ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A FRAMEWORK FOR MONITORING BLOOD PRESSURE OF PATIENTS IN THE RURAL AREA USING INTERNET OF THINGS TECHNOLOGY

[1]DR. MODESTA .E. EZMA, [2]MR. CELESTINE .I.UGWU

[1]lecturer I ., Department of Computer Science University of Nigeria Nsukka

[2]Technologist Department of Computer Science University of Nigeria Nsukka

E-mail: [1]modesta.ezema@unn.edu.ng, [2]celestine.ugwu@unn.edu.ng

ABSTRACT

The convergence of multiple technologies, ranging from wireless communication to the internet and embedded systems, such as wireless sensor network, control system and automation gave rise to the internet of things (IoT). The application of IoT in healthcare system, typically use sensors enabled devices to assist in remote health monitoring. This health monitoring devices can range from blood pressure and heart bit monitors to advanced devices capable of monitoring specialized implants. In this paper we have proposed a framework for monitoring blood pressure of patients in the rural area using Internet of Things technology. We also discussed the background of IoT technology, application areas of Internet of Things technology, Internet of Things communications model, an overview of enabling communication and cooperation technologies for the IoT and issues in IoT.
Keywords: *Internet of Things, Sensor, Heart, Health Network*

1. INTRODUCTION

The steady advances in microelectronics, communications and information technology witnessed in recent years have revolutionized the internet and gave rise to what we call internet of things (IoT). The internet of things sometimes refer to Internet of Objects generally refer to scenarios where network connectivity and computer capability extends to object, sensors and everyday items not normally considered computers, allowing this devices to generate, exchange and consume data with minimal human intervention[1]. Consumer products, durable goods, cars and truck, industrial and utility components, sensors and everyday object are being combined with internet connectivity and powerful data analytic capabilities that promise to change the way we work, live and play [1]

Although military tactical communication is still considered the primary application for ad-hoc networks, commercial interest in this type of networks continues to grow. Applications such as rescue mission in times of natural disaster, law enforcement operation, commercial, educational and health use of sensor network, personal area networking are just a few possible commercial examples. Internet of Things technology has the potential of addressing some technological challenges in the area of healthcare and management in the rural areas where there is no internet availability. This technology is embodied in a wide spectrum of

networked product, system and sensors, which take advantages of advancement in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previous possible.

Personal IoT devices like wearable fitness and health monitoring devices and networked enabled medical devices are transforming the way healthcare services are delivered. This technology promises to be beneficial to people living in rural areas of developing countries, enabling improved level of independency and quality of life at reasonable cost [1].

In this paper we present a detailed framework for monitoring blood pressure of patients living in the rural area of developing countries using Internet of Things technology. IoT, because of its ubiquitous sensors and connected system, will provide health authorities with more health information and control in other to identify and fix high blood pressure related problems among those in the rural area. IoT can significantly improve quality of life for the surging number of elderly people [2]. For example, imagine a small wearable device that can detect a person’s vital signs and send alert to a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

health care professional when a certain threshold has being reached or sense when a person has fallen down and can't get up. The proposed blood pressure monitoring device for those in the rural area is expected to be powered by solar energy when the blood pressure is high the information is pushed out to the individual concerned and even to the medical personnel connected for immediate treatment, this has a lot of advantages ; 1. It does not depend on the electricity for the device to function 2. It operates at a reduced cost 3. The life of the individual involved is saved. This paper is organized as follows. Section II presents background information on Internet of Things technology. Section III gives a brief description of the proposed framework. Section IV briefly presents applications areas of IoT technology. Section V briefly presents t IoT communications models. Section VI gives an overview of enabling communication and cooperation technologies for the IoT. Section VII presents issues in Internet of Things. Section VIII gives conclusions.

2. INTERNET OF THINGS - BACKGROUND

The term Internet of Things was first used in 1999 by British technology pioneer, Kelvin Ashton to describe a system in which objects in the physical world could be connected to the internet by sensors [1]. Ashton coined the term to illustrate the power of connecting radio frequency identification (RFID) tags used in corporate supply chains to the internet in order to count and track goods without the need for human intervention. In 2009, a dedicated EU commission action plan ultimately saw the Internet of Things as general evolution of the internet "from a network of interconnected computers to a network of interconnected objects" [3]. According to [1], from the technical point of view the Internet of Things is not the result of a single novel technology; instead several complementary technical developments provides capabilities that taken together help to bridge the gap between the virtual and physical world, this capabilities include communication and cooperation among objects and the internet addressability of objects in the internet , unique identification of objects , sensing ability of objects , actuation ability of objects , embedded information processing , localization and user interface of smart objects. In [1], confluence of several technologies and market trends is making it possible to interconnect more and smaller devices cheaply and easily. These include ubiquitous connectivity , wide spread adoption of IP- based networking, computing economics, miniaturization, advances in data analytics and rise of cloud computing. Currently, sectors such as healthcare, manufacturing, automotive, home and consumers electronics among others are considering the incorporation of IoT technology potentials into their products, services and operations [1]. The International Telecommunication Union (ITU), described Internet of Things as a global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communication technologies [4]. According to Internet Architecture Board (IAB), Internet of things denotes a trend where a large number of embedded devices employ communication services offered by the internet protocol [5]. Many of these devices often called smart objects are not directly operated by humans, but exist as components of buildings or vehicles, or are spread out in the environment.

