Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 12, No. 1, March 2024, pp. 87~100
ISSN: 2089-3272, DOI: 10.52549/ijeei.v12i1.5191

Design of Service Oriented Architecture for an IoT Healthcare Management System

Amira G. Hosary[1], Ahmed Emran[2], Basel El-Saghir[2]
[1]Department of Electronics and Communication Engineering, Thebes Higher Institute, Maadi, Cairo, Egypt
[2]Department of Electrical Engineering, Al-Azhar University, Nasr City, Cairo, Egypt

Article Info

Article history:

Received Oct 25, 2023
Revised Feb 14, 2024
Accepted Mar 3, 2024

Keywords:

Internet of Things
Personalized healthcare
Pulse sensor
Room temperature sensor
Autonomous devices
Healthcare Protocols

ABSTRACT

Healthcare services maturities are increasing dramatically over the last decade towards better patient anomaly detection, early diagnosis, and more accuracy in manipulation. The applications of IoT in healthcare are becoming more popular day after day with a good focus on the autonomy of detection and decision-making of patient's vital data during admission phases, which could enable an envisioned environment for the right decisions on time. This paper focuses on developing a framework of architecture, protocols, and algorithms for IoT Healthcare system aimed at increasing the efficiency of systems operation and enhancing the reachability of different types of devices in the same patient or across several patients. The proposed architecture ensures that each individual device is autonomous and can work independently with the surrounding environment. The study includes as well as proof of concept pilot with a-capability to measure the patient's vital information on a non-invasive basis, such as the pulse sensor unit, room temperature, and the display out device. The concept is validated, proving that devices can communicate together optimally, reliably, intelligently and autonomously in the same patient or across patient categories according to the status of patients without human intrusion.

Corresponding Author:

Name of Corresponding Author,
Department of Electrical and Computer Engineering,
National Chung Cheng University,
168 University Road, Minhsiung Township, Chiayi County 62102, Taiwan, ROC.
Email: abcdefg@ccu.edu.tw

1. INTRODUCTION

The Internet of things was first introduced conceptually by Kelvin Ashton in 1999 [1], in his proposal to associate anything or any object with an RFID and possible connectivity to the internet that makes things interconnected over the internet. In the 2010s [2], research explored the use of IoT in healthcare within smart cities, emphasizing its role in improving public health and emergency response systems. This was followed by a comprehensive overview of IoT applications in healthcare, highlighting its potential for remote patient monitoring, chronic disease management, and medication adherence. In the 2020s, research delved deeper into the challenges associated with remote patient monitoring and medication adherence systems using IoT, including security, privacy, and interoperability concerns. Additionally, a systematic review of research on IoT for chronic disease management was conducted, showcasing its effectiveness in monitoring vital signs, medication adherence, and improving patient outcomes. According to Gartner[3], the internet of things is expected to connect 50 billion devices by the Year 2025. On the other hand, technology in healthcare and healthcare applications is being improved through implanting actuators and sensors in patients and the surrounding environment, including medications. The IoT is utilized by clinical care to screen physiological statuses of patients through sensors by gathering and analyzing their data and then sending analyzed patient's data remotely to handling focuses to patients appropriate activities. IoT can be utilized to supplement quiet treatment through remote observing and correspondence, and to monitor patients

as they move through a healthcare facility. Figure 1 shows the study of healthcare using IoT [4]. Embedded sensors are used with patients and their treatments for continuous remote monitoring.

