex process which has been fully elaborated in texts outside of this one. However, wirelessly connected implantable devices have only been recently explored by the FDA in a systematic way. The FDA has approved wireless services associated with medical devices in the past, mostly developed by large manufacturers such as Medtronic (http://www.medscape.com/viewarticle/783361; http://www.diabetesincontrol.com/new-product-medtronicscarelink-pro-30/). However, the universe of IoT connectivity and mobile device has expanded much more quickly than regulatory agencies have had to evaluate their safety. Finally, in January 2015, FDA issued draft guidance that would permit device accessories (including linked software platforms) to be classified at a lower risk than their associated hardware devices. Accessories are defined in two categories: (i) one in which the article is labeled and branded to indicate use with the parent medical device; or, (ii) the article is intended for support, supplement, or augment the function of a parent medical device. (http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ ucm429672.pdf)

In the universe of digital health, the development of software platforms associated with wearable devices meant for diagnostic purposes or which provide treatment algorithms would mostly fall into the first category. It is acknowledged by the FDA that the risk profile of the device accessory may have a very different risk profile, and would undergo a different pathway for review. It can be expected that the targeted patient population, and the complexity of the data analysis and automation will influence the requirements for regulatory process. As is increasingly recognized, proving validity of a connected device platform will require demonstration of selected outcomes in real-world user cohorts. Without these, certain functionalities of the software may be restricted for clinical use. Deborah Kilpatrick, PhD, CEO of Evidation Health, anticipates this development.

She states, “We use linked medical, behavioral and contextual datasets to define "digitally-enabled" health outcomes in a patient population. That approach theoretically holds for any connected device. One the other hand, it could depend on how the connected, behavioral data feed is used. If its source is a clinical-grade wearable being used by a physician to manage care, there could be differentiating regulatory drivers of how such data feeds would be handled to measure patient benefit.”

As a final point, it is important to mention that the FDA has not made demonstration of data security a prerequisite for digital health IT platforms; it has up to this point laid the responsibility for implementing security measures for a medical device on the manufacturer itself. One may argue that given the growing impact of IoT in medical device and wearable platforms, a greater oversight of this aspect of product development may emerge in the near future.

Security Issues

“The biggest vulnerability was the perception of IT health care professionals’ beliefs that their current perimeter defenses and compliance strategies were working when clearly the data state otherwise.”

FBI Advisory, April 8th, 2014—PIN# 140408-009

The security of connected implantable devices is a potentially devastating concern (Blake, A. Medical devices too prone to hackers, researchers say. Washington Times, August 6, 2015).

While most of the hardware and software pairings may not contain security flaws leading to adverse health effects on the user, there are often links to protected health information (PHI) which can be lucrative to the opportunistic hacker. Neither the FDA nor HIPAA policy focuses on IT security. Names, dates of birth, home or email addresses and even social security numbers can be extracted from hacked medical records. It has been reported that private medical information is 10 times more valuable than a credit card number (http://www.reuters.com/article/us-cybersecu-rityhospitals-idUSKCN0HJ21I20140924), the temptation to sell private information found in health records is real and is growing.

When former U.S. Vice President Dick Cheney had the battery of his implantable cardiac defibrillator replaced in 2007, physicians made the decision to disable the wireless capabilities of his device because of of his device because of plausible security threats (http://www.cnn.com/2013/10/20/us/dick-cheney-guptainterview/). The possibility of a terrorist breach of implantable cardiac devices was then resurrected in a 2014 episode of the Showtime series Homeland (https://www.newscientist.com/article/mg22429942-600-murder-by-hackable-implants-nolonger-a-perfect-crime/). According to medical device and healthcare security experts Scott Erven and Shawn Merdinger speaking at DefCon, the world's largest hacking conference in August 2014, the digitalization of medical devices has exposed hospitals and patients to increasing rates of security breaches and interference with medical device function. Using open source reconnaissance tools, the pair was able to gain swift access to over 100 credentials used to manipulate the function of common medical devices manufactured at GE Healthcare and Phillips, just to name a few. They disclosed their successful breaches to ICS-CERT, a unit operating under the U.S. Homeland Security Department to coordinate government, law enforcement, and industry entities to mitigate cyber security emergencies. While many of these breaches did not directly endanger patient well-being, the impact on future risk assessment of any digitally connected implantable medical device was not lost on these experts.

Security breaches in the software component of medical devices may be due to fixed manufacturer-created passwords, patient data transmitted across improperly secured networks, and software security flaws which are replicated faster than they can be repaired (https://ics-cert.uscert. gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf). Many security vulnerabilities are notoriously found in the linkage of new health IT software to legacy systems within medical centers and other healthcare enterprises. While hackers looking at connected implantables may only have the intention of pilfering demographic information for a quick payoff, the potential is clearly there for more nefarious activity.

The Design Challenge

The design cycle for implantable medical devices has proven to be a lengthy and challenging one. Hardware design protocols have focused on absolute size, battery life, incorporation of wireless capabilities, and reduction in risk of the implant process. However, the addition of wireless connectivity and the IoT revolution have created another design challenge—one that puts the patient in the center of the healthcare data matrix. Software platforms which communicate with implanted hardware will be increasingly operated by the patient. What is seen, what response is provoked, and how the system finds value in a person's lifestyle are items which cannot be assumed by digital health companies.

Enter a new outlook from design experts now exploring the ecosystem surrounding digital health technologies. Karten Design, a product design consultancy in Marina Del Rey, CA, has taken the plunge to make connected implantable devices seamless for patients and clinicians, and ultimately successful for manufacturers. Stuart Karten, Principal at Karten Design, has made it the company's priority to support patient experience and address the needs of in-home caregivers, a group he feels is an underserved population within healthcare. "Our goal is to make the product blend invisibly with the lifestyle patients have. We want to transform data into information—information implies a value to the user", Karten explains.

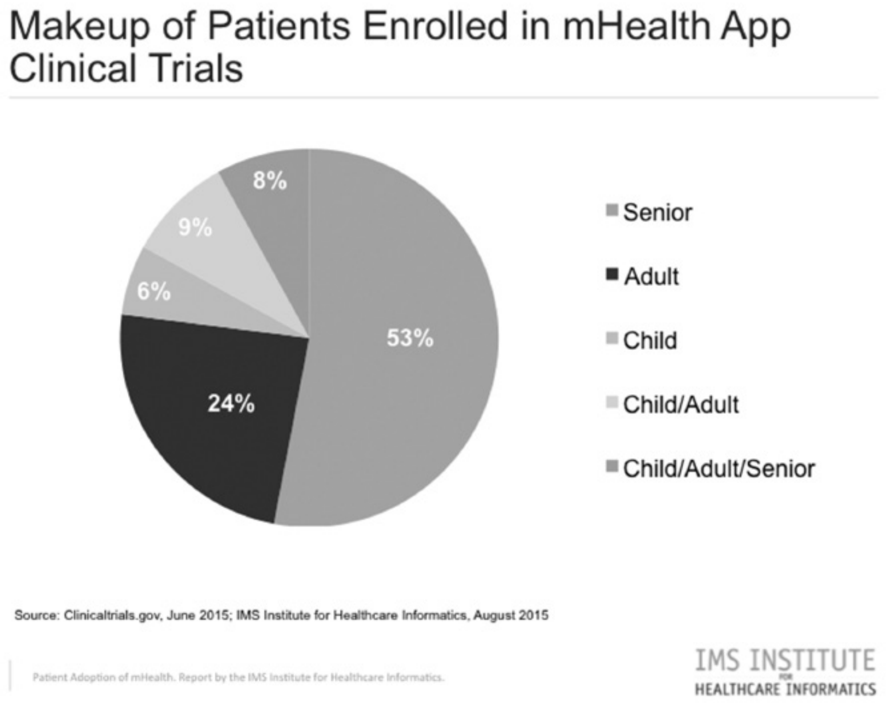
Companies like Endotronix, which has developed an implantable sensor to track pulmonary artery pressure as a marker for congestive heart failure management, have leveraged this kind of expertise to develop their digital platforms. In the case of Endotronix, a portable handheld reader and a streamlined user interface was developed to make acquisition and utilization of patient generated data easy and effective.

Design of the interface with connected implantable devices is an enormous key to adoption. Patients must find these platforms simple and convenient to operate. The design of the hardware and software needs to account for the lifestyle and limitations of the likely end user demographic. Even though most noninvasive wearable technologies are marketed towards consumers in their 20's and 30's, 53% of study subjects involved in research of mHealth tools were seniors (Figure 2). The time and effort required for remote monitoring, data review and communication on the part of the patient must outweigh time and effort for traditional calls and visits with caregivers and clinicians. The data presented must be valuable and unobscured by extraneous features to both patient and clinician, essential to usability. As Karten expressed, "The biggest false assumption is that physicians will be looking at this information all the time—there is a lack of understanding of where this technology fits into a clinical workflow." Finally, while implantable devices partly remove the need for a patient feedback loop for participation in health management, an effective digital interface can further engage patients in their treatment plan. In the future, if digital health devices evolve in a more implantable direction, smart design will make these tools not just an optional accessory, but an integral part of the user's health, even part of their identity.

The Road to Commercialization

Commercialization of implantable devices as an extension of the wearables market must address all of these rapidly evolving topics. In addition to this, how a wearable digital health product achieves adoption by multiple parties in the healthcare ecosystem must be seen strategically and thoughtfully. While wearable technology has been made feasible by the incredible advancement of biosensors and wireless communication, a successful product cannot thrive on the sophistication of the tech alone.

Virtually no one disagrees that the patient is the focal point in the development of a diagnostic or therapeutic device. Even more consideration for safety and risk is deserved when the device is invasive. The invasive nature of any device requires that both patient and physician must be persuaded that the implantation of the device garners more benefit than risk to the patient. As physicians are inextricably linked to the process of implantation, as well as the fallout from any complications, they will naturally voice the most skepticism toward these technologies. Questions will arise as to what training and quality assurance is needed for clinicians to safely implant and manage a device.


Makeup of Patients Enrolled in mHealth App Clinical Trials

Source: Clinicaltrials.gov, June 2015; IMS Institute for Healthcare Informatics, August 2015

2 | Patient Adoption of mHealth. Report by the IMS Institute for Healthcare Informatics.

Clinical trials using wearable technology, with questions directed at what benefit is gained from an implantable model, will need to be conducted with likely significant investment of time and finances. It is worth reiterating that the ALTITUDE implantable defibrillator trial, conducted simply to demonstrate the benefit of wireless data transmission, enrolled 185,778 subjects to support the final outcome. The scale of what may be needed to support manufacturer claims should not be underestimated.

The value of the digital platforms connected to these devices will also be a challenge for some physicians to accept. Physicians are already overwhelmed with data from EHRs and various other databases, and don't feel that more data equals useful data (http://www.npr.org/sections/health-shots/2015/01/19/377486437/sure-you-can-track-your-health-databut-can-your-doctor-use-it). Data as presented to medical personnel has made a poor first impression. The power of data for examining population health and providing preemptive treatment based on clinical markers has not diffused extensively into the wider medical community. Dr.Joseph Kvedar, Vice President of Connected Health, Partners Healthcare and Associate Professor at Harvard Medical School, agrees that physicians will be the most difficult to win over. But this is not always the fault of the developers. While data supporting the use of a connected device or software platform is important, Kvedar states, "Sometimes physicians don't think creatively, and resist the insights that data analytics could provide." This being said, the ability to sell to physicians and medical enterprises will often require an appeal to the hardware's ability to intervene and the software's capability of averting the intervention through intelligent data interpretation.

Device development often has a prolonged cycle, whether from an investigational or regulatory standpoint. With the complexities involved in an implanted medical device, the resources needed to conduct adequate studies on the technology and design concept, as well as the capital needed for the regulatory process, often weeds out the smaller scale entrepreneur. There are certainly notable exceptions which have thus far overcome these obstacles, notably Endotronix (heart failure management), Axonics, Inc. (neuromodulation for urinary incontinence), Dexcom, Inc. (connected continuous glucose monitor for diabetes) and the Pulsante SPG Microstimulator (migraine and cluster headaches). However, the larger device companies (e.g., Medtronic, St. Jude Medical, Boston Scientific) continue to dominate the cardiovascular, neuromodulation, and diabetes implant market, with progressive adoption of wireless connectivity and mobile health tools to improve convenience and accessibility of data for patients and clinicians. They have also been able to successfully lobby the Center for Medicare and Medicaid Services (CMS) for new procedure codes to gain reimbursement, a big obstacle in the commercialization of digital health tools. The chronic care management reimbursement code allowing for remote encounters implemented in January 2015 has also been an encouraging measure. There are still, however, large gaps in payment for even the most standard device monitoring, both in the U.S. and Europe (http://europace.oxfordjournals.org/content/17/5/814).

This being said, there is a question whether creating a de novo implantable product is always the best pathway to creating disruption in the wearable market. It already has been mentioned that the orthopedic surgery field would be a growth market for biosensors. Already, small populations have been studied with gyroscopes and accelerometers for gait analysis and assessment of recovery after knee replacement in the UK (Kwasnicki, RM, et al. Int J Surg. 2015 Jun; 18: 14-20). The potential to scale these technologies in existing implanted devices is certainly worth exploring, and may be a wise next step in mitigating risk.

The Future of Implantables

The technology at the foundation of wearable health devices has been a source of hope for transforming the way we manage the most challenging and costly medical conditions people experience. The union of medical devices, digital connectivity, and IoT access can provide more value, more directly, to people suffering from chronic disease. Implantable devices have gravitated initially towards the cardiovascular and neuromodulation spaces, with some more recent advances in diabetes management. With increasing investigation into the benefits of digital connectivity of such devices, findings of decreased rates of hospitalization, decreased time to clinical interventions, and increased patient satisfaction are supporting further deployment of wirelessly enabled devices.

There continue to be obstacles to building, developing, researching, securing and selling the value of new connected implantable devices. The invasiveness issue is certainly the elephant in the room when it comes to discussing these technologies, especially if similar or equivalent data can be acquired using less invasive (and cheaper) methods. Another alternative is to examine existing devices which could be fit with specific biosensor technology, which is a strategy supported by Dr. Joseph Kvedar, "Sensors are getting better and more versatile...I would support more of an augmented version of devices which would already be implanted in patients."