3. THE PROPOSED FRAMEWORK

High Blood Pressure (High BP) is a common disease condition in the rural area that often result to stroke or other ailments which can lead to death. In this section, we describe the proposed framework for monitoring the blood pressure of patients in the rural area using Internet of Things technology. Timely and accurate data is necessary to ensure urgent provision of healthcare services for patients in the rural area. Patients to be monitored have on-body blood pressure monitors (BPMs) that were interfaced with wireless sensor node. The sensor node control the BPM to initiate a reading, then collect the data and forward raw and processed data to healthcare servers over GPRS enabled sink (base station). Additional nodes (router node) are required to pass the data to the base station. These sensor nodes use Bluetooth or ZigBee technology for the transportation of data. Every village in the area has at least a sink or base station depending on the size of the village. Each router node in the network has a fixed location and its function is enabling prompt data transfer to the next router node or base station. Sinks can be connected to the healthcare servers over GSM telephony. The healthcare servers store the real time and historic data, detect the user defined events and issue notifications about these events. The user can query the data stored on the servers, including raw and processed data, either locally or remotely over the Internet. This can be achieved by querying the data from PDA or a smart phone connecting directly to the servers. Thus, Wireless Sensor Networks (WSNs) are highly relevant to this research domain, as they allow both real time and long-term blood pressure monitoring of patients.

4. APPLICATION AREAS OF INTERNET OF THINGS TECHNOLOGY

At present, a wide range of industry sectors – including automotive, healthcare, manufacturing, home and consumer electronics, and well beyond -- are considering the potential for incorporating IoT technology into their products, services, and operations [6]. The McKinsey Global Institute describes the broad range of potential applications in terms of "settings" where IoT is expected to create value for industry and users.

Table 1 Settings For Iot Applications

"Settings" for IoT Applications		
Setting	**Description**	**Examples**
Human	Devices attached or inside the human body	Devices wearables and ingestibles) to monitor and maintain human health and wellness; disease management, increased fitness, higher productivity
Home	Buildings where people live	Home controllers and security systems
Retail Environments	Spaces where consumers engage in commerce	Stores, banks, restaurants, arenas – anywhere consumers consider and buy; self-checkout, in-store offers, inventory optimization
Offices	Spaces where knowledge workers work	Energy management and security in office buildings;improved productivity, including for mobile employees
Factories	Standardized production environments	Places with repetitive work routines, including hospitals and farms; operating efficiencies, optimizing equipment use and inventory
Worksites	Custom production environments	Mining, oil and gas, construction; operating efficiencies, predictive maintenance, health and safety
Vehicles	Systems inside moving vehicles	Vehicles including cars, trucks, ships, aircraft, and trains; condition-based maintenance, usage-based design, pre-sales analytics
Cities	Urban environments	Public spaces and infrastructure in urban settings;adaptive traffic control, smart meters, environmental monitoring, resource management Outside Between urban environments (andoutside other settings)Outside uses include railroad tracks, autonomous
Outside	Between urban environments (and outside other settings)	Outside uses include railroad tracks, autonomous vehicles (outside urban locations), and flight navigation; real-time routing, connected navigation, shipment tracking

5. INTERNET OF THINGS COMMUNICATIONS MODELS

The Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects which outlines a framework of four common communication models used by IoT devices [1]. These communication models are:

5.1 Device-to Device Communication
The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. Often, however these devices use protocols like Bluetooth [7], Z-Wave [8], or ZigBee [9] to establish direct device-to-device communications.
5.2 Device-to-Cloud Communication
In a device-to-cloud communication model, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service.

5.3 Device-to-Gateway Model
In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and the cloud service and provides security and other functionality such as data or protocol translation.

5.4 Back-End Data-Sharing Model
The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. This architecture supports "the [user's] desire for granting access to the uploaded sensor data to third parties". This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where "IoT devices upload data only to a single application service provider''.51 A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed.