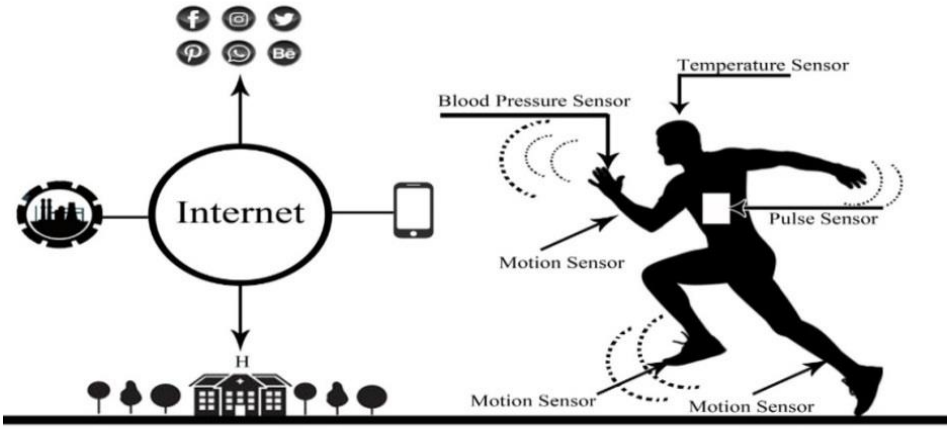


Figure 1. Healthcare using IoT

The classification of IoT Based Personalized Healthcare System is selected as two parts: Remote Monitoring, which is defined as numerous health dangers not discovered due to lack of preparation for incoming to active health monitoring systems [5] which is an issue being confronted everywhere through effective remote arrangements associated with the IoT to make it feasible to check patient health remotely. The data is analyzed and shared through wireless connectivity using a variety of complex algorithms and sensors. Clinical Care [6] which is defined as IoT, is utilized by hospitalized patients whose physiological status requires consistent close consideration; it provides a continuous automated flow of information. Thus, the quality of care is improved through constant attention, which in turn lowers the cost of care and eliminates the need for a caregiver to actively engage in data collection and analysis.

This paper generally grouped the discourse in two angles: services and applications. Applications are additionally isolated into two gatherings: clustered- and single -condition applications [7]. By using IoT, this sorting structure is arranged depending on today's obtainable healthcare solutions. This list is naturally unique and can be effectively improved by including extra administrations with unmistakable features and various applications covering both clustered and single-condition solutions. A clustered-condition application compacts with a number of diseases or conditions together in general, whereas a single-condition application mentions a specific disease or infirmity.

2. THE PROPOSED IoT HEALTHCARE ARCHITECTURE

Figure 2 shows the proposed architecture design. It consists of numerous devices connected through heterogeneous infrastructures. These devices are grouped based on their function. Each group is controlled by an ID zone (Intelligent Device Zone), which is responsible for managing the devices within the group. These groups can be classified as complementary or non-complementary based on the nature of their work and the types of devices they contain. The ID zone also determines the location of each device. Additionally, there is a Device Broker (DB), which acts as our gateway. It uses D2D (device-to-device) capabilities to ensure M2M [8] (machine-to-machine) device interoperability and connection to the communication network. Our server, the IoT AAA [9] server, is a program that manages user requests for access to computer resources. It provides authentication, authorization, and accounting (AAA) services. The AAA server interacts with network access, databases, gateway servers, and verifies user information. Also, it plays a crucial role in assigning IDs to users for accessing the network through the DB. Additionally, TNS (Thing Naming Server) allows devices to exchange data and information with each other by naming them according to the nature of their work.

Finally, the IoT architecture model has evolved into a network connected to an IoT cloud (Human Interface Point) [10], enabling applications and a control environment. This allows devices to communicate not only with each other but also with human interfaces like doctors and nurses. This facilitates seamless communication between doctors and patients, ensuring continuity of care.