The future of connected implantable device technology is complex. Implanted devices naturally lend themselves to certain medical specialties, and the extraction of granular, real time data using digital connectivity increases their value proposition. Other tracking of clinical data may not justify an implant due to a risk-benefit imbalance. However, the potential of digital technology and smart data analytics to provide better health outcomes and contain costs is impressive, and is being demonstrated in health care systems every day. As stated by Deborah Kilpatrick, "I do believe it is a question of "when", not "if", when it comes to new, digitallyenabled outcomes---and they will impact our understanding of how therapeutic devices work in the real world."

Chapter 13

Internet of Things (IoT) Deployment in Wearable Healthcare: A Sociotechno Evaluation

Gaurav Mishra
Development Management Institute (DMI)

Balakrishnan Unny
Institute of Management, Nirma University (IMNU)

Nityesh Bhatt
Institute of Management, Nirma University (IMNU)

13.1 The Internet of Things: Result of Digital Convergence

Digital convergence results in the integration of different components of computer technology and telecommunications technology into a single entity, i.e., information technology (IT) (Ogunsola 2005). Smartphone is the best example to elucidate the concept of convergence. Smartphones enable interactive voice and text communication in addition to synchronous and asynchronous multimedia communication capabilities. According to Mueller (1999), digital convergence happens when different forms of media are incorporated into one technology. For example, digital computer has integrated circuits, audio–video components, and uses different information theory models for functioning.

Technology improvements like enhanced data transmission and devices that have efficient computing capacity and improved data storage are important for technology convergence (Tiwari et al. 2006). In addition to these factors, Tufano and Karras (2005) included interactivity, self-configuration, and customization as significant factors for convergence. According to them, due to the increased processing capability of devices, users are becoming more comfortable in self-configuring applications. Users can configure various aspects, for example, they can add/remove/set alert for events on calendar, set notifications for content, and customize the user interface with respect to its look, feel, and layout of applications on their devices. Adoption of standards for data transmission is also seen as a precursor for convergence. According to Mueller (1999), the development of common protocols and technical standards is a result of synchronized acceptance of well-matched technology platforms by different stakeholders.

According to Finger (2010), convergence of technologies is the major contributor to the exponential growth of Information and Communication Technologies (ICTs) in different parts of the world. With the proliferation of such converged devices, the result is a completely new media ecology (Mueller 1999). The benefits of technological convergence are observed in domains from agriculture to health and business to infrastructure. For example, M-commerce is seen as coming together of IT and telecommunication technologies (Tiwari et al. 2006). The convergence of sensor and network technologies provide us the ability to measure, infer, understand, and communicate various critical indicators on a real-time basis. Technologies such as wireless sensor networks (WSNs), cloud platform, communication standards and protocols, radio frequency identification (RFID), etc. serve as the building blocks of this ecology (Roman et al. 2013).

Hence, we see that convergence of technologies support the development of a new ecosystem, and this chapter deliberates on how the convergence of technology has helped in the evolution of the Internet of Things (IoT). In addition, importance is laid on how the IoTs are applied in the health-care domain. It is well accepted that the IoT offers enormous benefits to various stakeholders. One of its applications can be remote monitoring of patients' health through healthcare wearable devices. Hence, a thorough understanding of the current trends in this segment is desirable for everyone interested in IoT deployment. However, the IoT remains in its introduction stage of product life cycle in the health-care field, especially in a developing country like India. Given the amount and sensitivity of health-related data, questions of security and privacy need utmost attention as these are being exchanged with other devices, people, and organizations. IoT deployment in healthcare raises numerous challenges such as identity management, interoperability, authentication, authorization, and management of several wearable connected devices. The chapter aims to elucidate various sociotechnical challenges of IoT deployment in health-care domain followed by possible solutions.

13.2 Internet of Things

With convergence of WSN technologies, open wireless technologies like Bluetooth, RFID, wireless fidelity (WiFi), telecommunication network, digital electronics, etc.; embedded devices are now able to exchange data with each other. This exchange of information among the various embedded computing devices is termed as IoT (Borgohain et al. 2015). The concept of "Things" in the IoT is generally used to reflect ordinary objects like televisions, watches, air conditioners, etc. The IoT results into an immensely distributed network of devices that communicate with people as well as other devices (Xia et al. 2012). They provide the benefit of creating a communication channel with all the entities in the network, supporting access to services ubiquitously. According to Ma (2011), the IoT has the following important characteristics:

1. Day-to-day "things" such as books, chairs, mobile phones, and foods can be instrumented (i.e., chip, RFID tags can be embedded, etc.).
2. Instrumented objects are connected as autonomic network terminals.
3. Autonomic terminals communicate with each other to make the pervasive service intelligent. As an example, the sensor nodes present on healthcare wearable devices can provide information related to the status of human body and provide reliable and real-time information to individuals, doctors, etc.

Realization of the IoT benefits is possible if ICTs integrate seamlessly with the real world of things. Through ICT usage in the "anytime" and "anywhere" mode, real world becomes more accessible in various domains as well as everyday scenarios (Uckelmann et al. 2011). However, integration of technologies shown in Figure 13.1 is crucial to materialize the advantages of IoT.

Some of the important or crucial technologies discussed in literature are as follows:

a. RFID: This technology is being used in many areas like retail, logistics, anti-counterfeiting, healthcare, and supply chain management. In simple terms, RFID works like barcode technology; however, it does not require a direct visibility of the monitored entities. RFID requires an interrogator, backend

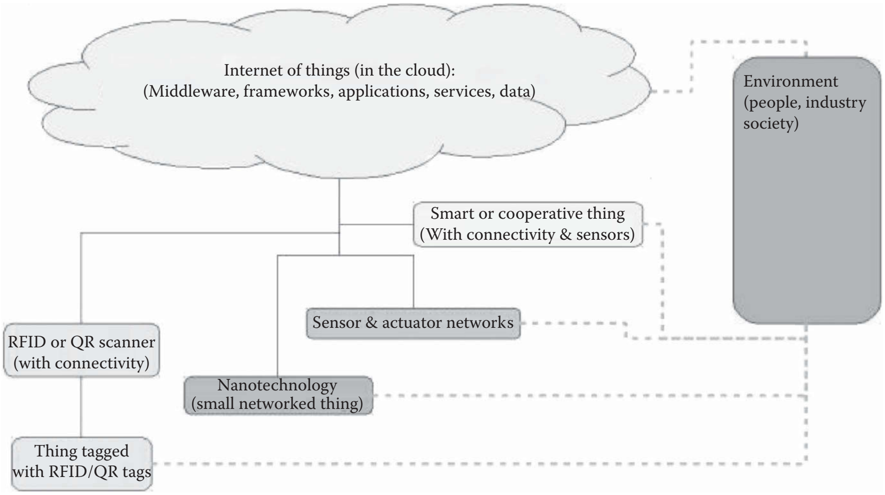

Internet of things (in the cloud):
(Middleware, frameworks, applications, services, data)
Environment
(people, industry
society)
Smart or cooperative thing
(With connectivity & sensors)
Sensor & actuator networks
RFID or QR scanner
(with connectivity)
Nanotechnology
(small networked thing)
Thing tagged
with RFID/QR tags

Figure 13.1 Components of IoT ecosystem (Coetzee et al. 2011).

system, and special tags for an entity tracking. Tags contain information about the item/asset. Interrogator communicates with the RFID tags, and backend system connects the interrogator with the centralized database. This technology has been there since long, but recently this technology has seen immense potential in the IoT due to its lower cost and increased capabilities (Sun 2012).

b. WSNs: It is a network of tiny low-cost devices equipped with sensors with a capability of taking measurements, storing locally, and communicating with each other (Bellavista et al. 2013). The most important advantage of WSN is that it makes interconnections quite easy and simple when compared with designing and implementing of wired connections. Ease of installation of WSNs reduces the cost and efforts for a large number of sensors (Ghayvat et al. 2015). WSNs find use in healthcare, where a number of discrete sensors provide different health parameters of individuals.
c. WiFi: In WiFi technology, the wireless network has an access point. This access point is the hub that provides connections to electronic devices, such as computers or mobiles phones, wirelessly. Most of us have used a WiFi network at home, company, institution, university, and many other places for the Internet services. Latest advances in WiFi technology have provided opportunities for a larger area coverage and has helped to extend the technology use in consumer electronic applications like video calling, streaming of videos and music, playing of games, exchange of data, etc. (Kaushik 2012). In addition, the cost and dimensions of WiFi chips have significantly decreased compared with their predecessors. WiFi may provide the communication fabric for the IoT applications and provide location-based services (Acer et al. 2015).
d. IoT Gateway: Due to lack of standard communication protocols, it is not easy to network the WSNs and mobile communication networks or the Internet with each other. Also, transmission of data from WSN to long distance is not possible due to the constraints posed by WSN's transmission protocols. To address this challenge, the IoT gateway is invented, which attempts to tackle the discreteness between WSNs, telecommunication networks, or the Internet and the diversity of protocols. It helps to bridge the available customary networks with sensor networks for better network communication. The IoT gateway helps in protocol conversion and device management (Zhu et al. 2010).

13.3 Applications of Internet of Things

IHS Markit forecasts that there will be 20 billion IoT devices in 2017. It is estimated that such devices will be 75.4 billion in 2025.* McKinsey estimates that the

* Information retrieved from www.ihs.com/industry/telecommunications.html, accessed on 2/10/2017.

total IoT market size will be USD 3.7 billion by 2020.* Gartner reports that the consumer segment is the major user of IoT with 5.2 billion units in 2017. It consists of approximately 63% of the total number of units in use.† Business Insider estimates that by 2019, the market of the IoT devices will be larger than that of the size of the mobile phones, computers, connected vehicles, and the combined wearable devices market.‡ McKinsey estimates that the total economic impact of the IoT will be greater in developed countries than in developing countries because of greater cost savings and better adoption rates§ (Please refer to Table 13.1).

Literature varied the applications of IoT in diverse domains. Figure 13.2 shows the heat map of key prospects of the IoT in different industries. Here, hotter shows the highest potential of IoT deployment. It can be reflected that health-care sector with "warm" category is still in the nascent stage of IoT usage.

Table 13.1 An Estimated Share of Economic Impacts of IoT, 2025

Settings	*Advanced Economies (%)*	*Developing Economies (%)*
Humans (wearable segment)	89	11
Homes	77	23
Offices	75	25
Retail environments	71	29
Vehicles	63	37
Cities	62	38
Factories	57	43
Others	56	44
Work sites	54	46
Overall estimates	62	38

* Refer to the report available on http://hk-iot-conference.gs1hk.org/2016/pdf/_04_Mc%20Kinsey%20-%20(Chris%20Ip%20)%20ppt%20part%20%201%20_IoT%20-%20Capturing%20the%20Opportunity%20vF%20-%2021%20June%202016.1pptx.pdf, accessed on 29/10/2017.

† Information retrieved from www.gartner.com/newsroom/id/3598917, accessed on 29/10/2017.

‡ Information retrieved from www.businessinsider.in/The-Internet-of-Things-Will-Be-The-Worlds-Most-Massive-Device-Market-And-Save-Companies-Billions-Of-Dollars/articleshow/44766662.cms, accessed on 29/10/2017.

§ Source: www.mckinsey.com/business-functions/digital-mckinsey/our-insights/an-executives-guide-to-the-internet-of-things, accessed on 29/10/2017.

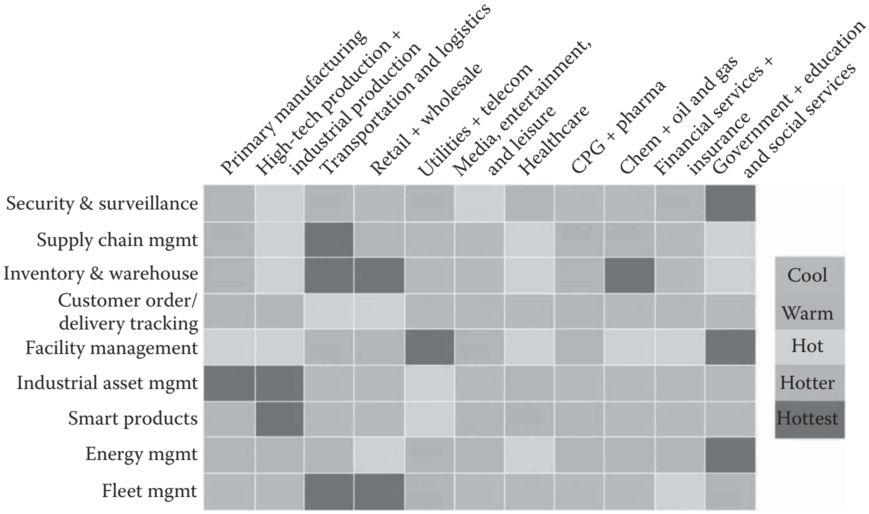


Figure 13.2 Heat map of the key IoT prospects in different domains (Pelino and Gillet 2016).

With the advancement and decrease in the cost of IoT technology, the possibility of including more and more objects into the IoT ecosystem is increasing. Through the IoT, it is possible to interconnect number of objects/entities, storing real-time data, and analyzing it for decision-making. Below are few examples where the IoT has been used successfully:

13.3.1 IoT in Business

Any business wants to have competitive advantage to survive in the competitive and dynamic market. The IoT can play a significant role in providing necessary and relevant data to businesses for better decision-making. As rightly pointed by Lee and Lee (2015), adoption of the IoT is rapidly gaining momentum in industry as technological, societal, and competitive pressures are driving them to innovate and transform. Real-time data and its processing have immense applications in manufacturing organizations, where the overall status of the machineries can be easily monitored using IoT. Through IoT, predictive maintenance is possible. Management will be in position to decide on replacement, repair, and preemptively follow maintenance of machineries before any major breakdown occurs. Companies can know the status of oil, brakes, engine, etc. along with the location of the fleet of vehicles used in logistics. As an example, in 2012, JCB India started using the IoT so that its customers are in constant touch with their machine by sending out real-time data and keeping them informed all the time. Through the system, in operations, users were able to collect important parameters for monitoring equipment usage, fuel consumption, status and health, and idle time. The system helped the organization in implementing product-as-a-service business models with no revenue leakage (Ramchandran 2015). In addition, information sharing and collaboration become efficient through the IoT. For example, managers can assign tasks to employees via an IoT-enabled mobile device. Insurance companies can set premium on car insurance based on the data on the driving behavior of the driver received through IoT-enabled devices in cars. Companies may use the location data of the customers to provide specialized services, such as alerting about the nearest retail store available to him/her.

