Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 6183732, 11 pages
https://doi.org/10.1155/2018/6183732

Research Article

Framework for E-Health Systems in IoT-Based Environments

Maruf Pasha and Syed Muhammad Waqas Shah

Department of Information Technology, Bahauddin Zakariya University, Multan, Pakistan

Correspondence should be addressed to Maruf Pasha; maruf.pasha@bzu.edu.pk

Received 30 October 2017; Revised 14 January 2018; Accepted 4 February 2018; Published 7 June 2018

Academic Editor: Yin Zhang

Internet of things technology consists of physical objects that are accessible via the Internet, for example, devices, vehicles, and buildings. Internet of things technology is used to connect these physical objects by utilizing the existing infrastructure of networks. A unique identifier is assigned to identify the objects in IoT environments. Internet of things technology is used to make productive decisions on the sensed data after converting it into information. IoT technology is being used in various life disciplines, such as smart health services delivery, smart traffic management, border management, and governmental control. There is no single standard for IoT technology; thus, interoperability between IoT devices that use different protocols and standards is required. This research was carried out to provide and develop a specialized framework for an IoT-based smart health system by focusing particularly on interoperability problems. Based on different technology standards and communication protocols, the specific requirements of the IoT system were analyzed and served as a basis for the design of the framework. The protocols and standards within the framework utilize existing web technologies, communication protocols, and hardware design. This approach ensures that the specific expectations of the proposed model can be fulfilled with confidence. The experiments showed that interoperability between different IoT devices, standards, and protocols in a smart health system could be achieved using a specialized gateway device and that different web technologies could be used simultaneously in constrained and Internet environments.

1. Introduction

Many physical objects such as devices, vehicles, edifices, and other objects are used in traditional network infrastructure to define the Internet of things [1]. IoT technology uses the preestablished infrastructure of networks to ensure its validity. Many popular smart devices are utilized widely, including smart phones, tablets, and sensor-equipped devices [2]. Sensors in smart phones include the accelerometer, gyro, and proximity sensors. The acceleration of a body and the change in rotational angle are measured by using accelerometer sensors, the detection of nearly placed objects is measured with a proximity sensor, and body positioning is measured by GPS technology. IoT objects can be identified by using RFID tags [3]. The application list for uses of IoT technology is increasing day by day. There is also a research-based prediction that by the end of 2020 there will be 36.5 billion wireless connections, and 70% of wireless connections will consist of sensor devices while 30% will be without sensors [4].

Various IoT projects encourage the use of IoT technology, including body applications, the smart home, the smart city, and smart environment projects. In the smart home, protection and automation projects are involved. To create the smart environment, pollution, weather, earthquake and tsunami detection, and monitoring projects have been initiated. Smart city projects include smart transportation, country border security, electronic governance systems, smart city supply chain management, and grid station monitoring [5]. Due to the extensive use of IoT technology in every single field of life, its use in the health sciences is also natural. Therefore, different IoT-based smart health services projects are being initiated worldwide. Various types of smart health services are being provided to the public. These may include the following: remote monitoring of patient health, patient handling in an emergency, medication and routine health checkup reminders, remote patient prescriptions, and searches for the nearest health resources to the patient, such as doctors, paramedical staff, medicines, ambulance services, and many

other health resources. Health is an important entity for human life, and it has a great impact on the economy [6].

Many frameworks have been proposed to implement IoT technology in health services [7]. Three major paradigms have been discussed in the literature for IoT technology: application, security, and efficiency domains. The framework proposed focuses on the security, efficiency, and application domains of IoT technology in health services. This framework provides an overall design and implementation strategy with IoT technology. It addresses all the practical implementation issues of the technology (i.e., communication entities, communication technologies, hardware structure, data storage, data flow, and access mechanisms). A framework proposed by Zhao et al. [8] remotely monitored elderly people. They focused on the application domain of IoT technology. Their model facilitated the needs of elderly people. Machine learning techniques were utilized in their proposed model [9]. To monitor elderly people and patient status, another framework, Help to You (H2U), was proposed by Basanta et al. [10].

In the application paradigm, the importance of remote monitoring for patients was presented by Swiatek and Rucinski [11]. Their proposed model emphasized distributed system in delivering smart health services. They also addressed the innovative and commercial aspects of e-health services. Yang et al. [12] merged the traditional concept of a medical box with smart health services. iMedBox, iMedPack, and Bio-Patch are being used to provide medical services. An efficient resource-optimized rehabilitation system in IoT environments was proposed by Fan et al. [13]. Semantic information was utilized in their proposed model to efficiently identify the medical resources of a smart health system.

To keep the electronic health record and location information confidential, a specialized framework was proposed by Ding et al. [14]. They worked on the security paradigm of IoT technology. However, their main focus was limited to the security of personal location, personal identification, and identification of queries and personal electronic health records. Gong et al. [15] proposed and implemented a lightweight algorithm for the smart healthcare system. A lightweight private homomorphism was proposed, in addition to modified encryption DES algorithms. Improved algorithms provide the confidentiality needed for electronic health records during communication and while residing on the server. Various researchers have shown the use of IoT environments in the medical field [16–18].

2. Methodology

Different frameworks have been proposed to implement IoT technology in smart health systems. A specialized framework is required to address technical issues, such as interoperability and constrained and open Internet environments, as well as to address the nontechnical aspects, such as smart health services at the door step and remote consultancy for the poor people of underdeveloped countries. In this paper, we model a specialized architecture to provide smart health services in a smart health unit by using a specialized IoT gateway, which provides the interoperability between different sensor-based communication devices and provides the translation between local and Internet traffic. The IoT gateway also provides connectivity with backend cloud services.

The model presented also uses the constrained application protocol in the constrained environment and the hypertext transfer protocol in the Internet environment, due to the different requirements of both environments. The proposed framework also used the JSON format to store the list of remote consultants on the cloud, which was verified by the governmental health authorities. Only the physicians at local health centers who are registered practitioners can use the list verified by the health authorities. This approach ensures that only qualified practitioners at local health centers and remote consultants can use the list.