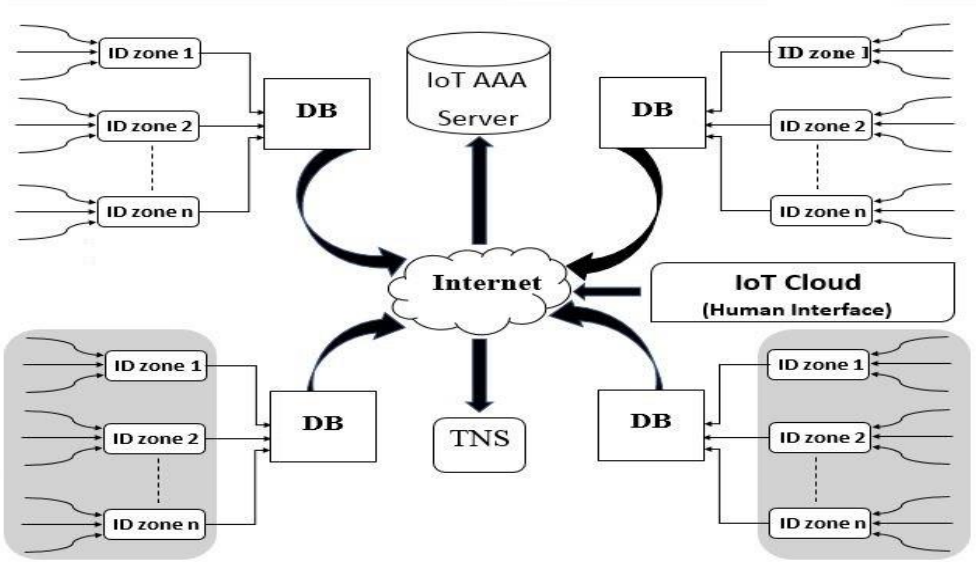


Figure 2. The proposed IoT healtheare architecture

3. THE PROPOSED IoT HEALTHCARE PROTOCOLS

Registration and authentication protocols on IoT network: We will apply this by describing figure 3, showing a simple flowchart. First, a medical device (MDx) will send a registration request to the IoT AAA server with ($K^{/}$) where $K^{/}$ refer to message integrity data transit. It is important that the medical device sends a request by $K^{/}$ secured by applying a hash algorithm using SHA-1 on its Kthing to become $K^{/}$. Secondly, IoT AAA server also must apply the hash algorithm using SHA-1 on its Kthing to become K/sever to can make comparison between $K^{/}$ and $K^{/}$server, in case the result is the same then AAA server will send registration confirm with ($ID_{encrypted}$, Random number) to the device broker (DB) that the medical device belongs to, giving identification of the medical device encrypted and a random number that mean process of encoding a message is done at AAA server, this encryption process happens by using Advanced Encryption Standard (AES), $K^{/}$ and a random number which generated by the AAA server in such a way that only authorized parties can access it. Thirdly, the device broker will send registration confirmation to the medical device with ($ID_{encrypted}$, ID_{broker}, Random no.). In this case, the MDx must do the decoration process for the data sent from DB by using the same random number that the server used before to know its identification (IDx) and which device belongs to (ID_{broker}). Finally, Medical Device will acknowledge the device broker, then DB acknowledges the IoT AAA server.

Authentication protocols are utilized to authenticate and confirm a client or computer by approving its character against a confided in personality. The most critical security capacities to secure the Internet of Things associated devices are [11, 12]: Authentication, Secure storage, secure communication and secure execution of code. Figure 4 shows a simple flow chart divided into two stages. The first stage explains how the medical device authenticates and verify both the identity of the device that is requesting authentication and the server providing the requested authentication by avoiding any external things (Risk Assessment) or unauthenticated things to be an access connection in our IoT healthcare system, then when the IoT AAA server identifies the ID of the Medical Device, it will make a permission for it to access.

This will be done first by sending an authentication request with ($ID_{encrypted}$) to an IoT AAA server; this $ID_{encrypted}$ is the encrypted medical device identification which we explained before in the registration protocol. Secondly, the AAA server will reply to the ID zone with authentication confirming with the same ($ID_{encrypted}$) that it actually resisted inside the AAA server and has permission to access it. Then ID zone will also send authentication confirmation to MDx with (IDzone), to inform MDx that it has the permission to access the server and the intelligent device zone it belongs to. The second stage, called Permeability of dealing in which MDx will send an information request to the AAA server, means medical devices want permission from the server to deal with other medical devices for connection or exchange data with each other. Then an IoT AAA server will confirm this request by sending an open session and MDx reply with acknowledgment.