6. ENABLING COMMUNICATION AND COOPERATION TECHNOLOGIES FOR THE IOT- OVERVIEW

Objects have the ability to network with Internet resources or even with each other, to make use of data and services and update their state. Wireless technologies such as GSM and UMTS, Wi-Fi, Bluetooth, ZigBee and various other wireless networking standards currently under development; particularly those relating to Wireless Personal Area Networks (WPANs) are of primary relevance here.

6.1 Sensor Node

Sensors are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure [10]. Sensors measure physical data of the parameter to be monitored. The continual analog signal produced by the sensors is digitalized by an analog-to-digital converter and send to controller for further processing [8]. A sensor should be small in size and can be embedded into an object, sensors are classified into three categories namely passive Omni –directional sensors, passive narrow beam sensors and active sensors, passive sensor sense the data without actually manipulating the environment by active probing while active sensor actively probe the environment. Each sensor node has a certain area of coverage for which it can reliably and accurately report, the particular quality that it is observing. As a result of the small size of sensor, it can only be equipped with a limited power source of less than 0.5 to 2 ampere/hour and 1.2 to 3.7volts. Several sources of power consumption in sensors are signal sampling and conversion of physical signals to electrical ones, signal conditioning and analogue to digital conversion

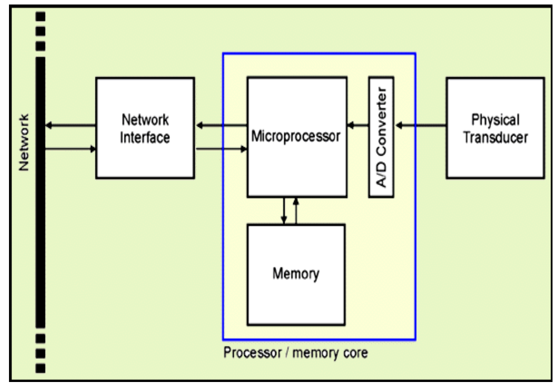

Fig.1, Sensor Node

The main components of a sensor node are a microcontroller, transceiver, external memory, power source and one or more sensors.

6.1.1 Microcontroller/Microprocessor

The controller processes data and controls the functionality of other components in the sensor node. In wireless sensor network, the wireless communication is of modest, i.e., simple, easy to process modulation and the signal processing tasks of actual sensing of data is less complicated

6.1.2 The Transceiver

The transmitter and receiver are combined into a single device known as transceiver. Transceiver often lack unique identifiers. The operational states are transmit, receive, idle and sleep. Current generation transceivers have built-in state machine that perform one operation automatically. Sensor node often makes use of ISM band, which gives free radio spectrum allocation and global availability. The possible choices of the wireless transmission media are radio frequency (RF), optical communication (laser) and Infrared

6.1.3 The External Memory

Memory requirement are very much application dependent. The most relevant kinds of memory are on-chip memory of a microcontroller and flash memory. Flash memories are used due to their cost and storage capacity. . Two categories of memory based on their purpose of storage are user memory used for storing applications related or personal data and program memory used for programing the device. Program memory also contains identification data of the device if present.

6.1.4 The Power Source

Power is stored either in batteries or capacitors. Batteries both rechargeable and non-rechargeable are the main source of power supply for sensor node, a wireless sensor node is a popular solution where it is difficult or impossible to run a main supply to the sensor node, since the wireless sensors are often placed in a hard-to-reach location, changing the batteries regularly can be costly or inconvenient. An important aspect in the development of a wireless sensor node is ensuring that there is always adequate energy available to power the system.

6.2 Global System For Mobile Communication (GSM)

GSM is a standard developed by the European Telecommunications Standard Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile phones. 2G networks developed as a replacement for first generation (1G) analog cellular networks, and the GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony. This expanded over time to include data communication, first by circuit-switched transport, then by packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution or EGPRS). GPRS Core Network is the optional part which allows packet-based Internet connection. GSM uses General Packet Radio Services for data transmission like browsing the web. One of the key features of GSM is the Subscriber Identity Module, commonly known as SIM card. This SIM is a detachable smart card containing the user's subscription information and phone book. GSM is one of the wireless technologies that enable Internet of Things.

6.3 General Packet Radio Services (GPRS) Technology

General Packet Radio Services is a radio technology for GSM networks that adds packet-switching protocol, shorter set-up time for ISP (Internet Service Provider) connections and offers the possibility to be charged by amount of data sent rather than connect time. It is a new bearer service for GSM that greatly improves and simplifies wireless access to packet data network. GPRS applies packet radio principle to transfer user data packets in an efficient way between mobile stations and packet data networks. The packet –based wireless communication service promises data rate from56 up to 114kbps and continuous connection to the Internet for mobile and computer users.