3. Research Scope and Validation Details

To summarize, the key goal of this paper is to present a specialized framework for an IoT-based smart health system. The framework uses a layered approach to address key issues of IoT-based smart health systems and provides a complete mechanism of data collection from the patient to cloud storage, which can be accessed either locally or remotely. The proposed model was tested using the Contiki real-time operating system, which utilizes the cooja simulation tool to simulate the behavior of network.

4. Background

In this section, we present background information for developing a better understanding of the proposed architecture.

4.1. IoT Devices. IoT devices are small in size, operate on a low power supply, and have limited processing capacity. Microcontrollers with 8-bit and 16-bit processors are well known in the market. A specialized foreground-background algorithm is used for a single processor to manage multiple processes at a time. Processors with 8-bit or 16-bit architecture are not specialized for planarity to support IoT devices, and these devices place demands on a real-time operating system. A real-time operating system requires more energy and memory and higher processing capabilities for working with devices. There are also many other issues for devices to work in the IoT paradigm. Devices must support TCP/IP stack for networking, but this stack is not a simple program, because more RAM is required to handle the number of network buffers for TCP. Furthermore, Java support is also a demand for an IoT device; therefore Java Virtual Machine (JVM) should also be run on the operating system of IoT devices. In conclusion, RAM and ROM support should be available for IoT devices to support the real-time operating system and communication stack.

Today, 32-bit microcontroller units that are small in size, operate on a low power supply, and have sufficient processing capacity to support IoT devices are also available on the market. These 32-bit microcontroller units are the best selection for IoT solution developers and providers.

Table 1: Wireless technologies for IoT systems.

Standards	Operating Frequency	Data Rate	Range	Power Consumption	Battery Time
IEEE 802.15.4	868/915 MHz, 2.4 Gz	250 kbps	10 to 300 m	Very Low	Months-year
Wi-Fi	2.4 to 5.8 GHz	11–105 Mbps	10 to 100 m	High	Hours
Bluetooth	2.4 GHz	723 Kbps	10 m	Very Low-Low	Days-Weeks

Table 2: Web technologies for IoT systems.

Protocol	Transport Mechanism	Messaging Method	Resource Consumption	Successful Applications
HTTP RESTful	TCP	Request/Response	10 Ks Flash or RAM	Smart home and grid
CoAP	UDP	Request/Response	10 Ks Flash or RAM	Used in Field Area Networks (FAN)
MQTT	TCP	Request/Response Public/Subscriber	10 Ks Flash or RAM	Remote monitoring and controlling of devices
XMPP	TCP	Request/Response Public/Subscriber	10 Ks Flash or RAM	Remote management of major appliances (white goods)

Data acquisition, processing, power management, communication stack, protocol conversion, firmware upgrade, and customizable security features can be implemented in IoT devices by using 32-bit microcontroller units. Intel and ARM families are well known in the market of 32-bit architecture processors.

The Intel family provides support for industrial Internet applications with atom processors, while the Intel Quark also captures the embedded system's market. On the other hand, the ARM Cortex-M0 processor is specialized to provide a low-cost product for IoT systems.

ARM Cortex-M3, M4, and M7 are the best choices to build IoT gateway devices. High performance, energy balance, and flexible system interfaces are major attributes of these processors for supporting IoT gateways. To support low energy consumption and high performance, the RL78 is the best 16-bit processor in a new generation of Renesas microcontrollers.

Different competitors for microcontroller units are providing their market solutions with pros and cons, but to support smart and small-embedded systems, ARM, Intel, and Renesas are popular and well tested. To support small IoT resource-constrained devices, Oracle's Java ME embedded 8 has also been designed. Java ME embedded 8 is widely used in wireless modules, buildings, industrial controls, health systems, grid monitoring, and many other applications.

Java ME embedded 8 requires that the system is based on the ARM architecture system-on-chips (SOCs), has only 128 KB of RAM and 1 MB of ROM, has a simple embedded kernel or operating system, and has a network connection that is either wired or wireless [19]. Java ME embedded 8 is also among the low-cost solutions and is sufficient to support resource specific devices of an IoT system.

4.2. Wireless Technologies for IoT. A standard communication technology is required for an IoT system. For communication between IoT devices and backend service providers, a communication technology should be chosen. IoT devices are enabled with wireless connectivity. There is no single standard wireless technology to support an IoT system. A number of technologies that have pros and cons are available. Implementation of wireless technology also depends upon the IoT project. For example, it may be a healthcare or home automation project, or a smart grid or environment-monitoring project. A comparison of some wireless technologies is given in Table 1.

4.3. Web Technologies for IoT. Existing web advancements can be used to develop IoT systems. However, these advancements are not sufficient to properly support IoT systems; therefore, results are poor. JSON and XML can be delivered in payloads by using HTTP and WebSocket protocols. Existing web protocols can be implemented on IoT devices, but these protocols require more resources to support IoT applications. To support IoT systems, many specialized protocols have been developed that can work efficiently with resource-constrained IoT devices and networks. Some web technologies are presented in Table 2.

4.4. System Components. This section presents the various components of the proposed system and further outlines the proposed model with the functionality of each layer.

The proposed model defines the structure of the IoT-based smart health system. The data collector, IoT gateway, backend facilitator, and access applications are the major components of the model. Fundamental parts of the proposed system are described below.

4.4.1. Data Collector (Dc). This component of the IoT system is used to sense the patient body. Data collectors are the sensor devices. These sensors monitor the health state and convert it to digital values. Data collectors support various types of wireless communication technologies to communicate with IoT devices.

4.4.2. IoT Gateway (iGW). The IoT gateway is a key component of the IoT system that connects the local processing units with the remote backend facilitator by using the Internet protocol IPv4 or IPv6. The IoT gateway is also used to convert the protocols, manage the IoT devices, and provide temporary storage. It is also a middle entity between the local sensor network and remote IP network. The IoT gateway also acts as middleware. It supports different modules to provide different functionalities in the IoT system.