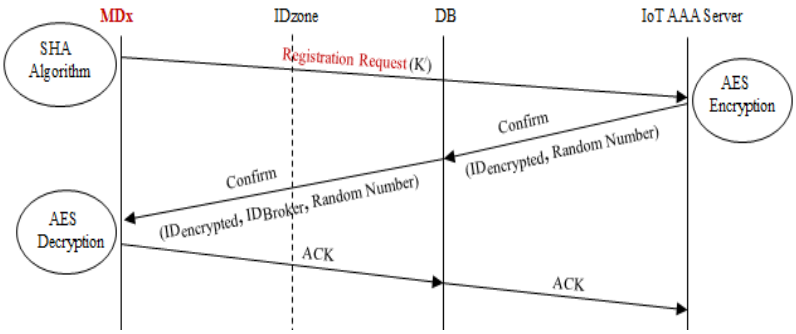


Figure 3. Security protocol for registration

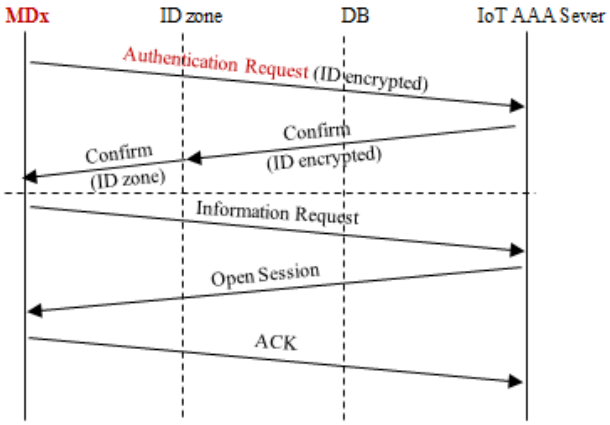


Figure 4. Security protocol for authentication

3.1. Four Modes Operation

Figure 5 explains the four modes of operation applied to the architecture proposed through four different states (normal, emergency, sleep, service). These modes operations for the reference nodes used in the model, namely Node A (temperature node), Node B (pulse node) and Controller (display node) respectively.

Select a mode depending on the temperature measurement (Normal, Critical). Firstly, the normal mode sends the measured temperature value or pulse value to display in a frame format for 1sec. Secondly, emergency mode is when the temperature is critical (out of the range). In this mode, node A should connect to, Controller to send the value, then connect to node B to send request to let it take the lead on display. In the service mode, you should listen to the incoming connections from node B or controller. Finally, sleep mode, which is node A, takes sleep every 5 seconds to save power.

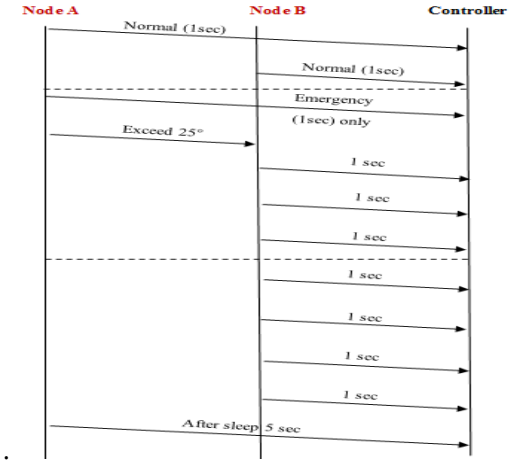


Figure 5. Modes of operations

3.2. Device want to communicate to device

This communication paradigm facilitates ubiquitous communications with full mechanical automation, where many intelligent devices connected by wired/wireless links interact with each other without direct human intervention. This communication between two devices can occur in three scenarios: Communication in the same ID zone, Communication in a different ID zone and Communication in a different location.

3.3. The Connection between two devices in the different location

The AAA server will be the primary key for this process, because it is the main factor in communication between DBs and all devices with each other. Figure 6 shows that MDx will send a connection request message to its ID zone for connection to another MD in a different location. Then, the ID zone will send this message to DB1, which is responsible for MDx. Secondly, DB1 will transmit the same message to the AAA server. In return, the AAA server will forward it to the right device broker (DB2) which is responsible for communication with the other device (MDy) in a different location. Thirdly, DB2 will send the message to IDzone2 and will reply by connection confirmation to DB2 again. Also, DB2 will send a connection confirmation message to the AAA server. Here comes the important role of the server where it will send a message to the device (MDx) for the final confirmation. Finally, communication between the two devices will occur.