13.3.2 IoT in Environment Monitoring

The IoT has been used widely for pollution monitoring, chemical hazard, earthquake and flood detection, weather forecasting, and precision agriculture. For example, Dubai Municipality, since 2012, uses a 14-station network comprising of air quality monitoring (AQM) stations to report and manage real-time data on air pollutants such as sulfur dioxide (from factories), carbon monoxide (from vehicles), ground-level ozone, and particulate matter.[*] In India as well, systems that provide real-time ambient air quality data have been implemented. For example, Delhi Pollution Control Committee provides real-time data on particulate matter in air for different regions of the Delhi city on their website.[†] The IoT has the potential to be used in the monitoring of varied environmental parameters. For example, we can monitor water level in lakes, dams, and rivers; air pollutant concentrations for cities; or for animal detection, detection of forest fires (Lazarescu 2013). Ridley Terminals Incorporation uses the IoT to prevent coal dust pollution. This system sends alerts to staff and management via SMS and e-mail whenever there is spontaneous combustion of thermal coal.[‡] This prevents spread of fire by timely control and reduces losses occurring due to such events.

13.3.3 IoT in Automotive Domain

The IoT provides a new relationship between people and vehicles. As per the report by IBM, tomorrow's automotive disruptors are likely to be organizations that are able to integrate digital business with a new level of digital intelligence to create exceptional mobility experiences (IBM 2017). The IoT can detect the driving patterns of individuals that can be useful in saving lives. Using sensors on cars, real-time data on vehicle can be collected and accessed to improve in-car experience.

[*] Please visit https://d2pwrbx99jwry6.cloudfront.net/wp-content/uploads/Dubai-Municipality.pdf for more information, accessed on 8/10/2017.

[†] Please visit www.dpccairdata.com/dpccairdata/display/ITIJahangirpuriView15MinData.php for more details, accessed on 29/10/2017.

[‡] Please visit https://d2pwrbx99jwry6.cloudfront.net/wp-content/uploads/Ridley-Coal-Terminals.pdf, accessed on 8/10/2017.

IBM has also reported about a Japanese auto manufacturer and identifies potential safety issues using advanced analytics to identify patterns and correlations between safety issues and root causes, allowing the automaker to find problems exponentially faster and more accurately. Vehicle tracking system is another application of the IoT that may help transportation fleet of a company by providing real-time information on the location aspects of a vehicle.

13.3.4 IoT in Home Automation

Products like Amazon and Echo Dot are changing the way we live. Through such systems, we are able to interact with small and large equipment, such as air conditioners (switching on/off, setting ambient temperature, etc.), lights (switching on/off, dimming, changing hues, etc.), controlling television, home theaters etc., both inside and outside our homes using mobile apps. Through products like Canary, Neurio, Connect Sense, etc., we can monitor temperature, humidity, security, power use, status of lighting, etc. Such devices are able to integrate electronic gadgets in a house with each other. With such incorporations, home devices are able to talk with each other, resulting in convenience, energy saving, and providing safety measures (Bhide 2014). Artificial intelligence and cloud computing are making these gadgets smart and responsive. For example, through Alexa (Amazon's cloud-based voice service), Echo Dot can stream music, provide answer to user's questions, suggest movies and its time, help in controlling home devices, and much more.

Under this backdrop, this chapter focuses on the IoT applications in healthcare. Therefore, from the following section, the authors discuss the IoT adoption in the context of healthcare with a particular focus on the reasons for their adoption and use. Though the IoT has the potential to offer enormous benefits in healthcare, the authors believe that it also faces many key challenges. The challenges such as identity management, interoperability, privacy, security, etc. (Khan et al. 2012) are covered in a greater depth in the context of healthcare.

13.3.5 IoT in Healthcare

The IoT can have one of the most promising applications in health-care domain. Markets and Markets estimate that the IoT health-care market is projected to grow to USD 158.07 billion in 2022 from USD 41.22 billion in 2017, at a compound annual growth rate of 30.8%.[*] In addition, they estimate that the market for global wearable medical devices will be USD 12.1 billion by 2021 from USD 5.3 billion in 2016, at a compound annual growth rate of 18.0%.[†] Major growth drivers of the

[*] Source: www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html, accessed on 29/10/2017.

[†] Source: www.marketsandmarkets.com/Market-Reports/wearable-medical-device-market-81753973. html, accessed on 29/10/2017.

IoT health-care market are evolution of artificial intelligence technology, rise in investments for the implementation of the IoT health-care solutions, and the penetration increase in connected devices in healthcare. Availability of real-time data for the purpose of monitoring or diagnosis can be crucial in saving a person's life. Given that the IoT has the potential to provide information about various health parameters from a number of interconnected sensor-based devices, lifesaving decisions can be taken not only by doctors but also patients. The advantages of the IoT in healthcare can also be leveraged in isolated or remote locations, where the presence of necessary medical facilities is not available for people who need constant medical supervision. There has been use of healthcare-related information systems since last few decades; however, such systems have restricted utility such as to store and view patient-related data. Analysis on such data is usually descriptive, such as knowing the number of visits made by a patient to the hospital, medications suggested, ailment symptoms, etc.

Most of such systems fail to provide real-time information about the patient health to doctors. With the IoT, there is immense possibility for transmission of data about a patient's condition to caregivers. With lower costs and good quality, wireless sensor based devices are available, which can detect various health-related parameters like blood pressure, heart rate, pulse rate, body temperature, etc. For patients, whose physiological status requires close attention can be constantly monitored using such noninvasive monitoring (Niewolny 2013). The IoT are being used in healthcare for better and efficient services. Niewolny (2013) describes a home health reference hub (refer to Figure 13.3) that enables collection and sharing of physiological information about a patient. The hub captures patient

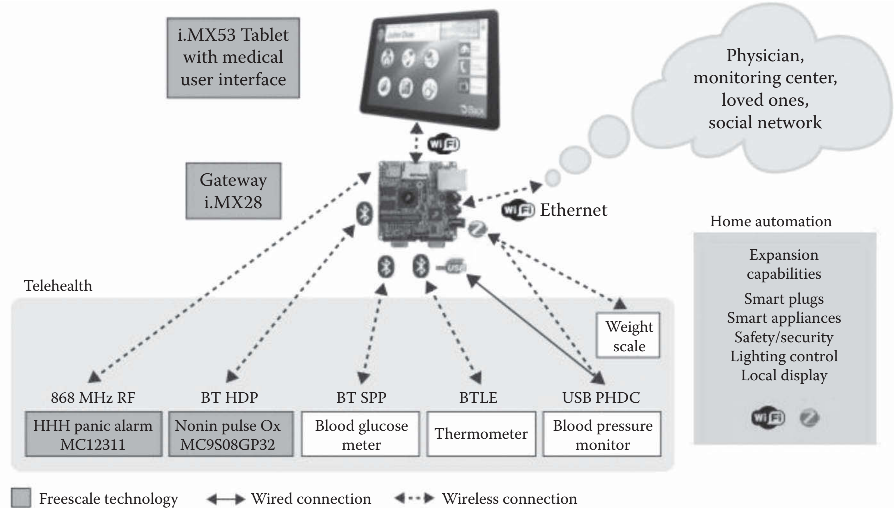


Figure 13.3 Home health reference hub.

data from different sensors and stores it in the cloud, where it can be accessed by caregivers.

Thus, we see that the IoT has uses in remote and real-time monitoring, clinical care, and early preventive care and medical emergencies.

13.4 IoT and Healthcare Wearable Devices

According to Gao et al. (2016), wearable devices are those devices that can be worn or mated with human skin to continuously and closely monitor an individual's activities, without obstructing the users' motions. Wearable devices are useful in unobtrusive monitoring of health-related parameters. Wearable devices may be embedded into textiles, in fashionable clothes or worn as mask to move voluntary muscles that have degraded due to medical ailments. Based on our literature review, healthcare wearable devices can be broadly categorized into "over-the-body" and "in-the-body" devices.

13.4.1 Over-the-Body Devices

Such devices are usually placed over the skin, worn on hands, arms, etc., or part of some external electronic gadgets. There are devices that can be laid as a patch on skin for monitoring and measuring a patient's heart rate, respiratory rate, skin temperature, and body posture. For example, Zio XT Patch,* developed by iRhythm, detects abnormal heart activity for two weeks and can be worn continuously. The data that is collected by the device is analyzed using a set of algorithms to provide necessary feedback. Wearable glucose monitoring devices are used to monitor glucose level continuously, and they seek to replace the need for users to rely on blood glucose meters. Some wearable devices use an accelerometer to gauge a user's activity level and help to alleviate pain in body parts.

13.4.2 In-the-Body Devices

These are placed inside the body as an implant to monitor and measure different health parameters. For example, some wearable devices are available to aid women to determine the time of ovulation and the most fertile period to conceive a child. The wearable device is inserted into the vagina, and then the biosensor monitors core body temperature throughout a woman's menstrual cycle. Through recent technological advancements, implantable devices are being used for better health monitoring, and in some cases, drugs or hormones are automatically released in the body based on analyzed data from the devices. For example, implantable skin

* For more information please visit: http://irhythmtech.com/products-services/zio-xt, accessed on 15/10/2017.

patches are available that sense arterial stiffening for heart attack related warnings. There are devices that can detect epileptic fits and automatically deliver drugs directly to affected areas of the brain.

It is observed that more impetus is being given to make wearable devices as small as possible so that the unobtrusiveness of such devices remains intact. In addition, emphasis is also on monitoring multiple vital parameters through a single device so that they provide a comprehensive bio/nonbiomedical data for analysis purpose. It can be rightly said that the IoT has undeniably immense opportunity for preventive, diagnostic, and recuperative healthcare. However, this development and deployment of IoT in healthcare is full of several challenges. In the next section, the authors discuss these challenges under the social, technical, regulatory, and managerial perspective.

13.5 Challenges of IoT in Healthcare

As every coin has two sides, the IoT applications in healthcare have positives and negatives. Most of the positives have been discussed in earlier sections; however, there are also some negatives that influence development and deployment of IoT-enabled wearable devices. Through literature review, the authors group such "negatives" into four broad categories: social, technical, regulatory, and managerial challenges. For smooth development and deployment of IoT in healthcare, strategies have been mentioned to overcome them. The major challenges in the IoT development and use are discussed as follows:

13.5.1 Social Challenges

According to Friedewald and Raabe (2011), possession of affordable devices, access to infrastructure and services and usability are important limiting factors in the adoption of IoT. However, factors such as awareness, cost of such devices, fear of technology, and resistance in adoption are also relevant for IoT-enabled wearable devices. Apart from these, legal and ethical challenges loom large on wearable medical devices. These factors have been discussed in detail later:

13.5.1.1 Awareness

Here, awareness is used in the context of healthcare wearable devices and individual's health consciousness. People's health and well-being are significantly affected by lifestyle factors such as smoking, hygiene, diet, and physical activity. These involve behaviors that are potentially controllable by the individual (Ryan et al. 2008). Hence, use of healthcare wearable device will be dependent on an individual's attitude toward health. It is likely that the person who seeks healthy lifestyle may use IoT-enabled devices.

13.5.1.2 Cost

The market for wearable technology is still at the stage of "early adoption" of Everett Rogers's diffusion of innovation trajectory (Sultan 2015). Hence, being in the early stage of innovation trajectory, IoT-enabled devices generally have high production costs driven by recently incurred design costs, frequent modifications, and low or unpredictable production volumes. Also in early stage of product life cycle, marketing costs may also be high. In addition, users have to bear an additional cost for repeatedly needing to learn new interfaces associated with the IoT (Costello et al. 2017). Therefore, the cost of wearable technologies might be high and may be a deterrent in its adoption. However, as these devices are early in their lifecycle, only early adopters may use such innovative products as they are likely to value performance over price (Solomon et al. 2000). In addition, according to Al Ameen and Kwak (2011), the cost of maintaining healthcare wearable devices may lay an extra financial burden on the person and the government.

13.5.1.3 Fear and Resistance in the Use of Healthcare IoT Devices

In their research on acceptance of WSNs by elderly people, Steele et al. (2009) concluded that there can be a lack of interest in using WSN systems due to the fear of not being able to interact with the system and the lack of confidence in them even though there are positive attitudes toward WSN systems. According to Schaar and Ziefle (2011), gender and level of technical experience have an influence on the adoption of technology. The authors point out that men are more willing to accept technology than women. Individuals with high technical experience are more likely to adopt technology in comparison with their low technical-experienced counterparts. Wearable devices inside human body may put psychological pressures on the mind of an individual (Al Ameen and Kwak 2011). In addition, fear related to privacy and security of data may also be a challenge in the adoption of healthcare wearable devices. There is also a social stigma attached with the use of healthcare wearables as people may feel pressured to adopt technology just to remain independent. In addition, some people may feel ashamed and view technology as an admission of dependence on wearable devices (Kang et al. 2010).

13.5.1.4 Less Social and Caregiver Contact

It is often believed that social contact is a sign of health in elderly patients. It is possible that monitoring technology could be used to replace caregiver–patient interactions. This may reduce the therapeutic aspect of social contact for the elderly patients, who are vulnerable to social isolation (Kang et al. 2010). Therefore, it is also important to ensure that technology is not a replacement of human care and does not contribute to the patient's isolation or does not threaten the trust in patient–physician relation (Lymberis 2003).