6.4 Bluetooth Technology

Bluetooth is a telecommunication industry specification that describes how mobile phones, computers and other digital devices can be easily interconnected using a short range wireless connection. Bluetooth requires that a low cost transceiver be included in each device. It operates in the globally available unlicensed ISM (industrial, Scientific, medical) frequency band at 2.4 GHz and applies frequency hopping for transmitting data over the air using a combination of circuit and packet switching [11]. The Bluetooth wireless technology is a low cost radio frequency that was created to solve a simple problem: replace the cable used by digital devices with radio frequency waves.

6.5 Wireless Networking Protocol: The IEEE 802.11(Wifi)

IEEE 802.11 is the wireless way to handle networking. It is a standard protocol used in wireless networking. It is also known as WiFi(Wireless Fidelity)with simplicity as a general advantage. Digital devices can be connected anywhere in homes or offices without the need for wires, rather, they are connected to the network using radio signals with a distance of up to 100 feet apart. This feature attracts IoT applications to be built on top of WiFi-Direct to get benefit from the speed of WiFi while they experience lower latency.

7. INTERNET OF THINGS ISSUES

While the possible applications and scenarios outlined above may be very interesting, the demands placed on the underlying technology are substantial [3]. In addition to the expectation that the technology must be available at low cost if a large number of objects are actually to be equipped, we are also faced with many other challenges, which among others include:

7.1 Security

While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be a fundamental priority. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

daily lives. Poorly secured IoT devices and services can serve as potential entry points for cyber-attack and expose user data to theft by leaving data streams inadequately protected [1].

7.2 Interoperability/ Standards

Since the world of physical things is extremely diverse, in an Internet of Things each type of smart object is likely to have different information, processing and communication capabilities. Different smart objects would also be subjected to very different conditions such as the energy available and the communications bandwidth required. However, to facilitate communication and cooperation, common practices and standards are required. This is particularly important with regard to object addresses. These should comply with a standardized schema if at all possible, along the lines of the IP standard used in the conventional Internet domain [3]. Appropriate standards, reference models, and best practices also will help curb the proliferation of devices that may act in disrupted ways to the Internet [1].

7.3 Privacy

The full potential of the Internet of Things depends on strategies that respect individual privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users, but concerns about privacy and potential harms might hold back full adoption of the Internet of Things. This means that privacy rights and respect for user privacy expectations are integral to ensuring user trust and confidence in the Internet, connected devices, and related services[1].

7.4 Power supply

Things typically move around and are not connected to a power supply, so their smartness needs to be powered from a self-sufficient energy source. Although passive RFID transponders do not need their own energy source, their functionality and communications range are very limited. In many scenarios, batteries and power packs are problematic due to their size and weight, and especially because of their maintenance requirements. Unfortunately, battery technology is making relatively slow progress, and "energy harvesting", i.e. generating electricity from the environment (using temperature differences, vibrations, air currents, light, etc.), is not yet powerful enough to meet the energy requirements of current electronic systems in many application scenarios [3].

8. CONCLUSION

In this paper we have described a framework that is based on Internet of Things that can be employed in the monitoring of blood pressure of patients in the rural area of developing countries. IoT, because of its ubiquitous sensors and connected system, will provide health authorities with more health information and control in other to identify and fix high blood pressure related problems among those in the rural area with a view of improving the quality of their lives. The challenges are as follows; Since the patients are in the remote areas it may not be easy for the connected physician in the IoT to get to the patience before the impending dome due to logistics like bad road, e.tc. While the potential ramifications are significant, a number of potential challenges may stand in the way of this emerging technology, particularly in the areas of security; privacy; interoperability and standards etc. The Internet of Things is happening now, and there is a need to address its challenges and maximize its benefits while reducing its risks.

REFRENCES:

[1] Marsan C. "The Internet of Things: An Overview" *report-InternetofThings-20151015* https://www.internetsociety.org
[2] Evans D. "The Internet of Things How the Next Evolution of the Internet Is Changing Everything "Cisco IBSG © 2011 Cisco and/or its affiliates. http:/www.cisco.com/go/ibsg
[3] Mattern F. and Floerkemeier C. "From the Internet of Computers to the Internet of Things" http://vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf
[4] "Overview of the Internet of Things." ITU, June 15,2012. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060
[5] RFC 7452, "Architectural Considerations in Smart Object Networking" (March 2015).Availat https://tools.ietf.org/html/rfc7452
[6] Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, June 2015. P.3. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world
[7] http://www.bluetooth.com and http://www.bluetooth.org

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[8] http://www.z-wave.com
[9] http://www.z-wave.com
[10] "Sensor node" Wikipedia, The Free Encyclopedia .Available at htp://en.wikipedia.org/wiki/Sensor_node
[11] Cali F., Conti M., Gregori E. (2000), "Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit", IEEE/ACM Transactions onNetworking 8 (6) 785–799.