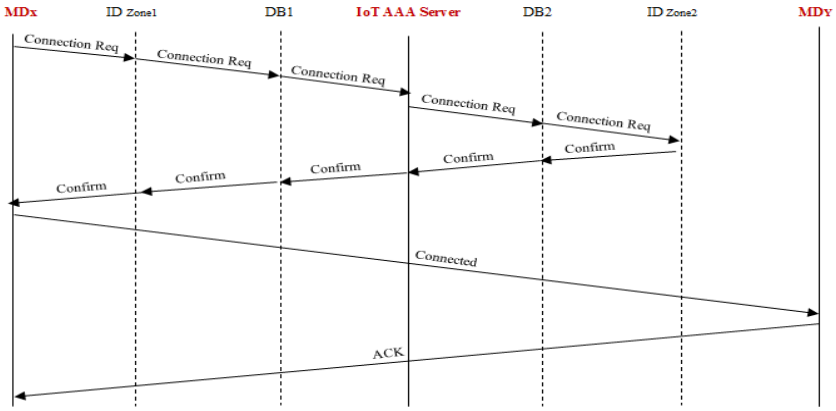


Figure 6. D2D in different location

4. SYSTEM ARCHITECTURE OVERVIEW

Design of block digram describes distributed pulse, room temperature and display systems based on IoT healthcare technology[13]. Figure 7 shows the designed system has been classified into three parts. The first part is a Pulse sensor connected with the development Board (Wi-Fi - Bluetooth) called the ESP Module. The second part is another Wi-Fi module with an LCD monitor display and the third part is a room temperature sensor with an ESP module. The important point in this system is that we create a network between these three parts for communication between them by using a Wi-Fi module in which each of them can be a transmitter and receiver at any time, depending on the priority for emergency cases.

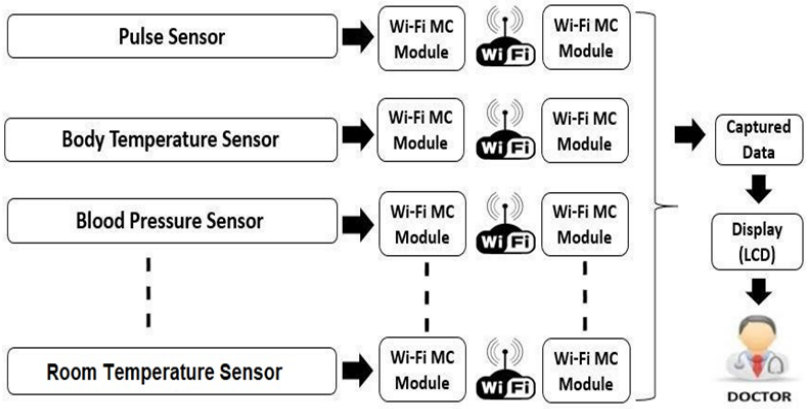


Figure 7. Block diagram

4.1. System decription

Figures 8, 9 and 10 show the flow charts for the designed system that has been classified into distributed heart pulse acquisition algorithm, room temperature acquisition algorithm and display acquisition algorithm based on IoT healthcare technology.