4.4.3. Backend Facilitator (Bf). The backend service provider is the backend facilitator. These services may be outsourced from a third party or may be their own deployment. The backend facilitator provides storage services to permanently store the IoT data and perform decisions and analytics on the stored data. The data integration facility integrates the different types of data. Tools for security management and application development are also part of the backend facilitator. Additionally, remote consultancy is also linked with backend services, since the backend facilitator manages the list of remote consultants.

4.4.4. Access Applications (AA). The final requirement of the IoT system is the access mechanism for the IoT services, which is accomplished by using the access application. The access application may be installed on smart devices or on desktop systems.

4.5. Proposed Layers. Three layers that address the complete functionality of the system have been proposed for the IoT system. This part of the research discusses the functionality of each proposed layer. Each layer is utilized to provide smart health services. Different protocols and standards are used by the components of each layer to carry out their respective functionality. The proposed layers are also helpful for understanding the functionality of different components of the IoT system.

The three layers of the proposed model are described as follows:

(1) Sensor layer

(2) Network access layer

(3) Service access layer

The *sensor layer* is the first layer of the proposed model that addresses the functionality of the various components. Data collectors in this layer are used to monitor and accumulate the health information of a patient. The data collectors are the sensor devices, which are sometimes embedded in the body or may sometimes reside on the body of a patient. Data that are detected by the data collectors may include the pulse rate and heartbeat. A sensor device supports different communication technologies, as these may be from different vendors.

The sensor layer includes the following components:

(i) *Communication technologies*

(ii) *Bar Code and RFIDs used for tagging*

(iii) *Data collectors such as sensor devices*

(iv) *IoT gateway device (iGW)*

Local communication technology is used to transfer the sensed information to the IoT gateway, and then the IoT gateway transfers the information to the backend facilitator in IP format.

The *network access layer* is the second layer of the IoT-based health system and is used to provide connectivity between the backend facilitator and IoT gateway. This layer also provides an interface to the devices in the sensor layer with the backend facilitator (Bf). The cloud service provider supplies backend services. Dslam, DSL, and 3G/4G technologies are used to provide connectivity between the IoT gateway device and the backend services over the cloud by using Internet services. Specialized web technologies for IoT systems are also used to obtain the data.

The data collected in the smart health unit is forwarded to the backend cloud over the Internet by using the IoT gateway device. Many services are provided by the backend facilitator, such as data storage to store the data permanently, allowing querying by using query services, data integration of data from multiple sites by using data integration services, data analysis for future prediction, and many development tools provided by the backend service provider to develop new applications for the smart health system. An authentic list of remote consultants is also managed over the cloud storage. Government authorities authenticate consultants who are experienced, well known, and experts in their profession. Only registered practitioners in the smart health unit can use this list whenever they want to access their patient records.

The network access layer includes the following components:

(i) *Communication technologies*

(ii) *Backend cloud services*

(iii) *IoT gateway*

(iv) *A list for registered remote consultants.*

Thus, the network access layer is also an important part of the proposed model.

The *service access layer* provides access to the services of the smart health unit by using access applications. Applications may be installed on the smart computing devices or on desktop computers. The doctor or medical professional can access the health information of a particular patient whenever it is required. Local medical professionals in the smart health unit can consult the remote consultants by using the special application in the smart health unit.

Different application protocols are used to access the patient data from cloud storage. Data are also queried by using specialized database applications that use specific application protocols. IoT devices can also be accessed locally or remotely for management purposes. Remote consultants can treat the patient remotely from anywhere in the smart health unit of the IoT-based smart health unit.

The IoT system works in a constrained environment and in an Internet environment. The smart health unit part works in the constrained environment, where data collectors

and the IoT gateway are available. Therefore, there should also be state-of-the-art web technologies to work in this environment. Fortunately, CoAP is the best choice for working in a constrained environment. CoAP works best with constrained devices and constrained networks. However, there is no need to use CoAP in the Internet environment. HTTP RESTful is the best choice for working in the Internet environment. In the Internet environment, much network bandwidth is available that has high processing capacity for network devices. HTTP and CoAP can be mapped by using proxy services on the IoT gateway device.

The service access layer includes the following components:

(i) *Medical professionals*
(ii) *Management authorities*
(iii) *Smart computing devices and desktop computers*
(iv) *Smart applications*
(v) *Modern web technologies*

The service access layer in the smart health unit provides the front-end interface for its users.

4.6. Security Model. To secure the IoT system, first the devices should be secured from physical access by using locked racks. The wired connections and device features, which are not required, should be disabled. Default passwords should also be changed, and strong passwords should be used on devices. The remote access should be restricted when there is no need, and updates should only be installed when they are available. Additionally, the vendor's security measurements on the device should be assessed before purchase. Where possible, devices enabled with a self-correcting mechanism should be purchased. There must be a strong authentication mechanism with the cloud to protect against misidentification of the device. A strong encryption mechanism during communication can protect the data against illegal access. TLS must be used with the certificate validation mechanism for authentication and secure key distribution.

Communication between mobile applications and devices is carried out on a wireless connection; therefore, data should be encrypted during communication; otherwise local traffic will be unveiled. The mobile application should use TLS/SSL and validate the device's TLS certificates, which will protect the communication against a man-in-the-middle attack. Communication between mobile or web applications and cloud services should be secured with TLS/SSL by allowing its use from the cloud service; otherwise the attacker will capture the data passively. Many cloud service providers allow users to create a weak password that is not secure.

The service should enforce strong password creation. Strong passwords increase the effort needed to crack them when brute force or dictionary attacks are used. Mobile applications should follow best practices and be designed to work securely with services. Applications should properly validate the server's TLS certificate. Thus, best practices lead to secure communication. Figure 1 shows the security model for the IoT-based health system.