13.5.1.5 Legal and Regulatory Issues

The major challenges of legal issues come with the data generated through IoT devices. In literature, we did not come across examples where a robust legal framework is prevalent to define the actual ownership (who has the authority to delete, edit, and add information to data) and use of medical data generated by IoT devices. These reflect the intellectual property rights associated with the data. In the context, where the data is exchanged among different stakeholders at different places, the most pertinent issue is who owns the responsibilities and liabilities for the data collected from a person (Al Ameen et al. 2012), security, privacy, and its use. In addition, the devices also need to meet international quality standards to transcend international boundaries from consumer gadgets to medical devices. However, to avoid stringent regulations of a country, wearable devices are categorized as wellness/lifestyle tracking devices, which do not require rigid standards (Hiremath et al. 2014). Most countries do not have legal or regulatory framework to control development and use of healthcare wearable devices. Few regulatory bodies have touched upon a legal framework. For example, the Food and Drug Administration (FDA) in the United States of America (USA) issued a guidance document on the use of medical apps on mobile phones on September 25, 2013. In addition, FDA regulates wearable medical devices that consumers use. There is an approval process for the wearable medical devices. Only after being approved, such devices can be sold in market. FDA also focuses on how people can use these devices safely and effectively. There are countries like India, which have enacted the "IT Act"; however, there is no reference on the use of data collected through such devices. Certain conditions, such as emergency, disasters, or remote patient monitoring may require disclosure of information to other people to serve the patient in need (Al Ameen and Kwak 2012). According to Kang et al. (2010), medical care must be provided in accordance with state law even for providing care "remotely."

13.5.1.6 Security and Privacy

These issues include access rights to data and its analysis, how and when data is stored, security during data communication, and the governing policies (Meingast et al. 2006). Data collected from wearable sensors is vulnerable to data privacy concerns. Health-related data is sensitive as it may have users' absolute location and movement activities that compromise the users' privacy in case there is no safeguard against such information during the processes of storage or communication (Hiremath et al. 2014). Technologies used in the IoT may pose severe information security risks. For example, RFID may allow access to security-essential or competition-critical information due to lack of cryptographic procedures

(Friedewald and Raabe 2011). Personal health information exchange on the Internet exposes this data to more hostile attacks compared with the paper-based medical records (Meingast et al. 2006). In addition, there is also a conflict between security and safety. Too strict and rigid data access control may prevent the health-related data being accessed in time by legitimate medical staff, especially in emergency scenarios where the patient may be unconscious and unable to respond. On the other side, a loose access control scheme exposes data to malicious attackers (Li et al. 2010). There is often a possibility of monitoring the individuals without them being aware of it. The huge volume of data recorded by the sensors and communicated in different ways through networks may bring prejudice to the individual's private life (Popescul and Georgescu 2014).

Therefore, wireless communications, due to their remote access capabilities, are vulnerable to eavesdropping and masking attacks (Miorandi et al. 2012). Characteristics of the IoT such as global connectivity ("access anyone") and accessibility ("access anyhow, anytime") make them vulnerable to a number of attack vectors available to malicious attackers (Roman et al. 2013). For confidentiality, established encryption technology exists; however, such encryption technologies may not be feasible for the IoT technologies due to their limited computing power. Measures that can ensure authentication, confidentiality, and access control in the heterogeneity and mobility of "things" in the IoT will help build trust in them (Sicari et al. 2015).

13.5.1.7 Ethical Issues

Such issues mainly are the result of privacy and security challenges, equity in the access, health gap between rich and poor (and the associated life expectancy gap) as a result of the IoT use, trust, agency, and responsibility of errors (Brown and Adams 2007). Human and technology interaction are often complex in nature. In a digital age, society is generally divided based on access to technology and its use. Such division is related to availability of technology, socioeconomic status of individuals, skill set of a person to use the technology, etc. Similarly, the IoT are also subject to such divides. Hence, there will be people who will have access to the latest IoT devices, while some will not be in a position to use the devices due to several reasons. Those who have access to the IoT-based wearable devices will reap its benefits and avail better health-related decisions than the disadvantaged ones.

In literature, terms like "digital divide," "information rich and information poor," "haves and have nots," etc. are generally used to describe the biases in the access and use of ICTs. ICTs are used as an empowerment tool that helps in providing right information at the right time. "Access to information" may be seen as a right and therefore quite relevant for developing countries like India. Empowerment of the disadvantaged is a necessity to enhance their livelihoods. However, is access to the IoT-enabled health-care devices a necessity or a luxury? Well, the authors believe that the IoT is in the very early stage of product life cycle, the demarcation based on the "haves and have nots" may not hold unless this technology move ahead in the product life cycle.

The ethical question "who is to blame, and how will the consequent cost be covered?" may arise if the IoT healthcare devices go wrong and harm results (Brown and Adams 2007). Popescul and Georgescu (2014) believe that the digital divide will increase in the IoT, as it will be understood only by experts. They are also concerned whether there will be a fair distribution of benefits and costs as well as equal access to advantages leashed by the IoT.

Trust is another issue that is of concern, since the IoT ecosystem is characterized by different devices that have to process and handle the data in compliance with user needs and rights (Sicari et al. 2015). Device trust refers to the need to interact with reliable devices such as sensors and actuators. Daubert et al. (2015) discuss trust with reference to device, process, connection, and system. Device trust reflects the need to interact with reliable devices such as sensors and actuators. Processing trust relates to the need to deal with correct, meaningful, and errorless data. Connection trust relates to the requirement to exchange the right data with right service providers. System trust is associated with an expectation to use a dependable overall system by providing transparency to all involved stakeholders regarding workflows, processes, and underlying technology. Such matching between different stakeholders is generally based on trust relationships (Bandyopadhyay and Sen 2011).

13.5.2 Technological Challenges

Apart from social issues, technological issues also limit the use of the IoT in healthcare. The technological challenges range from data storage and management (e.g., physical storage issues, availability, and maintenance) and not limited to interoperability and managing heterogeneity alone. The major technological challenges that are seen as impediments in the use of IoT for healthcare are as follows:

13.5.2.1 Software and Algorithm

According to Sundmaeker et al. (2010), there is a lack of a common software fabric underlying how the software in different environments can be integrated to function as a composite system. Other challenge is how to build an integrated application out of a large collection of heterogeneous software modules using open middleware. There is also a need for encryption algorithms that are energy efficient. There is also a requirement for intelligent algorithm to trigger activities from multiple events (such as group observations or sensor readings) rather than just a single event. For this, the algorithm must correlate among different events (Bandyopadhyay and Sen 2011). This may also require transformation of raw sensor data in some way or other for integrated analysis. Often these algorithms will have to consider correlation among events that may possibly require transformation of raw sensor data. Moreover, it is expensive to transmit enormous volume of raw data in heterogeneous network, so the data compression and data fusion provision of IoT should be in place so as to reduce the data volume (Qin et al. 2014).

13.5.2.2 Hardware

If the IoT has to provide a standard set of functionalities, there are some stringent requirements on the hardware capabilities of the devices (Miorandi et al. 2012) such as necessity of miniature devices and increased functionality. Often, there is a requirement to upgrade hardware whenever there is change in protocols and designs for high performance in case of scalable algorithms. Such need to upgrade hardware has to be minimized as it would resist various stakeholders in adopting the IoT. There is also a need for energy-efficient devices that require low power, as power and energy storage can be crucial for the use of IoT in healthcare. Microbatteries with enough energy to power devices and energy scavenging technologies that let them collect power from their operating environment are the need of the hour (Sundmaeker et al. 2010).

13.5.2.3 Sharing of Resources

According to Qin et al. (2014), there is a need for shared provisioning of network and sensor resources across multiplicity of applications for efficiency. In the heterogeneous and complex IoT ecosystem, different user-defined tasks may run simultaneously with differentiated quality requirements in terms of reliability (packet loss), latency, jitter, and bandwidth. Therefore, there are chances that these applications are often developed, deployed, and triggered in an uncoordinated manner. Hence, there is a need to coordinate and optimize sharing of resources in such a complex and networked heterogeneous environment. Data and service sharing infrastructure can address several application scenarios. For example, anomaly detection in sensed data can be shared between several applications to reduce computing load on a single device (Gubbi et al. 2013).

13.5.2.4 Interoperability

Interoperability addresses the need for a synched environment, where various heterogeneous devices and platforms are able to talk to each other and provide seamless services. In the present context, most of the wearable devices have their own standards for interoperability, and hence, such specific standards may not integrate different IoT devices. For the IoT, all the devices in the ecosystem should be able to intercommunicate with each other at any given time. This is important because information available on one device may be useful to other devices in the same environment. According to Korzun et al. (2013), device, service, and information interoperability are important in the IoT ecosystem. Device interoperability relates to technologies for seamless device discovery and networking with each other.

Service interoperability is about the technologies for heterogeneous devices to discover services and use them. Information interoperability relates to technologies and processes for seamless exchange of information between devices without a need to know interfacing methods of the entity creating or consuming the information. The overall objective of interoperability is to provide an environment where devices can be deployed in a way to allow them to blend with other IoT devices around them seamlessly (Gubbi et al. 2013).

13.5.2.5 Availability of Search Engine Technologies

Extrapolating the status of the IoT devices several years into the future, the magnitude of sensor-based devices will be more than currently existing webpages (Ostermaier et al. 2010). The IoT would require the development of lookup/referral services for linking information in a way that respects both the privacy of individuals and confidentiality of information (Sundmaeker et al. 2010). Other aspects relate to finding relevant information using search engines. Even though hundreds of general search engines are available, finding relevant and valid health information remains difficult due to the structure and size of the Internet (Ilic et al. 2003). With growing number of devices in the near future, the network traffic will be difficult to manage both in terms of the number of accesses to the devices and of the number of queries received by the search engines (Nitti et al. 2014).

13.5.2.6 Standardization

As we have seen in the previous sections, IoT devices have to be of low cost and should require less power. Due to such nature of devices, they are often disabled for long times (sleep periods) to save energy. Therefore, the networks formed by these devices have different traffic patterns, high packet loss, low throughput, frequent topology changes, and small useful payload sizes (Ishaq et al. 2013). Hence, the integration of IoT devices into the Internet introduces many challenges, as many of the existing Internet standards were not designed for them. Standards are necessary in the IoT as there is a need for bidirectional information exchange among things in the ecosystem. Therefore, it is important to have standards like architecture standards, security standards, data and information processing standards, communication protocol standards, and service platform standards (Chen et al. 2014). In the present context, there are not many standards available for information interchange on the IoT devices and even those that are available are at an abstract level or proprietary in nature. For example, ISO/IEEE 11073 standards are available. They are normally used for bedside monitoring in hospital environments, to wearable, multisensor monitoring systems designed for home healthcare (Yao and Warren 2005). IEEE 802.15.4 standard are there for low-power devices that communicate less data in a short range. If standards for information interchange are available for the IoT ecosystem, then the issues related to interoperability, security, and privacy can be reduced considerably.

Table 13.2 depicts a comparative assessment between in-the-body and over-the-body IoT sensors from the perspective of social and technological challenges discussed in previous sections.

Table 13.2 Comparison of in-the-Body and over-the-Body Social and Technological Challenges

Challenges		*In-the-Body IoT Sensors*	*Over-the-Body IoT Sensors*
Social	Awareness	Low	Comparatively high
	Cost	High	Comparatively low
	Fear and resistance	High	Comparatively low
	Legal and regulatory issues	High	Comparatively low
	Security and privacy	High	Comparatively low
	Ethical issues	High	Comparatively low
Technological	Software and algorithms	Not available for an integrated solution	Not available for an integrated solution
	Hardware	Design, development, and deployment of sensors is challenging	Design, development, and deployment is comparatively easy
	Interoperability and standardization	Lack of interoperable components and standards	Lack of interoperable components and standards

13.6 Strategies to Overcome Sociotechnological Challenges

The sociotechnological challenges discussed in the previous sections have to be addressed so as to enhance their adoption, thereby guaranteeing equitable and seamless services through wearable healthcare. There are many social challenges that cannot be addressed completely but can be reduced to a considerable extent. To reduce the effect of social isolation and stigma of wearable healthcare in elders, it will be an appropriate approach to present the technology to them as a useful, helpful option and as a way to promote safety. In addition, wearable healthcare should be adopted before it is needed, as an option, which could avoid stigmatizing older persons. Also, it is recommended that the wearable devices are as small as possible so as to make them literally invisible and sync easily with the day-to-day activities of elders. For example, these devices can be built into clothing (Kang et al. 2010). This would help in minimizing feelings of dependency, anxiety, and fear in elders.

Digital divide in the use of the IoT devices cannot be overcome only by reducing the cost of such devices or by increasing access to them. It requires a holistic approach by not only individuals but also other stakeholders such as hospitals, government, and private organizations. Skills have to be enhanced, attitudes toward such devices have to be changed, and policy measures toward communication standards, privacy, and security aspects have to be undertaken.

Changes in attitude toward healthcare IoT devices can be there if people understand the usefulness of such devices. Gao and Bai (2014), in their study on adoption of the IoT devices concluded that usefulness is the primary determinant of one's use of the IoT while ease of use, trust, and enjoyment are secondary determinants. In addition, they also conclude that social influence is a major determinant in the use of IoT. Therefore, it is necessary for the IoT service providers to focus on social influence for greater adoption of the IoT technology.

According to Prayoga and Abraham (2016), if people are provided with resources and support such as Internet access and elaborate information to use the device—combined with their tendency to relate the wearable healthcare device's usage to their personal problem, they will be more likely to perceive the device as useful. The IoT practitioners can also take benefit of earlier adopters of the IoT services, whose views and reviews may generate positive social influence on subsequent adoption behavior (Wiedemann et al. 2008). The overcoming of the slowing factors needs a coordinated effort of the IoT practitioners to stimulate interest in potential final users and, in parallel, to boost the evolution of readers, software, and devices toward a more interconnected aspect (Amendola et al. 2014).

Technological challenges too need coordinated efforts by the IoT community. According to Sundmaeker et al. (2010), through consensus processes involving the IoT practitioners, it will be possible to develop standardized semantic data models and ontologies, common interfaces, and protocols. These may be initially defined at an abstract level and then with example bindings to specific cross-platform, cross-language technologies. Semantic ontologies can help to overcome issues resulting from human error or differences and misinterpretation due to different human languages in different regions of the world. To make the devices tightly coupled, an ontological knowledge representation, supporting localized agreements and personalization, is a requirement. Interoperability issue can also be taken care by such mechanisms. It is necessary because the knowledge processors that run in the IoT devices and coordinate in various service scenarios are often loosely coupled (Korzun et al. 2013). As IPv4 addresses, which is a 4-byte addressing system, are decreasing at a fast rate, it is recommended that IPv6 addresses, which are 128 bits, are used to address all the IoT devices. IPv6 can define 10^{38} addresses, which may be enough to identify any object that is worth to be addressed (Atzori et al. 2010).

