ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)
Vol 3, Issue 6, June 2017

A Secured Remote Health Monitoring System Based on IoT

[1] Priya.R, [2] A. Pravin Renold
[1][2] Department of Electrical and Electronics Engineering,
[1][2]Velammal Engineering College,Chennai,India

***Abstract*-— The Personal Healthcare Devices (PHDs) measure vital signals of patient. The advantages of PHDs are: (1) wearable (2) Support diseased people (3) Continuous monitoring of health and precaution leads to increased lifetime. Due to the advent of different communication standards such as low power Bluetooth, zigbee, and Internet of Things, the PHDs could be connected to caretakers or doctors and provide proper advice or medication. This project deals with designing a firmware for PHDs, which is interoperable and secure.The advantages of the proposed system are:**

i. Low cost PHDs could be designed compatible for the firmware

ii. Ensures privacy

iii. Improves patient care

There exists a challenge in terms of maintaining privacy of patient's data when connecting PHDs to the network. .In this work, we integrate PHDs with internet for sharing health data using Constrained Application Protocol (CoAP) and AES algorithm for Security purpose. CoAP is based on the Representational State Transfer (REST) model and can be considered a real enabler for Internet of Things (IoT). IoT is characterized by an interconnected set of individually addressed and constrained devices in a distributed system, with sensing/active devices for physical phenomena, data collection, and applications using sensing, computation and actuation.

***Keywords*: Personal Healthcare Devices(PHD), Constrained Application Protocol(CoAP), Representational State Transfer(REST), Internet of Things(IoT),Advanced Encryption Standard(AES)**

I. INTRODUCTION

The next wave in the era of computing will be outside the realm of the traditional desktop. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another [1] .These results in the generation of enormous amounts of data which have to be stored processed and presented in a seamless, efficient, and easily interpretable form. With the growing presence of Wi-Fi and 4G-LTE wireless Internet access, the evolution towards ubiquitous information and communication networks is already evident. However, for the Internet of Things vision to successfully emerge, the computing paradigm will need to go beyond traditional mobile computing scenarios that use smart phones and portables, and evolve into connecting everyday existing objects and embedding intelligence into our environment. For technology to disappear from the consciousness of the user, the Internet of Things demands: A shared understanding of the situation of its users and their appliances. Maintaining good Health is one of the global challenges for humanity as in millennium website (2016). According to the constitutions of World Health Organization (WHO) the highest attainable standard of health is a fundamental right for an individual as stated in WHO website (2016) [2]. In this approach the patients are equipped with knowledge and information to play a more active role in disease diagnosis, and prevention.Smartphone, supported with high speed data services, has revolutionized healthcare by playing the role of a powerful medical device for monitoring the patients' health.In this work, for sharing health data we use Constrained Application Protocol (CoAP). CoAP is based on the Representational State Transfer (REST) model and can be considered a real enabler for Internet of Things (IoT). IoT is characterized by an interconnected set of individually addressed and constrained devices in a distributed system, with sensing/active devices for physical phenomena, data collection, and applications using sensing, of IoT.

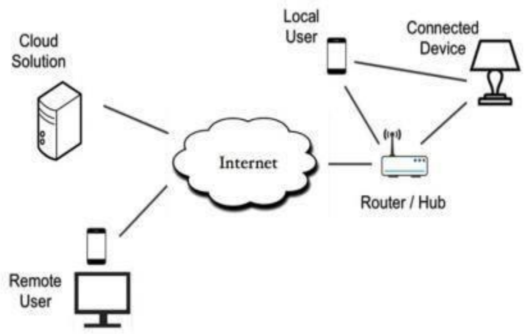


Figure 1 Overview of IoT

II.RELATED WORK

Without sufficient and elaborate study of the previous works of the projects, it is difficult to enhance or improve the shortcomings of it. So here a few words explaining the literature survey of the proposed work from various papers are given for reference.

2.1. A REST based Design for Web of Things in Smart Environments

In [3] realized that the main vision of "Web of Things" is the connectivity of web to billions of smart objects. The main challenge is interoperability, which is held in that application layer. An approach using REST (Representational Atate Transfer) principles for smart plant-watering application is briefed here. CoAP uses both messaging (asynchronous interaction) as well as request/response (uses method) model. Totally 19 Motes in which one is border router, one for CoAP server and others are CoAP clients in multihop fashion. The software used is cooja, wireshark, copper on Contiki-2.6 to perform experiments on TMote skys. Cooja simulator simulates the Contiki nodes, Wireshark is used as network performance analyzer tool and copper is added as Mozilla Firefox add-on. The novelty in this paper is an algorithm for an efficient PUSH scheme has been proposed and evaluated. The future work deals with the design of fragmentation, use of micro data and Efficient XML Interchange (EXI).

2.2. Secure User Authentication Scheme for Wireless Healthcare Sensor Networks

In [4]This work addressed user authentication scheme and data transmission mechanism that facilitates security and privacy protection, enable medical personnel to instantly monitor the health conditions of care receivers, and provide care receivers with prompt and comprehensive medical care. The security in implemented in different phases of operation such as registration, login, and authentication. Merits of the system are Only Authorized users can access the Data. Authorization has to be done with trusted authority individually. Disadvantage of the system is high computational complexity.