4.7. Modeling Exercise. Mathematically, the smart health unit can be presented as follows:

Generally, for the smart health unit,

$$\mathrm{SHU} = f\,(\mathrm{Dc}, \mathrm{iGW}, \mathrm{Bf}, \mathrm{AA}) \tag{1}$$

In (1), the smart health unit (SHU) variables are defined as follows: f represents function; Dc represents data collector devices; iGW represents the IoT gateway in the smart health unit; Bf represents the backend facilitator, which provides the backend services for the smart health system; and AA represents the access application. Equation (1) describes the complete smart health unit that depends on every component of the proposed model.

Equation (2) describes the smart health unit as follows:

$$\mathrm{SHU} = \left(\alpha + \beta\mathrm{Dc} + \gamma\mathrm{iGW} + \delta\mathrm{Bf} + \theta\mathrm{AA} + \mu^{\circ}\right), \tag{2}$$

where, for each component,

$$\mathrm{Dc} = f\left(\text{data collection}, \text{data forwarding}\right) \tag{3}$$

Dc is a function that represents the data collection and is used to accumulate the data and further forward it to the IoT gateway device for processing.

Now specifically,

$$\mathrm{CT} = f\,(\mathrm{iGW}), \tag{4}$$

where

$$\mathrm{CT} = (\text{Bluetooth, Wi-Fi, Zwave, 6LowWPAN, DSL, 3G, 4G}, \ldots, n) \tag{5}$$

The component CT represents the communication technologies that are supported by the IoT gateway device, iGW. Communication technologies may be Bluetooth, Wi-Fi, 6LowWPAN, DSL, or 3G/4G technologies.

4.8. Implementation Details. To access the health data locally or from cloud storage, state-of-the-art smart access applications are used. HTTP is an application layer protocol that is well known for web technologies, and it is used to retrieve and store the data over the backend cloud storage within the Internet environment. HTTP works with the transmission control protocol TCP, which is a transport layer protocol. To access the web resources, HTTP uses defined methods, such as "GET" to get the resource, "PUT" to put the web resource, and many other methods, such as "POST" and "DELETE".

When a particular client establishes a connection with the server, HTTP, which is a connection-oriented protocol, uses these defined methods after establishing the connection. The TCP 3-way handshake is a connection-oriented mechanism that is used to establish the connection from a client to the server. The HTTP request is sent from the client to the server, and the connection is established between the client and the server after the handshake process.

For example, if the body temperature of a patient is a resource, HTTP will use its "GET" method to access this resource. HTTP uses a universal resource identifier (URI) to

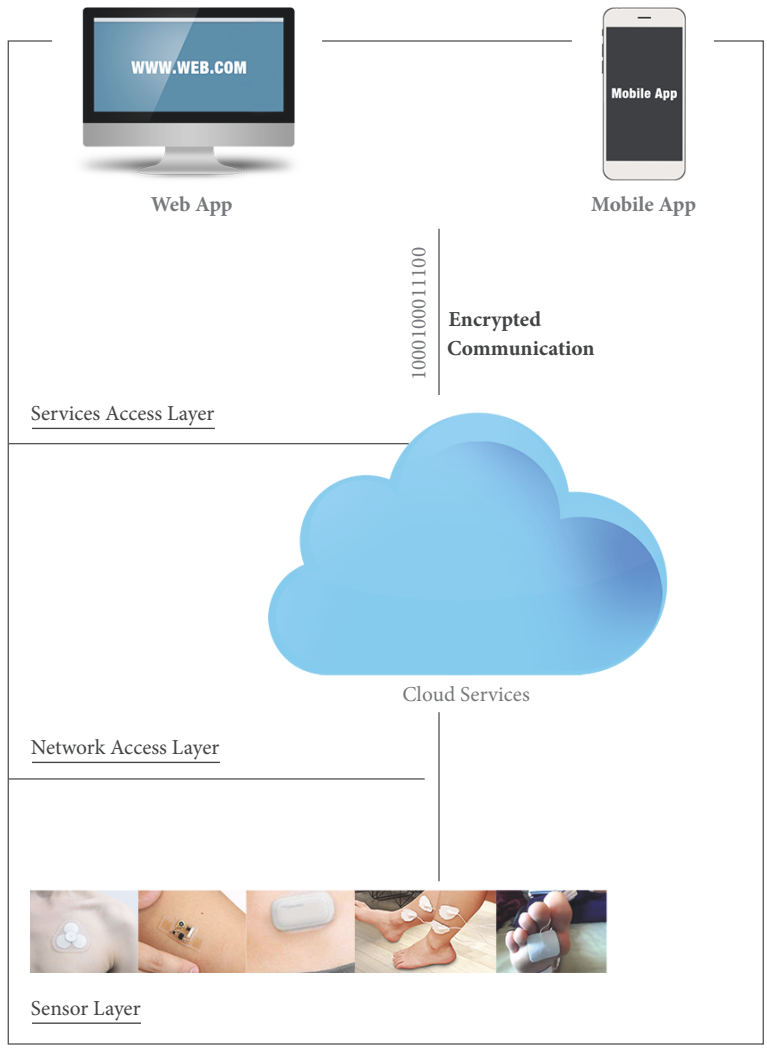

Figure 1: Security model.

identify the specified resource. Since HTTP is connection-oriented, it will also require the connection termination mechanism to terminate the connection. The termination process is also carried out by a 2-way TCP termination process. Once a connection is terminated, a connection establishment process will be needed to access the resource again. Establishing and terminating the HTTP connection process is shown in Figure 2.

A simple representational state transfer in the RESTful architecture is used by the HTTP. Predefined sets of operations are provided for its simple work. The XML, HTML, or JSON format are used to represent the resources in response to the RESTful request.

HTTP and CoAP are both used in the smart health system. In the constrained environment, only CoAP is used since it is specialized to work in constrained networks over constrained devices, and in the Internet environment, HTTP is used. Mapping between the HTTP and CoAP environments is performed on the IoT gateway device by using a special proxy module. The mapping is shown in Figure 3.