Bandyopadhyay and Sen (2011) recommended use of service-oriented architecture to support interoperable machine-to-machine and thing-to-thing interaction over a network as it helps to organize the web services and makes it a virtual network. To address the issue of heterogeneity, "Information Driven Sensornet Architecture" is recommended, as protocol designers have to consider only the "information exchanges" with respect to a network protocol. Responsibility of packet creation and buffer provisioning are delegated to the architecture. Because of this, network protocols are simpler and require less memory (De Poorter et al. 2011). Other benefit of the architecture is that it can connect objects directly without any gateway, interpret an incoming packet type and drop unrecognized packets, and support communication between devices that uses different protocols (Rehman et al. 2016).

With respect to data security and privacy, one of the ways to handle the issue is to have concrete security and data governance rules for health-related data access. Charani et al. (2014) elaborate on the need for data governance rules for mobile phones in organizations. Similarly, rigid data governance rules might be applicable in the access and use of data collected from healthcare IoT devices. There is a need to have stringent policies to protect sensitive personal health information as it becomes available electronically (Meingast et al. 2006). Users should be made aware of how the data trails being left by the healthcare devices are stored and used. This would not only be ethical but also help build trust of people in such devices. Framed rules should guide the process of data collection, defining its ownership, storage, use (update, delete, and dissemination) and anonymizing the collected data.

It is recommended that systematic and consistent monitoring of new technologies on their impact on privacy is carried out. There is also a need for role-based access control and security, which may result in the reduction of the network complexity and cost of security administration. In healthcare, role-based control can be done using encryption, which is useful to ensure the security of data and help prevent eavesdropping. Encryption both at hardware and at software level may ensure the highest level of security (Meingast et al. 2006).

13.7 Conclusion

As discussed, the IoT has an immense potential in healthcare; however, implementation challenges are also not less. Data and privacy challenges are at the forefront, given the sensitivity of information associated with the medical data. In developing countries like India, the economic impact of IoT can be materialized if there is a comprehensive strategy toward adoption of IoT technologies. Given that social and technological challenges do not come under the purview of a single stakeholder, all the stakeholders of the IoT community require a coordinated effort. To address security and privacy aspects, public and private players have to come under one roof. Governments may address the privacy and security issues of IoT-related data by formulating stringent data governance rules. In India, the honorable Supreme Court has regarded privacy as the fundamental right of a citizen. The court establishes that the private zone privacy, which relates to the personal data shared during the use of credit cards, social networking platforms, income tax declarations, etc., should be used for the purpose for which it is shared by an individual. Given this context, and especially in relation to health-care data, it is imperative for the Government of India to frame privacy laws so that there is accountability and liability for leakage and misuse of data by any person or organization. In addition, the healthcare wearable devices should come under strict regulations for approval and use. The approval process should focus on whether the medical wearable device is safe for use by common people. For this, health and IT departments of government have to function in sync to frame such monitoring and evaluation processes. In addition, emphasis should be there to monitor the data protection and security aspects of the device. The process should ensure that the technical standards used for data communication between devices are safe and secure.

Medical wearable devices manufacturing organizations also have a responsibility toward data protection. These organizations should ensure that the components used in the medical wearable devices are safe to use and reliable. In addition, the organization should adhere to existing privacy laws and act in accordance with them. Research and development should be an ongoing process to consistently improve data protection technology. Service providers also play a significant role in reduction of privacy and security challenges. They are the true custodians of users' data. Service providers with respect to data management require effective quality measures in accordance to the privacy and security laws of a country. At an individual level, we should be aware of how our data will be used by the service provider.

Social stigma associated with the medical wearable devices may be overcome by the government, hospitals, nongovernment organizations, doctors, and individuals. Through everyone's effort, an enabling environment can be created for the adoption of medical IoT devices. In addition, to reduce the impact of digital divide, the IoT community may create mechanisms for creating awareness on the use of wearable devices to reduce resistance in the use of technology. Doctors, nongovernment organizations, and wearable device users may socially influence others to allay fears of using medical wearables. Though the cost of such devices is reducing, however, the present cost is beyond the reach of people in developing countries like India. Hence, developing countries should engage in government–industry partnerships for social and medical researches/social research for cost reduction of wearable devices. As we are aware that these devices are early in their life cycle, the earlier steps will be important in creating trust of users in medical wearables and thereby foster smoother adoption.

References

Acer, Utku Günay, Aidan Boran, Claudio Forlivesi, Werner Liekens, Fernando Pérez-Cruz, and Fahim Kawsar. "Sensing WiFi network for personal IoT analytics." In *Internet of Things (IOT), 2015 5th International Conference on the Internet of Things*, Seoul, South Korea, pp. 104–111. IEEE, 2015.

Al Ameen, Moshaddique, and Kyung Sup Kwak. "Social issues in wireless sensor networks with healthcare perspective." *International Arab Journal of Information Technology* 8, no. 1 (2011): 52–58.

Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak. "Security and privacy issues in wireless sensor networks for healthcare applications." *Journal of Medical Systems* 36, no. 1 (2012): 93–101.

Amendola, Sara, Rossella Lodato, Sabina Manzari, Cecilia Occhiuzzi, and Gaetano Marrocco. "RFID technology for IoT-based personal healthcare in smart spaces." *IEEE Internet of Things Journal* 1, no. 2 (2014): 144–152.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The Internet of Things: A survey." *Computer Networks* 54, no. 15 (2010): 2787–2805.

Bandyopadhyay, Debasis, and Jaydip Sen. "Internet of Things: Applications and challenges in technology and standardization." *Wireless Personal Communications* 58, no. 1 (2011): 49–69.

Bellavista, Paolo, Giuseppe Cardone, Antonio Corradi, and Luca Foschini. "Convergence of MANET and WSN in IoT urban scenarios." *IEEE Sensors Journal* 13, no. 10 (2013): 3558–3567.

Bhide, Vishwajeet H. "A survey on the smart homes using Internet of Things (IoT)." *International Journal of Advance Research in Computer Science and Management Studies* 2, no. 12 (2014): 243–246.

Borgohain, Tuhin, Uday Kumar, and Sugata Sanyal. "Survey of security and privacy issues of Internet of Things." International Journal of Advanced Network Applications, vol. 6, no. 4 (2015). 2372–2378.

Brown, Ian, and Andrew A. Adams. "The ethical challenges of ubiquitous healthcare." *International Review of Information Ethics* 8, no. 12 (2007): 53–60.

Charani, Esmita, Enrique Castro-Sánchez, Luke S. P. Moore, and Alison Holmes. "Do smartphone applications in healthcare require a governance and legal framework? It depends on the application!" *BMC Medicine* 12, no. 1 (2014): 29.

Chen, Shanzhi, Hui Xu, Dake Liu, Bo Hu, and Hucheng Wang. "A vision of IoT: Applications, challenges, and opportunities with china perspective." *IEEE Internet of Things Journal* 1, no. 4 (2014): 349–359.

Coetzee, Louis, and Johan Eksteen. "The Internet of Things-promise for the future? An introduction." In *IST-Africa Conference Proceedings, Gaborone , 2011*, pp. 1–9. IEEE, 2011.

Costello, Richard W., Alexandra L. Dima, Dermot Ryan, R. Andrew McIvor, Kay Boycott, Alison Chisholm, et al. "Effective deployment of technology-supported management of chronic respiratory conditions: A call for stakeholder engagement." *Pragmatic and Observational Research* 8 (2017): 119.

Daubert, Joerg, Alexander Wiesmaier, and Panayotis Kikiras. "A view on privacy & trust in IoT." In *2015 IEEE International Conference on Communication Workshop (ICCW), London* , pp. 2665–2670. IEEE, 2015.

De Poorter, Eli, Evy Troubleyn, Ingrid Moerman, and Piet Demeester. "IDRA: A flexible system architecture for next generation wireless sensor networks." *Wireless Networks* 17, no. 6 (2011): 1423–1440.

Finger, G. "Digital convergence and its economic implications." Development Bank of Southern Africa, 2010. https://www.dbsa.org/EN/About-Us/Publications/Documents/Digital%20convergence%20and%20its%20economic%20implications.pdf. Accessed on 10/10/2017.

Friedewald, Michael, and Oliver Raabe. "Ubiquitous computing: An overview of technology impacts."

Gao, Lingling, and Xuesong Bai. "A unified perspective on the factors influencing consumer acceptance of Internet of Things technology." *Asia Pacific Journal of Marketing and Logistics* 26, no. 2 (2014): 211–231.

Gao, Wei, Sam Emaminejad, Hnin Yin Nyein, Samyuktha Challa, Kevin Chen, Austin Peck, et al. "Fully integrated wearable sensor arrays for multiplexed in situ perspiration analysis." *Nature* 529, no. 7587 (2016): 509–514.

Ghayvat, Hemant, Subhas Mukhopadhyay, Xiang Gui, and Nagender Suryadevara. "WSN-and IOT-based smart homes and their extension to smart buildings." *Sensors* 15, no. 5 (2015): 10350–10379.

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future Generation Computer Systems* 29, no. 7 (2013): 1645–1660.

Hiremath, Shivayogi, Geng Yang, and Kunal Mankodiya. "Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare." In 2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), Athens, pp. 304–307. IEEE, 2014.

IBM. The Cognitive Effect on Automotive Unleashing Exceptional Experiences from an Abundance of Data, 2017. www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03870USEN&. Accessed on 08/10/2017.

Ilic, Dragan, T. L. Bessell, C. A. Silagy, and S. Green. "Specialized medical search-engines are no better than general search-engines in sourcing consumer information about androgen deficiency." *Human Reproduction* 18, no. 3 (2003): 557–561.

Ishaq, Isam, David Carels, Girum K. Teklemariam, Jeroen Hoebeke, Floris Van den Abeele, Eli De Poorter, et al. "IETF standardization in the field of the Internet of Things (IoT): A survey." *Journal of Sensor and Actuator Networks* 2, no. 2 (2013): 235–287.

Kang, Hyun Gu, Diane F. Mahoney, Helen Hoenig, Victor A. Hirth, Paolo Bonato, Ihab Hajjar, et al. "In situ monitoring of health in older adults: Technologies and issues." *Journal of the American Geriatrics Society* 58, no. 8 (2010): 1579–1586.

Kaushik, Shailandra. "An overview of technical aspect for WiFi networks technology." *International Journal of Electronics and Computer Science Engineering (IJECSE, ISSN: 2277-1956)* 1, no. 1 (2012): 28–34.

Khan, Rafiullah, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. "Future internet: The Internet of Things architecture, possible applications and key challenges." In 2012 10th International Conference on Frontiers of Information Technology, Islamabad, pp. 257–260. IEEE, 2012.

Korzun, Dmitry G., Sergey I. Balandin, and Andrei V. Gurtov. "Deployment of smart spaces in Internet of Things: Overview of the design challenges." In *Internet of Things, Smart Spaces, and Next Generation Networking*, Edited by Balandin, Sergey, Sergey Andreev, and Yevgeni Koucheryavy, pp. 48–59. Springer: Berlin and Heidelberg, 2013.

Lazarescu, Mihai T. "Design of a WSN platform for long-term environmental monitoring for IoT applications." *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 3, no. 1 (2013): 45–54.

Lee, In, and Kyoochun Lee. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." *Business Horizons* 58, no. 4 (2015): 431–440.

Li, Ming, Wenjing Lou, and Kui Ren. "Data security and privacy in wireless body area networks." *IEEE Wireless Communications* 17, no. 1 (2010).

Lymberis, A. "Smart wearable systems for personalised health management: Current R&D and future challenges." In Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE Cat. No.03CH37439), Vol. 4, pp. 3716–3719. IEEE, 2003.

Ma, Hua-Dong. "Internet of Things: Objectives and scientific challenges." *Journal of Computer Science and Technology* 26, no. 6 (2011): 919–924.

Meingast, Marci, Tanya Roosta, and Shankar Sastry. "Security and privacy issues with health care information technology." In 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, New York, NY, pp. 5453–5458. IEEE, 2006.

Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. "Internet of Things: Vision, applications and research challenges." *Ad Hoc Networks* 10, no. 7 (2012): 1497–1516.

Mueller, Milton. "Digital convergence and its consequences." *Javnost – The Public* 6, no. 3 (1999): 11–27.

Niewolny, David. How the Internet of Things Is Revolutionizing Healthcare, 2013. www.nxp.com/docs/en/white-paper/IOTREVHEALCARWP.pdf. Accessed on 15/10/2017.

Nitti, Michele, Luigi Atzori, and Irena Pletikosa Cvijikj. "Network navigability in the social Internet of Things." In 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, pp. 405–410. IEEE, 2014.

Ogunsola, L. A. "Information and communication technologies and the effects of globalization: Twenty-first century "digital slavery" for developing countries – myth or reality." *Electronic Journal of Academic and Special Librarianship* 6, no. 1–2 (2005): 1–10.

Ostermaier, Benedikt, Kay Römer, Friedemann Mattern, Michael Fahrmair, and Wolfgang Kellerer. "A real-time search engine for the web of things." In *Internet of Things (IOT), 2010*, Tokyo, pp. 1–8. IEEE, 2010.

Pelino, Michele, and Frank E. Gillet. The Internet of Things Heat Map, 2016-Where IoT Will Have the Biggest Impact on Digital Business. Forrester, 2016. www.cloudera.com/content/dam/www/marketing/resources/analyst-reports/forrester-the-iot-heat-map.pdf.landing.html. Accessed on 29/10/2017.

Prayoga, Tommy, and Juneman Abraham. "Behavioral intention to use IoT health device: The role of perceived usefulness, facilitated appropriation, big five personality traits, and cultural value orientations." International Journal of Electrical and Computer Engineering 6(4): (2016): 1751-1765.

Popescul, Daniela, and Mircea Georgescu. "Internet of Things – Some ethical issues." *The USV Annals of Economics and Public Administration* 13, no. 2(18) (2014): 208–214.