2.3 A personal connected health system for the Internet of Things based on the Constrained Application Protocol

In [5] Implemented a ststem by integrating CoAP with Rabin Security. The light weight of the CoAP messages makes them suitable for constrained devices such as PHDs. Simple messages require less processing power from devices, and also require less internal storage buffers. Demerits of the system are all readings are shared with health service on the internet using CoAP that is large amount of data is transferred using rabin asymmetric algorithm it requires large amount of memory.

2.4 CoAP (Constrained application protocol) in M2M Environmental Monitoring System

In [6] deployed CoAP in mobile environmental monitoring system for transmission of a resource description and sensor environmental data from IoT nodes and vehicle tracking devices. CoAP is not just a compressed but subset of HTTP. A single layer protocol is encoded in a simple binary format. Telit GEM-GPRS modems used along with python interpreter. Payload is inserted into HTTP message and forwarded to a web server and stored in local database defined in Access. Wireshark is used for size determination. The performance parameter used is average transmission time between CoAP and HTTP which shows the time for message transport is 3 times smaller if CoAP protocol is used.

III.METHODOLOGY:

The Motes used for the three categories such as one mote as Server, one as Border Router and Clients may be in any number.

- Server – A Restful server shows how to use the REST layer to develop server-side applications
- Border Router – Border Router keeps radio turned on. Enabling of it helps in connection between that of client as well as server to that of CoAP web Address. Border-Router has the same stack and fits into mote memory.
- Client – A CoAP client that polls the /actuators/toggle resource every 10 seconds and cycles through 4 resources on button press

The communication between Border Router, Client and Server is shown in Figure 2.

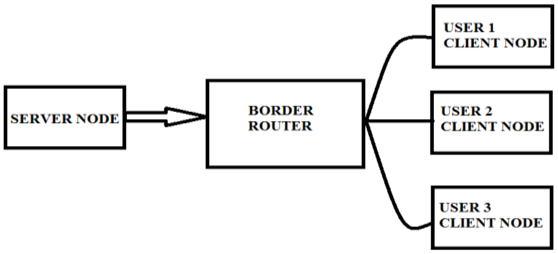


Figure 2 Communications between Border Router, Client, and Server

The client could be Bluetooth enabled device (PHD) or a sensor device (TelosB mote). The agents attached with sensor monitor the vital signs of human and transmit the data periodically to the manager. The TelosB mote equipped with temperature sensor monitor the body temperature and updates the manager in a periodical manner. The need for continuous monitoring of temperature is as follows:

- Body temperature represents the balance between heat production and heat loss
- Every 1°C rise in body temperature is a 10% rise in the rate of enzyme-controlled chemical reactions [5]
- At 43°C and above, cells are irreparably damaged and enzymes denatured, rendering death a certainty [5]
- As temperature drops, cellular processes become slow and the metabolic rate falls

Based on the temperature data received, the administrators (care taker, doctor) will take precaution measures to attend the patient. The communication between agent and manager are done using CoAP along with AES algorithm to achieve privacy. As the number of agent node increases the data could be transferred in a secured way.

IV. CoAP

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low- power, lossy) networks. CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments.

V. MESSAGE TYPES

- Confirmable Message - Some messages require an acknowledgement. These messages are called "Confirmable". as shown in Fig 3.

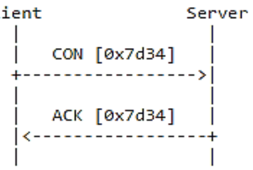


Figure 3 Confirmable Message

messages do not require an Acknowledgement. As shown in Figure 4.

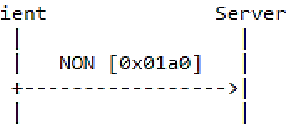


Figure 4 NON-Confirmable Message

- Acknowledgement Message - An Acknowledgement message acknowledges that a specific Confirmable message arrived.
- Reset Message - A Reset message indicates that a specific message (Confirmable or Non-confirmable) was received, but some context is missing to properly process it.

VI. CONTIKI ARCHITECTURE

The Contiki OS follows the modular architecture in [6]. At the kernel level it follows the event driven model, but it provides optional threading facilities to individual processes. The Contiki kernel comprises of a light weight event scheduler that dispatches events to running processes.

VII. COOJA SIMULATOR

With the rapid increase in the amount of wireless sensor nodes and other wireless devices forming heterogeneous networks, it becomes unfeasible to test real setups using physical hardware. While one can test systems and protocols on an abstract level by simulating wireless phenomena, such simulation alone is insufficient because software can be prone to bugs and unexpected interrelations. Simulating complicated wireless setups using exactly the same firmware image that will later be used on real wireless nodes is therefore crucial.

VIII.SECURITY

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits

all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix .Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.Fig 6 shows the working structure of AES algorithm.