In order to access the web resource, HTTP is used in the Internet environment, which is based on a variety of networks. Networks have high bandwidth; therefore there is no issue of resource consumption as in constrained environments. Only CoAP is implemented in the constrained environment, as it is specially designed to work with constrained devices.

The response code is used to determine the proxy/caching model that is supported by the CoAP [20]. The CoAP-HTTP proxy model provides efficiency in the constrained environment where IoT devices work. If a resource named "heartbeat" of a patient is accessed using the HTTP request, then this request is generated in the Internet environment. The IoT gateway device responds to the HTTP request that is supporting the proxy model. The IoT gateway converts the HTTP request to the CoAP request and then sends the response back to the HTTP request. Figure 4 shows how the CoAP-HTTP proxy model works.

The CoAP, as a built-in service, also supports the subscription mechanism. The CoAP supports a special option

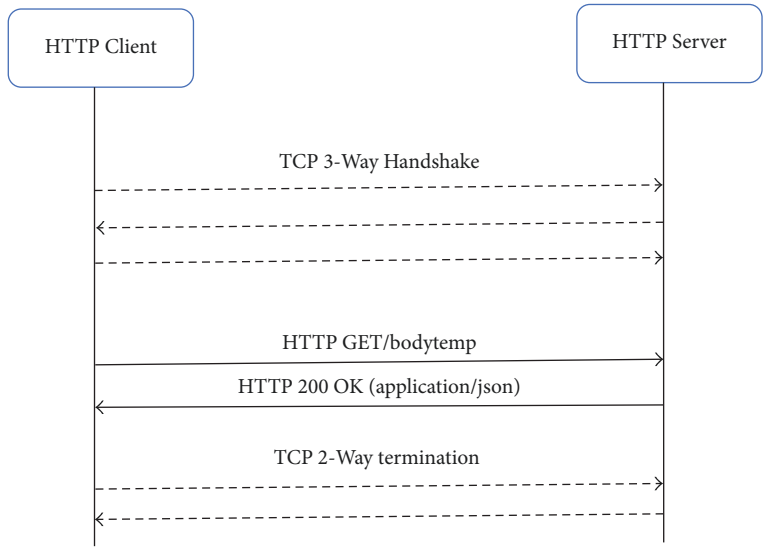

Figure 2: HTTP connection establishment and termination.

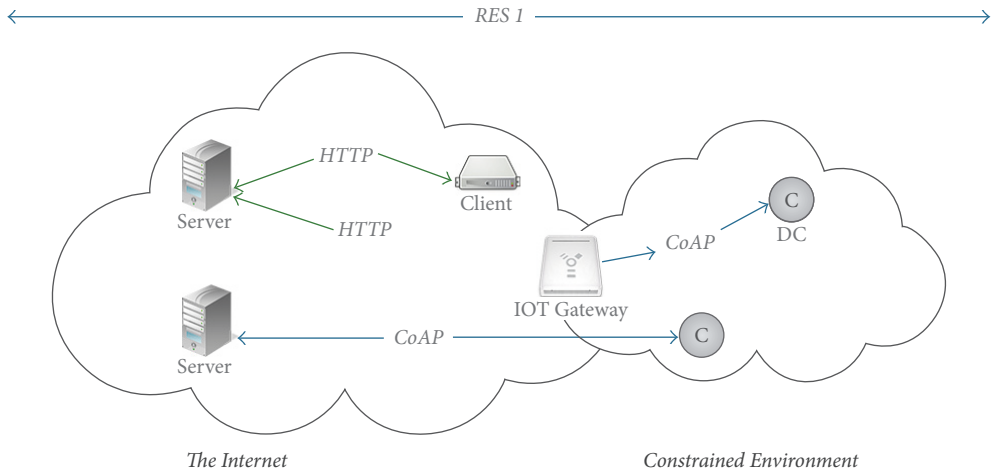

Figure 3: Mapping between CoAP and HTTP.

named "observe" to support the subscription method. Figure 5 shows the subscription-based "GET" method.

Different observations are separated by using tokens and therefore remain identified. When the value of the observation is changed, the server responds with a new observation but with the same token. The client also acknowledges when it receives the observation.

A lightweight data interchange format known as JSON is used to store the remote consultants list. It is a good format for the timely delivery of the message between the access entities and the service providers, for example, the backend facilitator Bf and the access application AA. The remote consultants list is accessed using the HTTP protocol, since the list is part of a web resource on the cloud storage [21]. A list in JSON format is shown in Algorithm 1.

The list of remote consultants that is stored on the cloud storage can be accessed by the authorized consultants in the smart health unit whenever they require it. A list is shown in Algorithm 1 that shows their name, age, gender, location, contact information, and time availability, so that the physician in the smart health unit can determine the appropriate remote physician. The list shown in Algorithm 1 provides the details of a physician, a pediatrician, and a cardiologist. The remote consultants list is also verified by the higher government authorities, so that only registered practitioners can participate in the IoT-based smart health system. This is compulsory; otherwise nonexperienced or even nonprofessional persons can register themselves inappropriately for the wrong purposes.