Qin, Zhijing, Grit Denker, Carlo Giannelli, Paolo Bellavista, and Nalini Venkatasubramanian. "A software defined networking architecture for the Internet-of-Things." In *Network Operations and Management Symposium (NOMS), Krakow, 2014 IEEE*, pp. 1–9. IEEE, 2014.

Rehman, Sadiq Ur, Iqbal Uddin Khan, Muzaffar Moiz, and Sarmad Hasan. "Security and privacy issues in IoT." International journal of communication networks and information security 8, no. 3 (2016): 147.

Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed Internet of Things." *Computer Networks* 57, no. 10 (2013): 2266–2279.

Ryan, Richard M., Heather Patrick, Edward L. Deci, and Geoffrey C. Williams. "Facilitating health behaviour change and its maintenance: Interventions based on self-determination theory." *European Health Psychologist* 10, no. 1 (2008): 2–5.

Ramchandran, S. IDC Manufacturing Insights #IN250976, May 2015. www.wipro.com/documents/insights/innovative-use-cases-for-the-adoption-of-internet-of-things.pdf. Accessed on 08/10/2017.

Schaar, Anne Kathrin, and Martina Ziefle. "Smart clothing: Perceived benefits vs. perceived fears." In 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops, Dublin, pp. 601–608. IEEE, 2011.

Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead." *Computer Networks* 76 (2015): 146–164.

Solomon, Rajeev, Peter A. Sandborn, and Michael G. Pecht. "Electronic part life cycle concepts and obsolescence forecasting." *IEEE Transactions on Components and Packaging Technologies* 23, no. 4 (2000): 707–717.

Steele, Robert, Amanda Lo, Chris Secombe, and Yuk Kuen Wong. "Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare." *International Journal of Medical Informatics* 78, no. 12 (2009): 788–801.

Sultan, Nabil. "Reflective thoughts on the potential and challenges of wearable technology for healthcare provision and medical education." *International Journal of Information Management* 35, no. 5 (2015): 521–526.

Sun, Chunling. "Application of RFID technology for logistics on Internet of Things." *AASRI Procedia* 1 (2012): 106–111.

Sundmaeker, Harald, Patrick Guillemin, Peter Friess, and Sylvie Woelfflé. "Vision and challenges for realising the Internet of Things." *Cluster of European Research Projects on the Internet of Things, European Commission* 3, no. 3 (2010): 34–36.

Tiwari, Rajnish, Stephan Buse, and Cornelius Herstatt. "From electronic to mobile commerce: Opportunities through technology convergence for business services." (2006).

Tufano, James T., and Bryant T. Karras. "Mobile eHealth interventions for obesity: A timely opportunity to leverage convergence trends." *Journal of medical Internet Research*, 2005;7(5):e58. doi:10.2196/jmir.7.5.e58

Uckelmann, Dieter, Mark Harrison, and Florian Michahelles. "An architectural approach towards the future Internet of Things." In *Architecting the Internet of Things*, Edited by Uckelmann, Dieter, Harrison, Mark, Michahelles, Florian (Eds.), pp. 1–24. Springer: Berlin and Heidelberg, 2011.

Wiedemann, Dietmar G., Tobias Haunstetter, and Key Pousttchi. "Analyzing the basic elements of mobile viral marketing-an empirical study." In 7th International Conference on Mobile Business, Barcelona , pp. 75–85. IEEE, 2008. pp. 75–85. doi: 10.1109/ICMB.2008.41

Xia, Feng, Laurence T. Yang, Lizhe Wang, and Alexey Vinel. "Internet of Things." *International Journal of Communication Systems* 25, no. 9 (2012): 1101.

Yao, Jianchu, and Steve Warren. "Applying the ISO/IEEE 11073 standards to wearable home health monitoring systems." *Journal of Clinical Monitoring and Computing* 19, no. 6 (2005): 427–436.

Zhu, Qian, Ruicong Wang, Qi Chen, Yan Liu, and Weijun Qin. "IoT gateway: Bridging wireless sensor networks into Internet of Things." In IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, pp. 347–352. IEEE, 2010.

6
Mobile Medical Devices

Wireless technology has played a significant role in reshaping healthcare over the last two decades. Wi-Fi began to impact the clinical workflow in a significant way starting in 1999. The two key catalysts that have propelled increased adoption within healthcare institutions are FCC regulations, as well as the evolution of the IEEE standards, and increasing maturity of the Wi-Fi Alliance. The other two major organizations that have helped push adoption are the Food and Drug Administration (FDA), and the Association for the Advancement of Medical Instrumentation (AAMI). Recent federal government mandates like the push to attain meaningful use have also contributed to driving increased adoption. Many areas have been impacted by mobility, including devices supporting voice and video, but the area that has seen the most dramatic workflow improvements is the medical device arena. With wireless medical telemetry systems (WMTS) on the decline, using Wi-Fi as a means of transporting data from medical devices to the network, and between sensors and medical devices, has been a growing field. Medical device vendors continue to struggle to integrate Wi-Fi into their devices, with hit-and-miss results. Prior to diving into specific use cases, the following section will address the roles that the various government and regulatory agencies have played in shaping the Wi-Fi-centric mHealth arena.

The FDA is heavily involved with clearing different types of medical devices to be introduced to the U.S. market. The Medical Device Amendments Act of 1976 lays the foundation for the 510(k) process, which is used to clear upwards of 90 percent of medical devices to be sold in the U.S. market. Thankfully this process is not as stringent as the processes that are used to introduce a new drug to market. Medical devices are classified into one of three classes as follows.

Class I: Devices that are not intended to sustain life do not require undergoing the 510(k) process or clearance but needing to follow general controls. Tongue depressors and latex gloves are examples of Class I devices.

Class II: Devices that need to meet minimal performance requirements and need to be cleared for safety and efficacy using the 510(k) process. IV Pumps are a Class II device.

Class III: This class of devices is necessary to sustain life, and must undergo the 510(k) premarket approval process, and are often used in clinical trials prior to release. These include devices such as defibrillators and implanted medical devices.

Generally only Class II and Class III devices will require network connectivity and thus can potentially leverage Wi-Fi. The 510(k) process is often lengthy and involves substantial testing which is generally focused around patient safety and the efficacy of a given device. Network communications capabilities are often taken for granted and are an afterthought. Areas like how a device will function in a dense Wi-Fi environment, preferred frequency bands, and supported authentication and encryption schemes are generally farmed out to the manufacturer of the wireless card being used, with little consideration for wireless best practices. The line of demarcation between regulating a device as a medical device and regulating it as a communications device has prompted the FDA to work closely with the FCC when dealing with wireless medical devices. In 2011, the FDA released draft guidance on mobile device applications (Medical Device Data systems rule). The integration between these two organizations is crucial for the success of the mHealth space.

The FCC released the MBAN proposal in 2012 which allocates a dedicated spectrum for body sensors to transmit data in real time. The idea is that these types of sensors will result in a substantial return on investment for healthcare institutions by decreasing the risk of infections and promoting early decisions and better outcomes.

Although the FDA is starting to move in a direction that is helping drive mHealth forward, there is still much lacking. When medical device vendors design a device, it often takes upwards of a year to introduce it to market. In the telecommunications space, the span of a year can see tremendous improvements from the perspective of standards, security, or bandwidth availability. By the time a device makes it to the market, the integrated Wi-Fi capabilities are often outdated. The device can have a lifecycle spanning upwards of 5 years, or longer in some instances. It is crucial for these types of medical devices to have a flexible networking architecture that allows for upgrading drivers and even hardware if needed, with minimal scrutiny from the FDA. If the sole functionality being impacted is Wi-Fi functionality, it would be beneficial to have a series of high-level wireless tests that can be conducted to clear the firmware, or even hardware upgrade path.

We only touch the tip of the iceberg when discussing medical devices. A new type of medical device that integrates with smart phones and tablets is really pushing the traditional boundaries with the FDA. This area, compounded by the explosive growth of healthcare-related mobile applications, has been forcing the organization to rethink and reinvent its review mechanisms.

In June of 2013 the FDA released a draft guidance pertaining to the cybersecurity of medical devices. The target audiences were primarily medical device manufacturers, and the document entitled "Content of premarket submissions for management of cybersecurity in medical devices" calls attention to intentional threats to medical devices. These range from Malware and viruses infecting medical devices to organized penetration and Denial of Service attacks. The ruling urges medical device manufacturers to develop a set of security controls to assure medical devices maintain information confidentiality, integrity, and availability. In part, this means implementing two factor authentication mechanisms including passwords, biometric identifiers, or smartcards in order to restrict the number of individuals capable of interacting with the product.

It can be argued that the FCC is one of the key reasons that wireless technology was able to thrive in healthcare. Since the organization released the ISM band for unlicensed use in 1985, and more recently dedicated a portion of the radio spectrum to WMTS in 2000, it laid the foundation for medical device manufacturers to start to focus on this space. The FCC continues to play a fundamental role in driving mobility in healthcare. The organization's National Broadband Plan released in 2010 along with the ruling allocating 40 MHz of spectrum—2360 to 2400 MHz—for use by medical body area networks

(MBAN) devices in 2012 is a testament to this. They have also been involved in creating some best practices documentation around securing wireless devices. In an effort to remain a leader in the mHealth space, in 2012 the FCC announced that it would be adding a position of Health Care Director to continue to drive innovation in this space. The FCC continues to work with the FDA to ensure that available spectrum is allocated to promote mHealth as much as possible. They have been making every effort to foster innovation.

The AAMI has always been a fundamental player in medical device innovation and design. The organization has been developing standards for medical device design for decades. Wireless medical devices have traditionally been viewed like any other medical device. The typical AAMI audiences are clinical or biomedical engineers who generally deal with the maintenance and repair of medical devices. As medical devices become more dependent on networks and make use of Ethernet and Wi-Fi, the organization has been promoting the need for collaboration between IT and clinical engineering. Many healthcare institutions have taken this mantra to heart, and have shifted their reporting structure so that clinical engineering staff reports to IT leadership. This is an inevitable step given the growth of Wi-Fi-capable medical devices.

By leveraging Wi-Fi, medical device manufacturers have ventured into a shared medium that is outside of their control. When one also considers that many medical devices leverage fairly widespread core operating systems, like Windows, the number of variables that can cause data transmission issues grows. AAMI released the IEC 800001-1 series of standards between 2008 and 2012. These are intended to apply appropriate risk management to IT networks that support medical devices. This is in line with ISO 14971. The standards address safety, system security, and effectiveness, which are generally regarded as necessities for patient well-being. It incorporates best practices for risk management as well as change release management. These are in line with ITIL is the most popular and widely accepted approach to service management. It stands for information technology infrastructure library methodology which is well adopted in the pure IT arena. "Accordinding to the AAMI (Association for the Advancement of Medical Information) IEC 80001-1 it defines responsibilities for parties such as medical device manufacturers, non-medical device manufacturers, the responsible organization, IT-network integrator, and potentially others, engaged in installing, using, configuring, maintaining and decommissioning IT-networks incorporating medical devices." There are four key areas that the standard highlights:

- The three risk components to be managed are safety, effectiveness, and security—and in that order of priority.
- It is ultimately the responsibility of the "responsible organization" (typically, the healthcare provider) for risk management of medical devices interacting with an IT network.
- "Responsible organization" includes health-delivery organizations of all size, such as physician single and group practices, as well as hospitals, clinics, etc.
- For the objective of 80001 to be met, the "responsible organization" will need to work closely with medical device manufacturers and providers of information technology.

The AAMI has paved the way for healthcare IT staff to be able to reach out to medical device manufacturers directly and work on fine tuning the network performance of a given device. Some examples of this are highlighted in the use case section of this chapter. The organization continues to provide best practices for managing wireless medical devices in their publication *Biomedical Instrumentation and Technology*. In addition, the AAMI established the Wireless Strategy Task Force (WSTF) in 2013. The group, comprised of manufacturers, regulators, users of technology, and other interested parties—is developing educational resources and tools and sharing best practices to address wireless challenges in healthcare. Group priorities include clarifying roles and responsibilities in the wireless arena, managing spectrum to improve safety and security, designing wireless infrastructure for high reliability, learning from other industries, managing risk and preventing failure. The group released a special compilation of articles in 2013 entitled "Going Wireless", which is a great resource for anyone working with mobile medical devices (https://www.aami.org/hottopics/wireless/AAMI/Going_Wireless_2013.pdf).

There are many other organizations that can be mentioned in these sections, such as the National Institute of Standards and Technology (NIST), the Healthcare Information and Management Systems

Society (HIMSS) and its mobile initiative mHIMSS, and the federal government, but the last one that will be discussed is the Wi-Fi Alliance. The background of this organization was discussed in the introduction, but for the purposes of this chapter, it is important to note that the Wi-Fi Alliance has been instrumental in publishing guidelines for deploying, securing, and leveraging Wi-Fi in healthcare.

New wireless medical devices are a blessing; they can also be difficult to troubleshoot, as many large medical device manufacturers such as GE, Medtronic, Philips, Baxter, and CareFusion, are designing and adapting medical devices for use on unlicensed radio frequencies. Often, manufacturers will cut costs by using noncompliant or out-of-date wireless devices (adapters, bridges, etc.) embedded in the medical devices. This effort to reduce cost and to gain market share has been a growing challenge for network administrators in healthcare. From diagnostics and monitoring, to the operating theatre and managing patient medical records, demand on wireless technology is more complex and mission critical in the healthcare industry. As medical device manufacturers race to introduce new devices, in many cases they must adhere to HIPAA-HITECH requirements and the FDA's 510(k) approval process. Healthcare organizations often face a lack of central control over procurement because departments have their own budgets and purchasing power. As ubiquitous Wi-Fi is becoming a reality, it is increasingly challenging to manage existing and legacy wireless medical devices while continuing to drive forward and utilize the latest available technology. Often manufacturers will take shortcuts by introducing an add-on Wi-Fi integration using wireless bridges, or will opt to utilize lower-end, cheap wireless cards in their equipment. This makes managing wireless medical devices a challenge requiring a close working relationship between clinical engineering and IT.