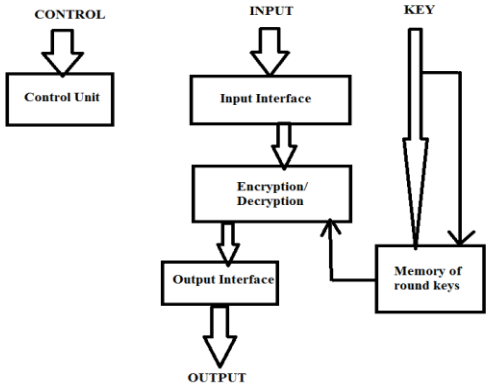
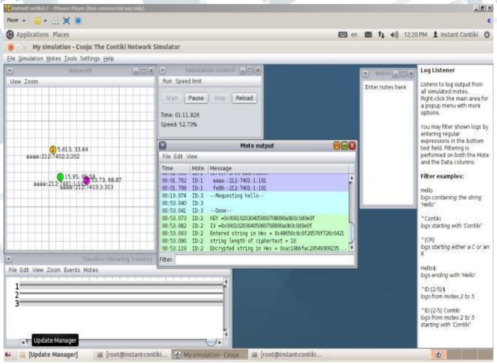


Figure 5 The schematic structure of AES

IX.SIMULATION RESULTS

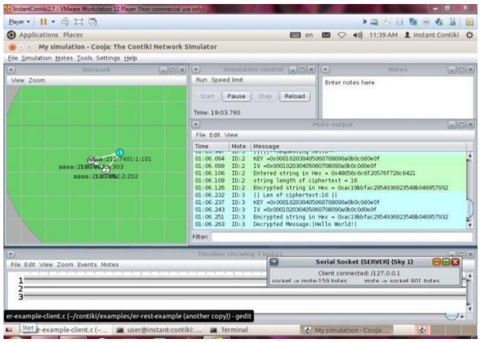
9.1 Encryption of Message Using AES



```
Time       Mote  Message
00:01.702  ID:1   aaaa::212:7401:1:101
00:01.708  ID:1   fe80::212:7401:1:101
00:10.974  ID:3  --Requesting hello--
00:53.040  ID:3
00:53.041  ID:3  --Done--
00:53.073  ID:2  KEY =0x000102030405060708090a0b0c0d0e0f
00:53.082  ID:2  IV =0x000102030405060708090a0b0c0d0e0f
00:53.093  ID:2  Entered string in Hex = 0x48656c6c6f20576f726c6421
00:53.096  ID:2  string length of ciphertext = 16
00:53.119  ID:2  Encrypted string in Hex = 0xac19bbfac29549369235...
```

Figure 6 : Encryption of Message

9.2 Decryption of Message Using AES



```
Time       Mote  Message
01:06.094  ID:2  KEY =0x000102030405060708090a0b0c0d0e0f
01:06.099  ID:2  IV =0x000102030405060708090a0b0c0d0e0f
01:06.106  ID:2  Entered string in Hex = 0x48656c6c6f20576f726c6421
01:06.109  ID:2  string length of ciphertext = 16
01:06.126  ID:2  Encrypted string in Hex = 0xac19bbfac29549369235480046957932
01:06.232  ID:3  || Len of ciphertext:16 ||
01:06.237  ID:3  KEY =0x000102030405060708090a0b0c0d0e0f
01:06.243  ID:3  IV =0x000102030405060708090a0b0c0d0e0f
01:06.251  ID:3  Encrypted string in Hex = 0xac19bbfac29549369235480046957932
01:06.263  ID:3  Decrypted Message:|Hello World!|
```

Client connected: /127.0.0.1
socket -> mote:159 bytes   mote -> socket 801 bytes

Figure 7 : Decryption of Message

Fig 6 and 7 shows about the message encryption on server side and decryption of the encrypted message on the server side using AES security algorithm.

X.CONCLUSION

Personal Health Devices (PHDs) allow patient to measure or monitor health status. Due to the recent developments in communication methodologies the devices can transfer data using short-range wireless technologies such as Bluetooth, Near-Field Communication (NFC), ZigBee or Bluetooth Low Energy (BLE), to mention some. The main challenge is to seamlessly integrate PHDs, mobile devices and Internet services, considering scalability, flexibility and heterogeneity of devices and technologies.The proposed system helps to achieve secured interoperable communication between different PHDs.

XIV.RFERENCES

1. A Right to Health available at http://www.who.int/mediacentre/factshee ts accessed in (September 2016).

2. mHealth App Developer Economics (2014) available at ttp:// mheal the conomics. com/ mhealthde veloper-economics – report / accessed in 2016.

3. Elias, S., Shivashankar, S., & Manoj, P. (2012, December). A REST based design for Web of Things in smart environments. In Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on (pp. 337-342). IEEE.

4. Liu, Chia-Hui, and Yu-Fang Chung. "Secure user authentication scheme for wireless healthcare sensor networks." Computers & Electrical Engineering (2016).

5. Santos, Danilo FS, Hyggo O. Almeida, and Angelo Perkusich. "A personal connected health system for the Internet of Things based on the Constrained Application Protocol." Computers & Electrical Engineering 44 (2015): 122-136.

6. Boswarthick, David, Omar Elloumi, and Olivier Hersent, eds. M2M communications: a systems approach. John Wiley & Sons, 2012.