4.9. Experimental Results. An experiment was conducted using the Contiki operating system with 8 sensor nodes in a medical unit. The Contiki operating system also has a cooja simulating tool that monitors the behavior of network. The following results show the behavior of a network at the proposed sensor layer. The results show the behavior of the

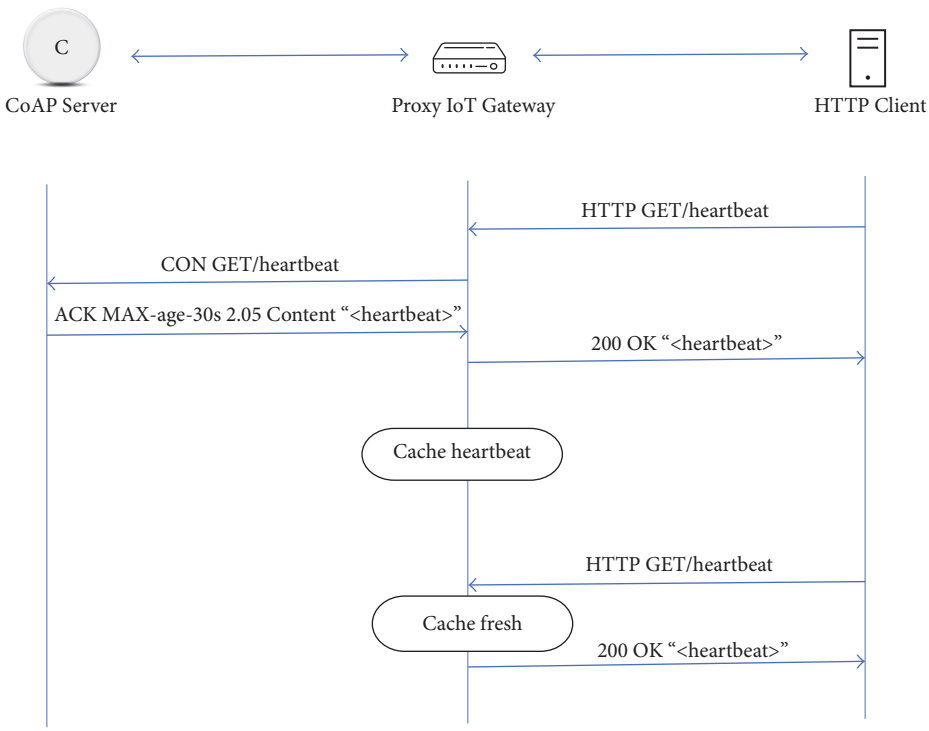

Figure 4: CoAP-HTTP proxy using the GET method.

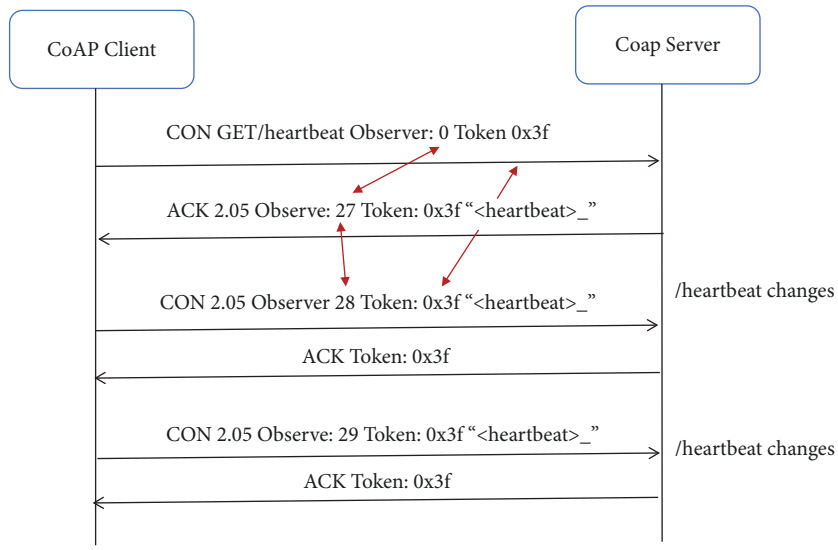

Figure 5: CoAP subscription-based GET method.

constrained environment in which smart IoT devices and gateways work, where collecting, processing, and forwarding the sensed data occur. Since IoT devices work in a constrained environment, there is a limit to the data rate and usage of sensor devices. Wireless terminals have a limited capacity to send and receive data, similar to this experiment. The maximum data rate, as given by the IEEE 802.15.4 standard, is 250 kbps [22]. Figure 6 shows the bandwidth consumption of the data collectors in the smart health unit.

The results show that the data rate varies with respect to the work of all of the nodes. However, it is not necessary that all devices must work at the same time. There is the possibility that, at a given time, some devices may be sending and receiving data, but other devices may not be doing so. Only the number of devices and the bandwidth do not measure the data rate. Protocols, which are being deployed for communication, and the network topology are also concerning factors for measurement of the efficiency of a system. The IoT gateway device's capacity is also a factor in

```
var consutants = {
    "physician" : {
      "name" : "Ijaz Malik",
      "age" : "50",
      "gender" : "male"
      "location" : "NH Multan"
      "contact" : "03xxxxxxxxx"
      "availability" : "Morning"
      "mail_id" : "exmple@gmail.com"
},
 "pediatrician" : {
      "name" : "Fawad Bukhari",
      "age" : "45",
      "gender" : "male"
      "location" : "BVH BWP"
       "contact" : "03xxxxxxxxx"
       "availability" : "Morning"
       "mail_id" : "exmple@gmail.com"
},
"cardiologist" : {
      "name" : "Aftab Ahmmad",
      "age" : "38",
      "gender" : "male"
      "location" : "CPEIC Multan"
       "contact" : "03xxxxxxxxx"
       "availability" : "Morning"
       "mail_id" : "exmple@gmail.com"
  }
}
```

Algorithm 1: Remote consultant list stored in JSON format.

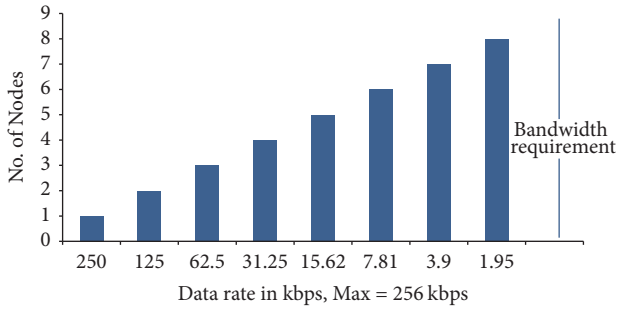

Figure 6: Bandwidth consumption by the data collectors.