When it comes to patient data, securing medical devices and their data is vital to providing safe and effective healthcare. As Wi-Fi is growing the risks associated with the technology are inherent and are becoming more lucrative for hackers to try and take advantage of. Some of these risks are associated with security, availability, quality of service (QoS), and privacy. As the healthcare industry continues to expand and enter the ever-growing wireless space, including patient monitoring equipment, physicians' PDAs and laptops, and wireless-enabled medical devices, the risks associated with their use also rise. Some healthcare organizations have stayed ahead by deploying secured wireless networks for their medical devices. They often have to tweak their network to accommodate nonstandard or legacy medical devices.

Different organizations and departments within the hospital often mandate the wireless medical devices to purchase. In order to avoid a chaotic situation, they must be required to utilize risk management techniques and to thoroughly test each and every device that is being proposed for deployment on the Wi-Fi network. If any of the devices cannot meet minimal security requirements, they need to be identified.

The rapid pace of wireless medical device procurement presents an opportunity to create a focused certification process for the wireless medical devices. The certification process entails thoroughly testing the wireless medical device, and clearly identifying clinical workflow and support expectations. The IT department and clinical staff can work together to create a detailed inventory of all the wireless medical devices deployed in the hospital. Once that is done an OLA (operational level agreement) and SLA (service level agreement) can be set up to describe the maintenance and support matrix for each type of device. Proper planning and design are important to ensuring that the wireless network will support certain devices. Healthcare institutions wishing to manage their wireless medical devices should develop a consistent process for onboarding devices as well as phases for bringing all of their wireless medical devices up to a minimal set of authentication and encryption requirements.

The current industry consensus is that the best practice for wireless medical device authentication and encryption is using 802.1x with EAP TLS and AES encryption. This enforces mutual authentication and requires each medical device to have an x.509 certificate installed before it is allowed onto the wireless network. Due to the wide spectrum of device wireless capabilities, it is often necessary to use a phased approach to manage wireless medical devices and promote ongoing authentication and encryption best practices. HIPAA advisory and wireless interoperability-certifying Wi-Fi Alliance has acknowledged that the typical 802.11 security features such as WEP and/or shared key authentication are not secured enough. The phases are outlined in the bullet points below:

- **Phase 1:** All medical devices that support a certain authentication and encryption should be configured to use a dedicated SSID, keeping the number of SSIDs as low as possible. This phase is targeted at minimizing the amount of wireless overhead traffic. IT and clinical engineering staff need to consolidate a detailed inventory of all wireless medical devices in the hospital. This should include the make and model of the device, network connectivity requirement, device classification, supported spectrum, and high bandwidth requirements. This process will provide more insight into which wireless medical devices are capable of handling and supporting certain authentication and encryption methods.
- **Phase 2:** The purpose of the medical device policies on the network is to ensure that each device is suited for its purpose and meets clinical and patient needs, to make sure that the device complies with safety and quality standards. Since medical devices are regulated by the FDA, their design and operation cannot be modified by the end user. For many years, device manufacturers have been responsible for the installation, service, and support of their devices, including the network. This has resulted in several small independent networks in the hospital. As wireless technology continues to expand, hospitals feel the increasing financial pressure to deploy medical devices on their existing enterprise network. Network policies need to be applied to limit medical device network access to required IP addresses.
- **Phase 3:** Continuously refresh medical devices that do not support WPA2 EAP TLS. This should eventually result in one SSID using EAP TLS.
- **Phase 4:** Implement EAP TLS. The complexity associated with deploying EAP TLS is dependent on whether the hospital has a PKI and a certificate authority in place. Building such a system can be an expensive undertaking.
- **Phase 5:** Develop an overall stringent wireless security policy for medical devices that is interdepartmental and ties into IT governance, security, and procurement. Part of the policy needs to be ongoing device certification as a part of onboarding.

The questions that should be posed when evaluating a new wireless device can be broken down into three test categories, functional, network, and failover/redundancy. In addition to these, a detailed risk assessment of the device should be clearly documented. The bullet points below can serve as a starting framework for each of these categories.

Functional Testing

The first series of tests are intended to validate that the wireless medical device being evaluated is IEEE compliant. The following should be validated as part of the test:

- Is the wireless-capable medical device designed to be mobile or stationary?
- Does the device operate in the unlicensed RF spectrum?
  - Is it IEEE 802.11a/b/g/n or any subset thereof compliant?
  - If not, what RF frequencies does it utilize?
  - Is it Wi-Fi certified?
  - What PHY rates are supported?
  - Is the wireless capability provided by a bolt-on bridge or an integrated wireless card?
  - What models of wireless card and chipset are used?
  - What is the average packet size transmitted, and the maximum latency and jitter requirement?
  - Does the wireless card on the device support "super frames"/frame aggregation (802.11n)?
- Is the device IEEE 802.11i compliant?
  - Is WPA2 encryption supported?
  - Does the device support 802.1X?
  - What types of EAP can the device support?
  - Can the device be added to a Windows domain within Active Directory?
- Is the device IEEE 802.11e compliant?
  - Does the device support WMM and/or WMM PS Mode?
  - What queue is recommended?
- Is the device IEEE 802.11r compliant?
  - Is fast secure roaming supported?
  - Is Opportunistic Key Caching supported?

  - Can the device firmware be updated as wireless authentication and encryption mechanisms evolve in the industry?

Network Testing

The tests/questions below are oriented toward understanding the impact of the proposed device on the wireless and the wired networks.

- Does the device support dynamic host configuration protocol (DHCP), or does it require a static IP address?
- What type of information is transmitted via the wireless medium?
  - Is it required for the device to be on the corporate wireless network?
  - What does the device need access to on the corporate network? Can you list all appliances and necessary TCP/UDP ports?
  - Does the device transmit ePHI (electronic protected health information)?
  - What is the network bandwidth requirement for the device?
  - Can the maximum transmission unit (MTU) size be manually modified on the device if needed?

Failover and Redundancy Test

- In the event that there is a disruption to the wireless network, what actions are taken by the device?
  - Does it support or provide a backup mechanism for transmitting data if needed?
  - Does it automatically try to retransmit the data once network connectivity resumes?
  - Does it have a password-protected administration mode for modifying network settings?
- If the device loses network connectivity, will it directly impact a life-sustaining ongoing process or procedure?
- Does the device support removable storage media?
  - Is USB or Firewire supported?

- Does the device have an accessible/removable hard drive?
- Does the device store ePHI on removable media?

The IEC 800001 standard clearly outlines a process for assessing the risk of using a given medical device on the network. Some of the areas that need to be clearly understood are things that can go wrong with the device resulting in unintended consequences. A risk acceptability matrix should be created for each wireless medical device being introduced to the network.

Wireless medical devices have gone through several design iterations, some of which are still around. WMTS and personal area networks are a few of the wireless technologies in use, but Wi-Fi seems to be the one medium that will last. The bandwidth available is significantly higher than any of the other wireless technologies. Cellular providers, who were against leveraging Wi-Fi by dropping their traffic locally onto corporate networks have been feeling the bandwidth crunch and are now fully supportive of Wi-Fi offloading.

In the next section the use cases with various types of medical devices, observations, and lessons learned are based on real-world experiences.

Mobile X-Ray Machines

Mobile x-ray machines are one of the first types of devices that have taken advantage of the wireless network to transmit images to a central server. These devices can be wheeled into patient rooms, and can be used to provide on-demand x-rays at the bedside. This is a significant workflow improvement over the older dedicated room with an x-ray device. In the early 1990s, it would often take a physician several hours to have a patient wheeled to the x-ray room and then have the final x-ray print in hand. Mobile x-ray devices can cut that process down to less than half an hour. These units can often be bulky, and they are fitted with a lead apron, motorized wheels, and often have an Ethernet connection as a backup way to upload x-ray films (Figure 6.1).

From a network traffic perspective, this type of device can be demanding on the wireless network due to the size of the files that need to be transmitted. These can be several megabytes large.

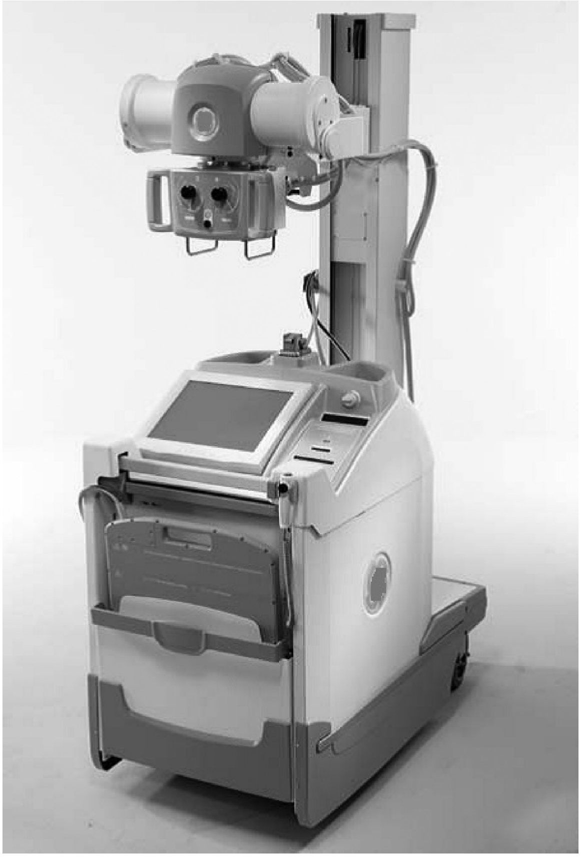


Figure 6.1 Example of a mobile x-ray machine.

Evaluating one such device by a prominent medical device manufacturer led to the following obervations:

1. The device had a built-in wireless card installed into the card rack of the computer in the bottom of the chassis. The signal output is set to its maximum setting and is not adjustable from the software. The wireless antenna is located under the top cover, below the LCD screen, and is vertically polarized.
2. Due to its poor wireless design, the positioning of the cart and its orientation relative to nearby access points significantly impacts its receiver sensitivity. The card has a stronger signal when the LCD screen is facing the nearest access point. The device does not support AES encryption but rather reverts to TKIP.

3. While rolling the mobile x-ray device around various parts of the hospital, it was noted that the roaming aggressiveness of the device is fairly low, which tends to cause the cart to roam very poorly. In effect, the x-ray device roams when the signal from the access point it is associated to becomes unusable, which tends to make the roaming process choppy.
4. The device does not have a wireless survey mechanism to assist IT professionals in determining the RSSI values that the device is detecting.

Medication Dispensing Systems

Medication dispensing units are generally used to securely store and tighten control over medication in hospitals. They also help manage errors associated with delivering the appropriate medication to the right patient. These can be found in various areas throughout the hospital ranging from inpatient floors to the intensive care unit and operating rooms. Generally, these resemble a large chest with drawers, with an imbedded or overlay monitor, with an integrated barcode scanner and sometimes a printer. Some of the newer iterations are smaller and feature Wi-Fi connectivity, but the nature of the device demands adequate storage space.

The reasoning behind using Wi-Fi to provide network connectivity is to avoid having to run a dedicated Ethernet cable for the device. Although this sounds great in theory, one needs to factor in the other devices utilizing the shared wireless medium, and the true necessity for the drug dispensing unit to be mobile.

Evaluating one such device by a prominent medical device manufacturer led to the following observations:

1. Although the device had an integrated wireless card, it required connection to an AC power outlet to function. This requirement limits the mobility of the device, and makes one question whether it truly needs to be on the wireless network.
2. These carts are generally left in one area, and can easily use a wired Ethernet connection, freeing up valuable wireless bandwidth.
3. If there is a strong enough demand for these devices to utilize the wireless network, it is essential to certify the functionality

> of the device on a given network. We ran into an issue where one of these devices did not properly support opportunistic key caching, and was running dated wireless drivers.

Due to their typical use case, it is more cost effective in the long run to plan to have wired connectivity for these devices as opposed to having them utilize the Wi-Fi network.

IV Pumps

The invention of the wearable intravenous (IV) infusion pump by Dean Kamen in the 1970s was a major catalyst for medical device engineers to start looking into ways to keep these types of medical devices connected to the network while being mobile. Infusion pumps can be used in scenarios ranging from basic hydrations to blood transfusions, or efficient delivery of medicines.

IV pumps (Figure 6.2) are one of the most heavily deployed wireless medical devices within hospitals and hospital systems. Their small form factor and modular design make these ideal for mobility. The Wi-Fi capability built into these types of devices ranges based on how well the unit was designed to be mobile. Some IV pumps that were released in the early 2000s are unable to support WPA2 (AES

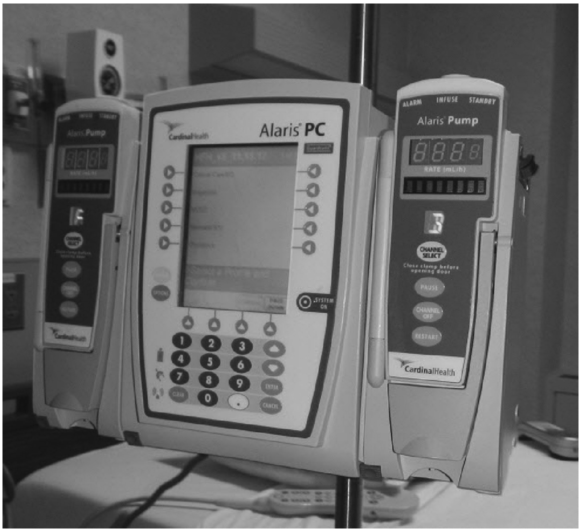


Figure 6.2 IV pump.

encryption), but newer models can support most forms of authentication and encryption. The network is utilized as a means of collecting and trending data from a given pump as well as a way to keep drug libraries up to date on a given pump. When dealing with multicampus or global wireless network deployments that rely on centralized controller architecture, it is important to understand the data set dependencies per site. For example, even if two different hospitals have access points that are hosted on a given controller, it is sometimes necessary to provision unique VLANs for each to ensure that the pumps at each hospital receive their intended drug library/data set.