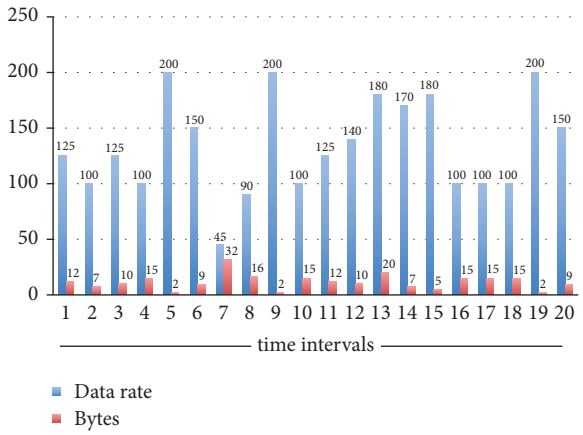

Figure 7: Data rate at different intervals of time.

understanding the proper working of the sensor devices since the IoT gateway directly interacts with the sensor nodes.

At different time intervals, the data rate is different for different devices in the smart health unit. Whenever there is a high amount of data to transfer, then the maximum data rate will be low, and whenever there is a low amount of data to transmit or receive, the data rate will be high. Figure 7 clearly shows the diversion in the data rate.

4.10. Implementation Scenario. A concept of the proposed model is illustrated in a particular smart healthcare scenario in Pakistan.

For example, people in Pakistan live mostly in villages, and when a patient in a village requires his medical checkup, he visits the nearest smart health unit in his village. In the smart health unit, all of the necessary equipment is installed to provide smart health services.

The smart health unit is equipped with data collector (Dc) sensor devices to sense the health information of the patient, such as body temperature, heartbeat, respiratory rate, and glucose level, and an IoT gateway to act as a middle entity between the local sensor network and the backend facilitator. The smart health unit is also equipped with the smart computing device and desktop computers, which will be used by the medical staff in the smart health unit to access the data and IoT devices. There is also an Internet connection to provide connectivity between the smart health unit and the backend facilitator, using either the mobile network GSM, 3G/4G, PSTN, ADSL, or a DSL connection.

When the patient asks for his medical checkup, the staff offers him wearable sensor devices that connect the patient to the devices of the medical staff. Wireless sensor devices may use Bluetooth, 6LowWPAN, ZigBee, Z-Wave, and many other wireless technologies. Data collectors process the sensed information to the IoT gateway device, which has temporary storage for the sensed data, and these data become accessible to the medical staff in the unit by using smart computing devices or desktop computers. The IoT gateway is smart enough to support multiple wireless technologies, which solves the interoperability issue between the sensor devices and the gateway device in the smart health unit. The IoT gateway device is also capable of formatting the sensed data to the Internet format, which supports the use of the Internet for communicating with the backend facilitator.

The smart health unit data are forwarded to the IoT gateway device and to the backend facilitator, that is, the cloud service provider. An authorized person from anywhere in the world can, at any time, access the data over the cloud. Since there is also an authorized consultant list in the cloud storage, the medical staff in the smart health unit can use it to consult with the remote consultants. Data using the cloud storage is permanently stored, so the patient data can be accessed whenever it is required. These data are also

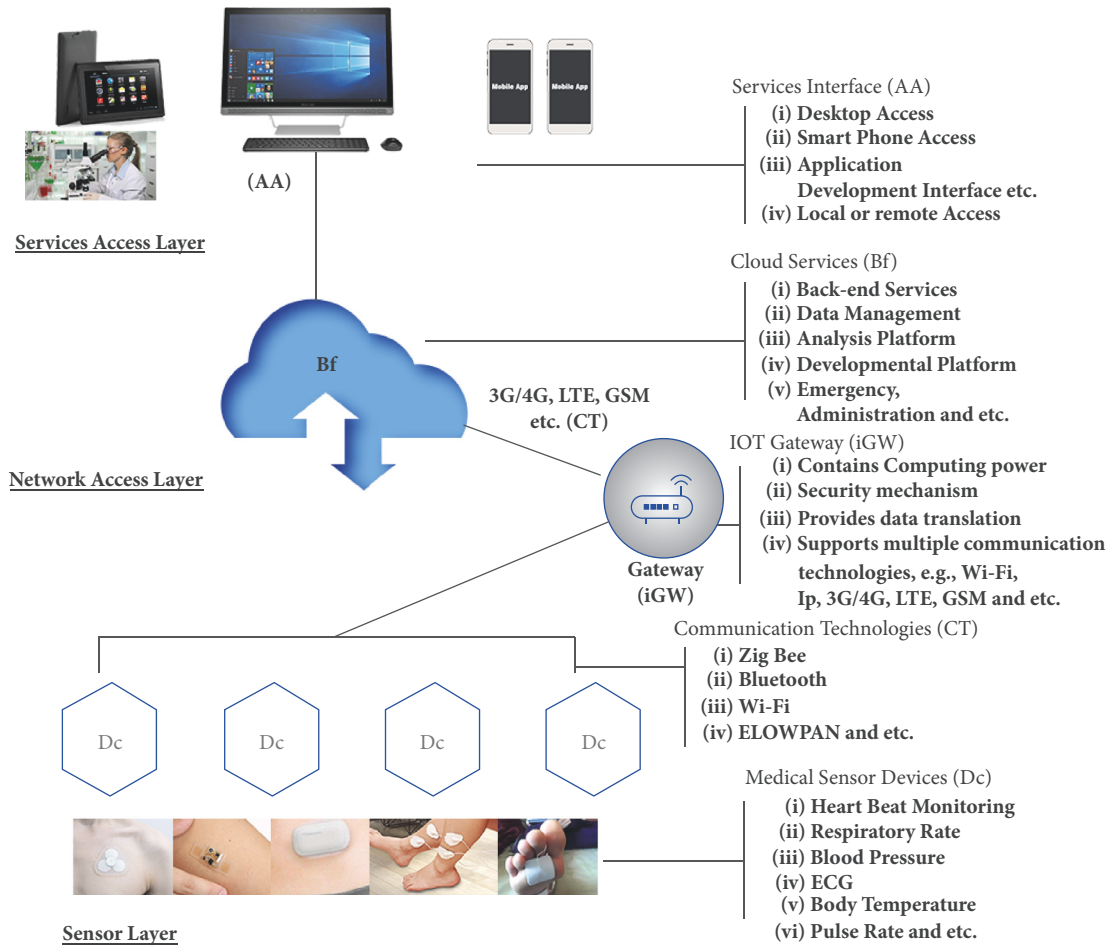

Figure 8: Smart health scenario.

accessible to government authorities to keep track of public health. Therefore, the patient in the smart health unit is taking advantage of health services at the doorstep. The medical staff is also taking advantage of the remote consultants to provide better health services. An IoT-based smart health unit scenario is shown in Figure 8.

5. Conclusions

Over the past few years, the scope of IoT technology has widened in every field of life. Different research problems have been raised in the deployment of IoT technology. To mitigate the problems and find better deployment solutions, different work has been performed in the research community. In the field of health sciences, different frameworks have been proposed to efficiently deploy the smart health services, and the focus has always been on the security and efficiency of these algorithms.

A specialized framework is presented in the current research that provides smart health services in underdeveloped countries, especially in rural areas. The framework studies various aspects of IoT technology for smart health services, such as the interoperability and standardization issues, constrained and Internet environments, specialized communication protocols, and web technology requirements. The proposed model consists of three layers, where each layer performs a specialized task. In the future we aim to develop a detailed security infrastructure that can be incorporated using the current framework.

Conflicts of Interest

The authors declare that there are no conflicts of interest related to this paper.

References

[1] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, 2010.

[2] C. Zhu, V. C. M. Leung, L. Shu, and E. C. Ngai, "Green Internet of Things for smart world," *IEEE Access*, vol. 3, pp. 2151–2162, 2015.

[3] E. Mok, G. Retscher, and C. Wen, "Initial test on the use of GPS and sensor data of modern smartphones for vehicle tracking in dense high rise environments," in *Proceedings of the Ubiquitous Positioning, Indoor Navigation, and Location Based Service (UPINLBS '12)*, pp. 1–7, IEEE, October 2012.

[4] "Internet of things vs. Internet of everything what is the difference, May 2014".

[5] J. Haase, M. Alahmad, H. Nishi, J. Ploennigs, and K. F. Tsang, "The IOT mediated built environment: A brief survey," in *Proceedings of the 14th IEEE International Conference on Industrial Informatics, INDIN 2016*, pp. 1065–1068, IEEE, July 2016.

[6] M. García, "The impact of IoT on economic growth: A multifactor productivity approach," in *Proceedings of the International Conference on Computational Science and Computational Intelligence, CSCI 2015*, pp. 855-856, IEEE, December 2015.

[7] M. A. Sahi, H. Abbas, K. Saleem et al., "A Survey on Privacy Preservation in e-Healthcare Environment," *IEEE Access*, 2017.

[8] W. Zhao, C. Wang, and Y. Nakahira, "Medical application on internet of things," in *Proceedings of IET International Conference on Communication Technology and Application (ICCTA 2011)*, pp. 660–665, Beijing, China, 2011.

[9] S. Earley, "Analytics, machine learning, and the internet of things," *IT Professional*, vol. 17, no. 1, Article ID 7030173, pp. 10–13, 2015.

[10] H. Basanta, Y. P. Huang, and T. T. Lee, "Intuitive IoT-based H2U healthcare system for elderly people," in *Proceedings of the Networking, Sensing, and Control (ICNSC), 2016 IEEE 13th International Conference on*, pp. 1–6, IEEE, 2016.

[11] P. Swiatek and A. Rucinski, "IoT as a service system for eHealth," in *Proceedings of the e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on*, pp. 81–84, IEEE, Lisbon, Portugal, October 2013.

[12] G. Yang, L. Xie, M. Mäntysalo et al., "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2180–2191, 2014.

[13] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, and F. Wu, "IoT-based smart rehabilitation system," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1568–1577, 2014.

[14] D. Ding, M. Conti, and A. Solanas, "A smart health application and its related privacy issues," in *Proceedings of the Smart City Security and Privacy Workshop (SCSP-W)*, pp. 1–5, 2016.

[15] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in *Proceedings of the Parallel Architectures, Algorithms and Programming (PAAP), 2015 Seventh International Symposium on*, pp. 217–222, December 2015.

[16] K. R. Amrutha, S. M. Haritha, V. M. Haritha, A. J. Jensy, S. Sasidharan, and J. K. Charly, "IOT based Medical Home," *International Journal of Computer Applications*, vol. 165, no. 11, 2017.

[17] M. M. Rathore, A. Ahmad, A. Paul, J. Wan, and D. Zhang, "Real-time Medical Emergency Response System: Exploiting IoT and Big Data for Public Health," *Journal of Medical Systems*, vol. 40, no. 12, article no. 283, 2016.

[18] G. Zhang, C. Li, Y. Zhang, C. Xing, and J. Yang, "SemanMedical, A kind of semantic medical monitoring system model based on the IoT sensors," in *Proceedings of the e-Health Networking, Applications and Services (Healthcom), 2012 IEEE 14th International Conference on*, pp. 238–243, IEEE, 2012.

[19] Java Embedded Documentation, http://www.oracle.com/technetwork/java/embedded/javame/embedme/documentation/index.html.

[20] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," Internet Engineering Task Force, RFC 7252, 2014.

[21] D. Crockford, "The application/json Media Type for JavaScript Object Notation (JSON)," RFC Editor RFC4627, 2006.

[22] "IEEE 802.15 WPANTM Task Group 4," http://www.ieee802.org/15/pub/TG4.html.