The wireless hospital system where the following observations were made is a fairly large system, which had approximately 2000 wireless IV pumps. These were distributed among the various hospitals and ranged from 900 at one site down to a handful at some of the smaller clinics. The pumps relied on a built-in wireless card which behaved very similarly to a Wi-Fi card on a given laptop. Earlier releases of code had issues with WPA2 encryption, but this was quickly corrected with a firmware update. The pumps have worked very smoothly and are very conservative in their bandwidth utilization. Furthermore, the wireless connectivity does not impact the core fluid pumping functionality of these devices. One of the key observations when dealing with these types of pumps is the necessity for a detailed inventory, ensuring that they are under maintenance and are running the latest firmware, and that the wireless network is able to provide high-level location tracking for these devices.

The largest hurdle when dealing with wireless IV pumps is revisiting the wireless network architecture to ensure that it can accommodate the drug library/data set push to each pump.

One topic that was touched upon in an earlier chapter is Real-Time Location Services (RTLS). This plays a significant role in the IV pump inventory and workflow management. It makes it easier to ensure that each IV pump is cleaned between uses rather than being moved from one room or floor to the next without any formal reconditioning and cleaning. Many hospital systems lose track of the locations of their IV pumps and start renting these devices at an astronomical monthly cost. With a finely tuned RTLS system, these recurring expenses can be eliminated.

Electrocardiogram Carts

Electrocardiogram (ECG) carts are often part of a larger system managed by the cardiology department. These can have a mobile form factor that can be rolled into a patient room and used for cardiac tests at the bedside. These are typically comprised of a mobile cart and several cardiac leads (Figure 6.3).

The model discussed here is manufactured by one of the largest medical device companies in the world, so some of the observations are quite alarming. The ECG device we were asked to bring onto the wireless network had some unique requirements which are puzzling to this day. These units do not have a built-in wireless card, but rather rely on a bolt-on wireless bridge. The bridge is a stand-alone device which is configured independently of the ECG device. It connects to the Ethernet port on the device with the intent of tricking the system into believing that it is connected to a wired network jack. The unique

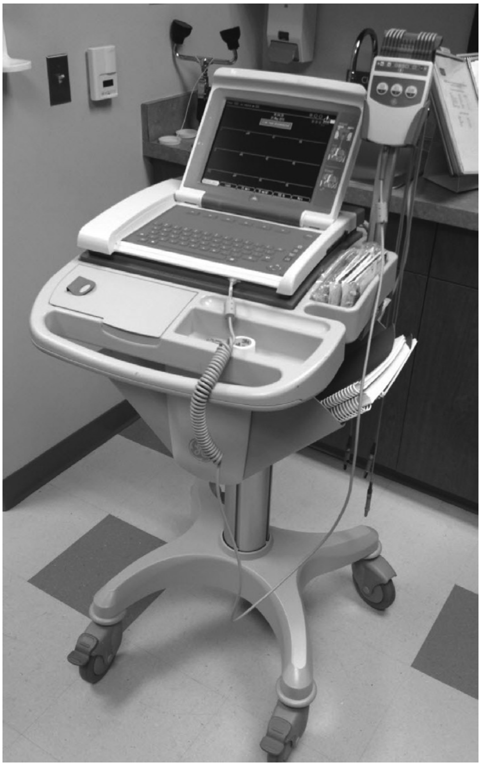


Figure 6.3 ECG cart.

requirements were for a reserved DHCP IP address, or a static IP address per device. It was also brought to our attention that the device does not support AES encryption, but rather supports TKIP.

The lack of support for AES can be addressed with a firmware upgrade, but the requirement that stood out was the IP addressing requirement. Any engineer who has worked in a large-scale environment understands that different intermediate distribution frame (IDF) closets on different floors of a facility can sometimes require different VLANS for capacity planning. This means that a device with an IP address on one floor cannot seamlessly roam to a different floor unless the same VLAN spans both floors. The wireless space is no different. If a client receives an IP address from an access point on one controller, it cannot seamlessly roam to an AP on a different controller without creative network architecture. In the case of the ECG devices, this means that they can only function in certain geographic areas and cannot roam throughout the hospital. The word "static" IP address should throw up a red flag when one is working on mobility.

Ultrasound Devices

Mobile ultrasound devices come in various shapes and sizes depending on their intended use. These range from a handheld tablet to dedicated workstations on wheels (Figure 6.4). The form factor is in part dependent on the function of the device and its required signal-processing capability. These devices provide clinicians with the ability to view subcutaneous activities ranging from potentially damaged organs to cardiac issues, and viewing the fetus in expectant mothers. All of these units rely on introducing high-frequency acoustic energy, and analyzing the return signals to generate images. They generally rely on dedicated transducers to analyze and digitize the return signals. The higher resolution units are generally not battery friendly, hence the onboard battery units. Portable units sacrifice performance for a longer battery life. From a mobility standpoint, both types can be integrated onto Wi-Fi networks. The size of the images and videos captured can range from several megabytes for high-resolution images to a dozen or more megabytes for videos. Historically these units have featured removable memory media for storing images, which can be used to transfer images. With growing

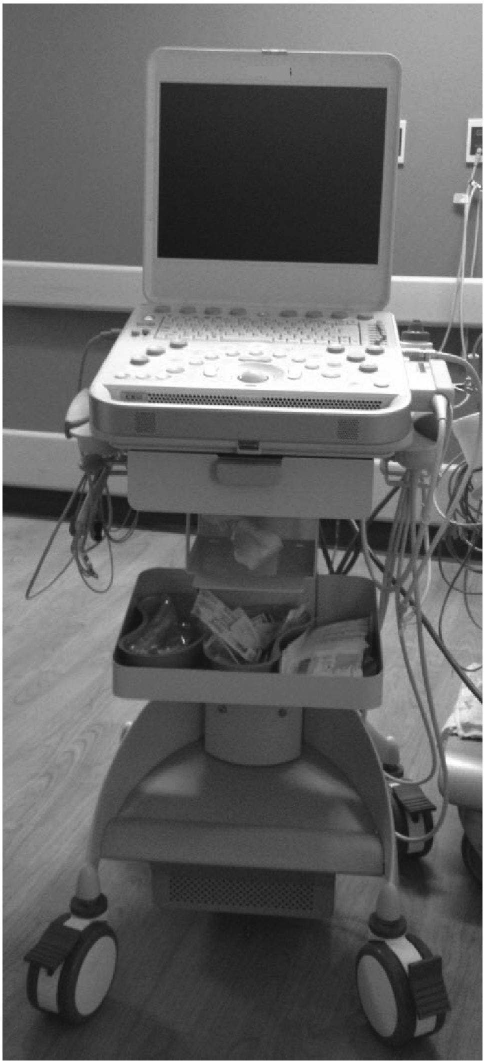


Figure 6.4 Mobile ultrasound machine.

patient privacy concerns, the newer devices have removed this capability, and only allow buffering capability in the event that network connectivity is lost. These devices rely on a central storage server for categorizing and storing images.

Different departments in the hospital deploy a preferred form factor based on their needs. A cardiac or a prenatal ultrasound device is generally integrated into a larger mobile cart with several dedicated transducers. The ER department hosts a variety of these to meet the various needs. The larger units have the same limitation as other mobile medical devices. They rely on wireless bridges or USB wireless cards. These pose a challenge for seamless roaming. The devices manufactured in the last 3 to 5 years host integrated wireless cards. The combination of old and new devices imposes a significant support burden on IT and clinical engineering. The tablet form factor devices integrate more readily and are easier to support with their integrated IEEE 802.11 a/b/g/n and 802.11i support. These can be used as a first line of diagnosis, but to avoid liabilities the testing is supplemented with the higher end units capable of more advanced signal processing.

A variety of handheld ultrasound devices have been introduced since 2010. These will be discussed in more depth later in the chapter, but many hospitals are starting to rely on these in place of the traditional stethoscope. A growing number of physicians are relying on these devices at the bedside to augment the ability of the traditional stethoscope. They have proven to be more effective for diagnosing conditions like pneumonia. With the proliferation of smart phones and tablets, these devices are beginning to rely on these form factors. There is still much work and research to be done in order to standardize these devices.

Blood Gas Analyzers

Blood gas analyzers range from benchtop to portable units, but they all perform the function of measuring base status, ventilation, and arterial oxygenation. The unit in this use case was designed to be mobile on a dedicated cart (Figure 6.5).

It did not have a wireless card and we managed to work with the vendor to migrate the device from relying on a wireless bridge to having a nano-USB based 802.11 b/g wireless card. Ultimately, the device will need to be transitioned to the 802.11a network to free up capacity in the 2.4-GHz space.

Hemodialysis Machines

In the hemodialysis machine space, a growing trend is to leverage the same device for patient entertainment as they undergo a procedure

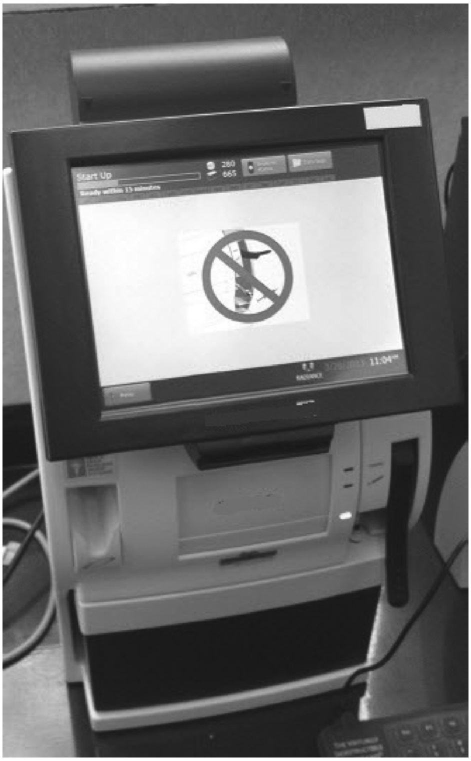


Figure 6.5 Blood gas analyzer.

that can take several hours. Devices that are prevalent in dialysis centers are about the size of an ATM machine with an onboard PC (Figure 6.6). Patients can use the PC portion of the device to access the Internet.

More than 400,000 Americans receive dialysis, about half of them over age 65. More than 90 percent go to dialysis centers for professional care, but the home dialysis options are beginning to take root, which is prompting some interesting, portable form factors. These units are fairly invasive, and require fine-tuning, so many patients shy away from them.

PC and dialysis functionality are logically separated, with the PC relying on Wi-Fi while the hemodialysis device leverages a serial interface. Data is not correlated to a specific patient until it reaches a central data repository. The Wi-Fi capability on these machines is required for the onboard PC, which typically runs a standard operating system like Windows XP, or Windows 7 with an integrated

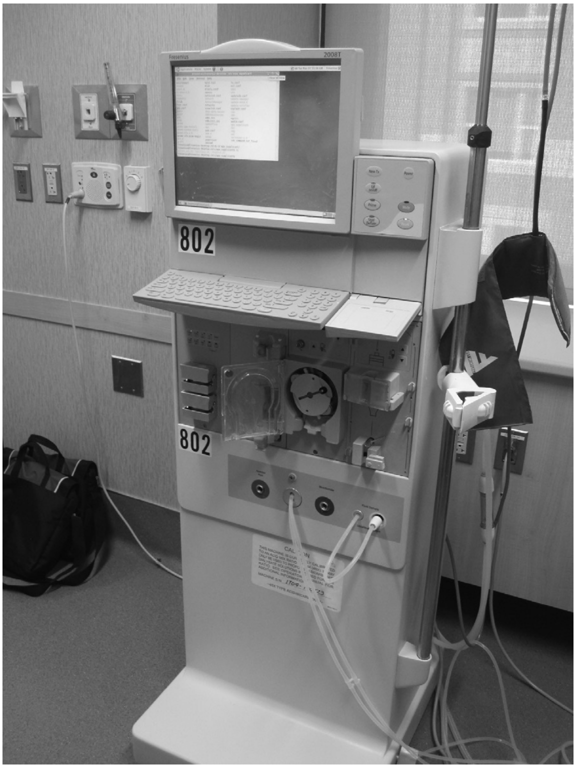


Figure 6.6 Hemodialysis machine.

wireless card. The card is fairly flexible from a configuration standpoint, and tends to roam as well as wireless cards that are found in a typical laptop device.

mHealth

With the growing focus on the empowered patient, many of the devices covered in this chapter are becoming increasingly mobile. Dr. Erik Topol, a pioneer in this space, demonstrated the power of the technology during a keynote address at the HIMSS conference in 2013 in New Orleans. Ironically, he put the AliveCor Heart Monitor, one of his showpieces, to use on a fellow passenger in distress shortly after his talk. When we combine the capabilities of some of these devices to help patients become more aware of their health with the growing trend of patients being able to review their medical records via cloud-enabled portals, it becomes clear where the technology is headed. The challenge for medical device manufacturers is to leverage authentication and accounting as well as provide a secure means of transferring this type of data to physicians. This trend has the potential to change patient care as we know it. Interestingly enough, a recent survey by Harris Interactive revealed that doctors are not supportive of full transparency. A survey of 3,700 doctors in eight countries showed that only 31 percent believe that patients should have full access to their own medical records via electronic means. The majority of those surveyed, some 65 percent, supported restrictive access. One can empathize with these results given that the vast majority of patients are not qualified to fully understand the results. What may appear to the patient as a major issue can sometimes be an anomaly, and only a trained physician can make the distinction. If one compares this to an adage in IT, this can be likened to someone reading a packet capture and analyzing it, and arriving at a root cause of a network issue.

With the leaps in artificial intelligence and the computational capabilities in line with Moore's law are enough to make one take a step back and ponder the future of patient care. After all, Watson, the IBM supercomputer has taken up healthcare. With the ballooning, unsustainable costs of healthcare, it may be these types of technologies that can help remold this field and make it sustainable. There is no denying that the per capita spending has little correlation to increased life expectancy. With a heavy focus on wellness, it is conceivable that mHealth applications will play a major role in allowing patients to assist in regulating their own health by becoming increasingly aware of their health.

The challenge to IT as portable mobile medical devices become more prevalent is to ensure that all relevant security guidelines are followed and to prioritize traffic appropriately based on applications rather than device types. If this is not managed properly, there could be a negative impact on patient care.

One area that is disturbing is our growing dependence on smart phones and tablets, and an augmented reality approach with a dependence on a smaller form factor will be a breath of fresh air.