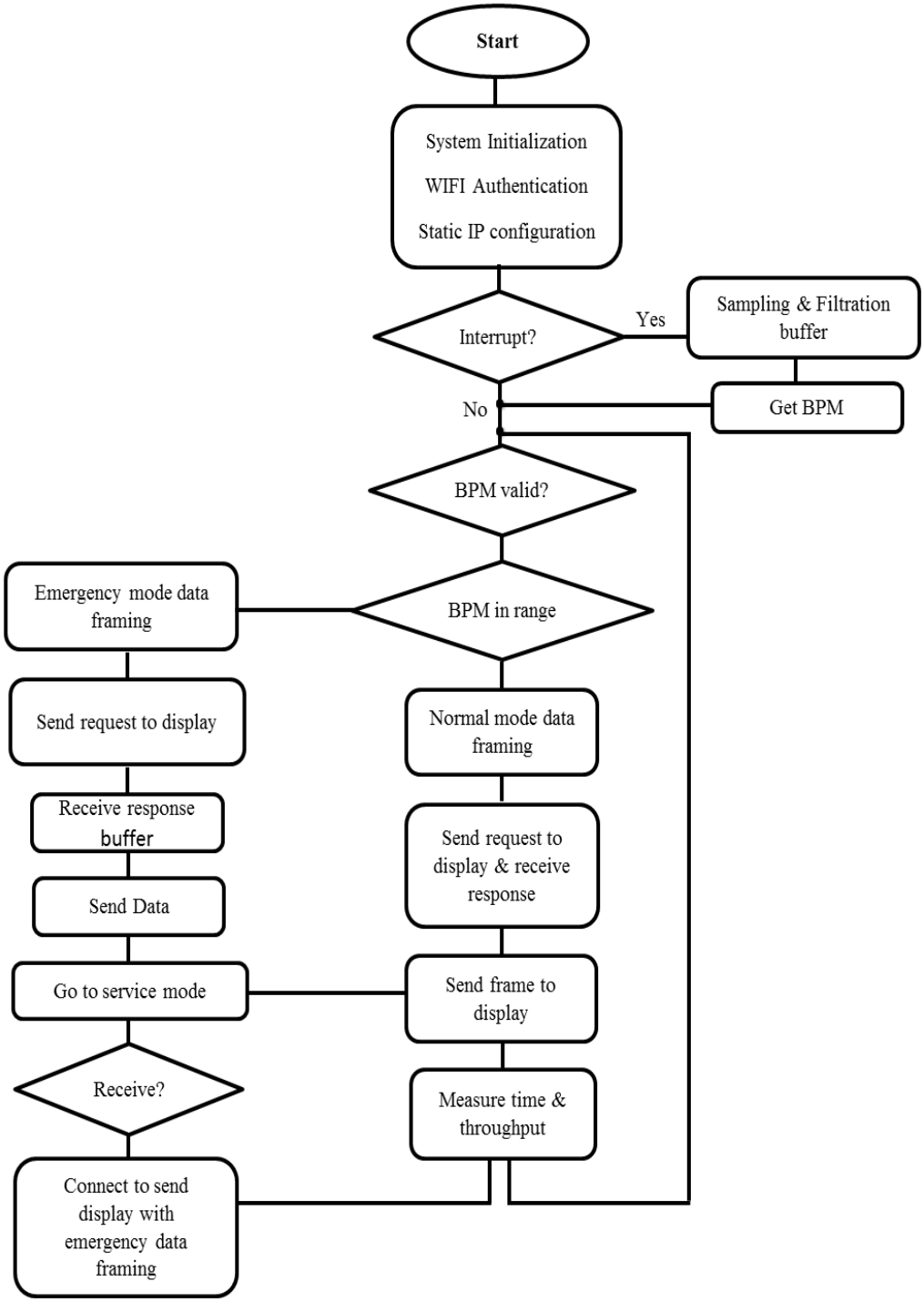


Figure 8. Heart pulse acquisition algorithm

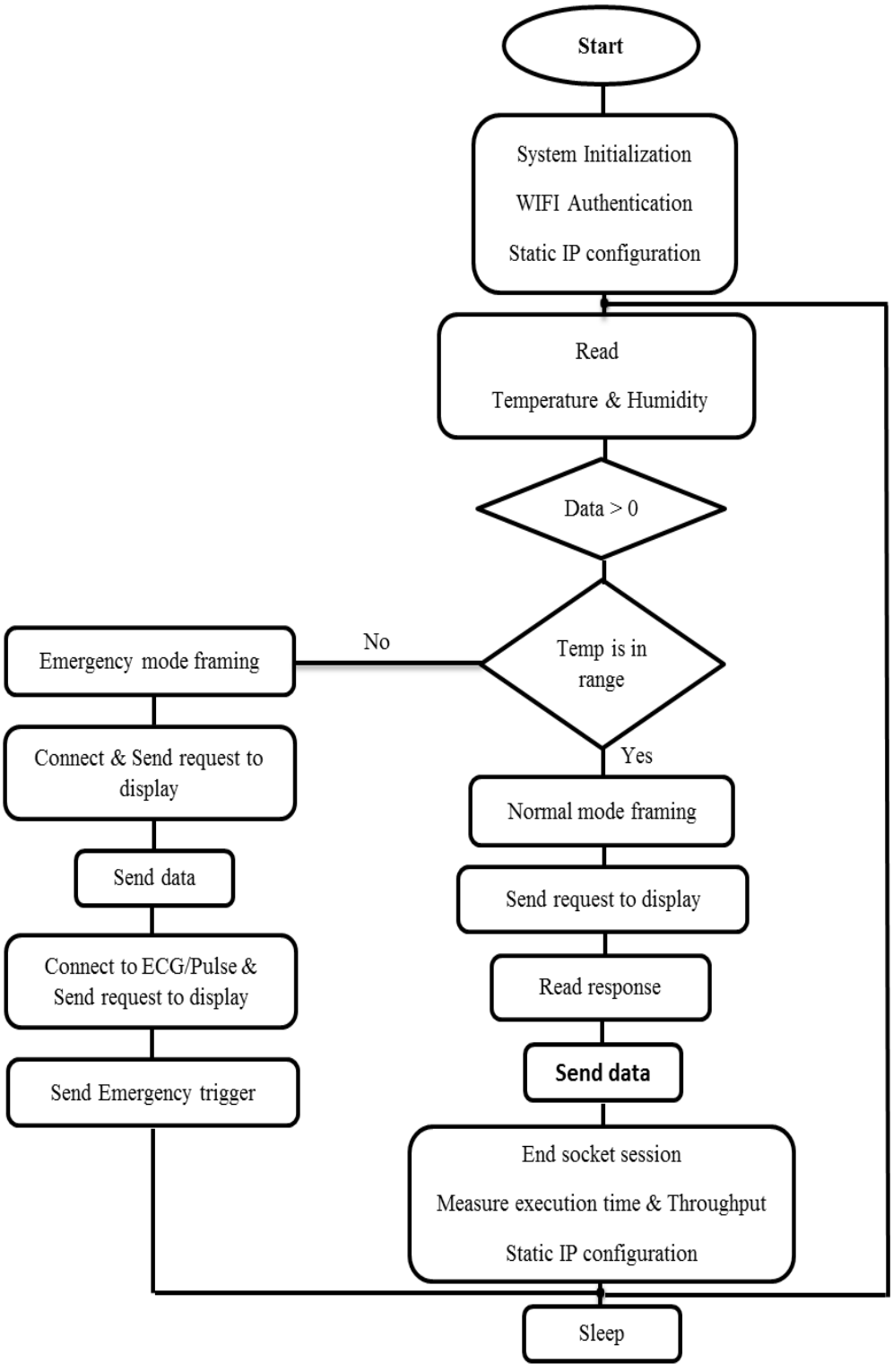


Figure 9. Temperature acquisition algorithm

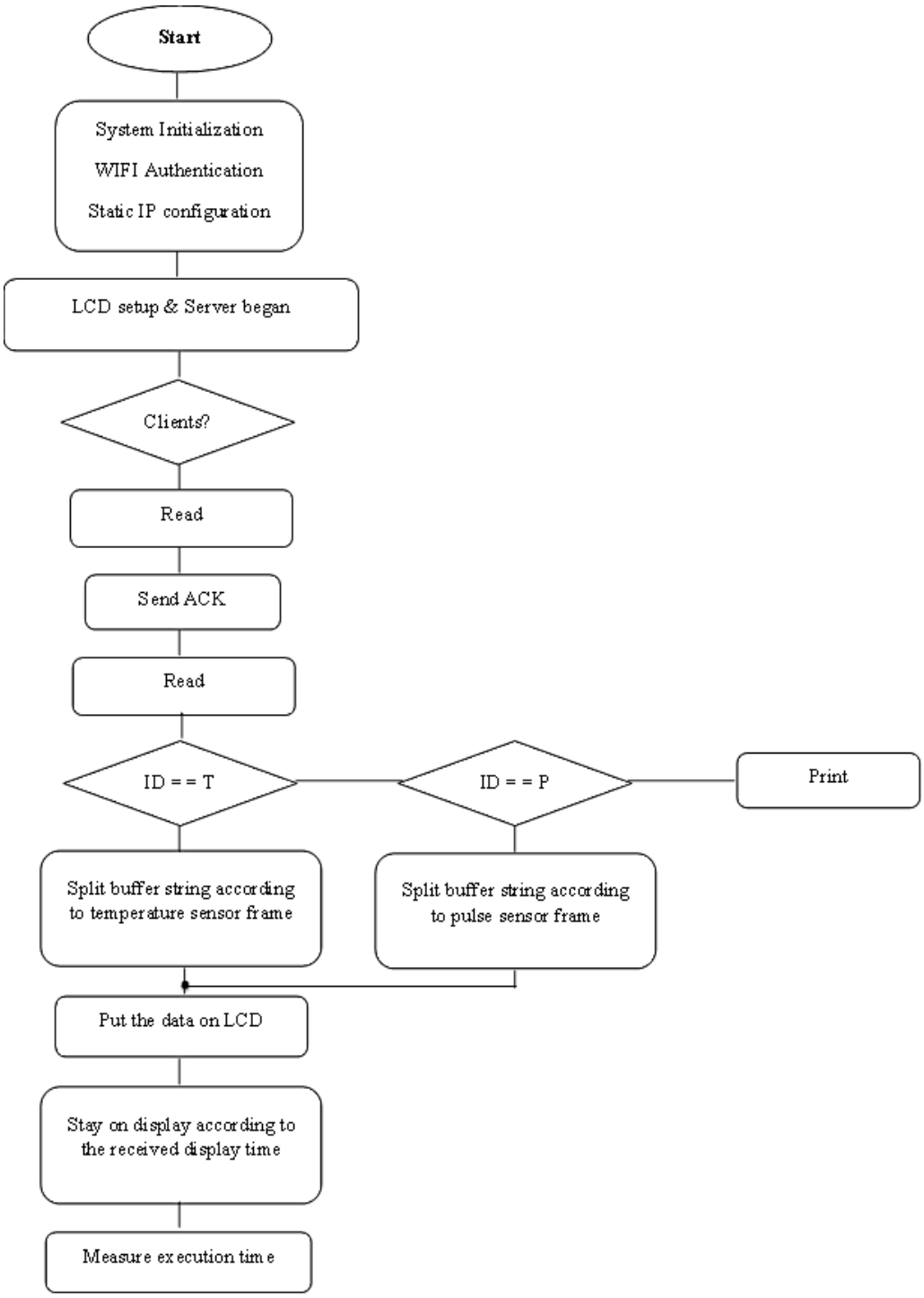


Figure 10. Autonomous display acquisition algorithm

5. RELATED WORK

Rita Zgheib, Emmanuel Conchon and Remi Bastide [14] offer a new Internet of Things architecture for IoT healthcare applications. The architecture concentrates fundamentally on the principles of weak coupling and of semantic data exchange. Also, they offer a software architecture that depends on OWL (Message Oriented Middleware) and on semantic data representation. This work deals with two main notions: Semantic representation of sensor data and middleware solutions for IoT applications. These two notions are linked to originating a new IoT environment: a semantic middleware for health applications.

Pooja M. and Deepthi Das [15] concentrate on the comparative analysis of smart healthcare architecture depending on research for each architecture and propose which architecture is preferable to implement in the Smart Hospitals. The present work is to compare the 4 architectures.

- Remote monitoring in wearable and personalized health care.
- Network model for patient monitoring using IoT cluster.
- Remote patient monitoring based on IoT-cloud architecture [16].
- IoT healthcare architecture.

Out of which deduce saying that architecture 3 is more credible architecture which uses advanced technologies like Zigbee, cloudlet and data analytics and visualization. These techniques ease the analysis of the gathered data and simplify the clinician to make the suitable decision. Usage of Zigbee and cloudlet lowers the design cost.

David Lake, Rodolfo Milito, Monique Morrow and Rajesh Vargheese [17] Achieving the main challenges must be overcome, especially concerning privacy and security. Examine using case scenarios, and advance a secure architecture framework. Also, the authors offered an architecture and framework that backups the development of a secure and privacy-preserving M2M/IoT infrastructure. The authors have further specified core standards and industry bodies where eHealth-M2M-IoT standardization is in advance.

6. DISCUSSION

The proposed architecture addressed a formulation study of a typical IoT architecture model for healthcare applications that targets patient status tracking based on internet of things technology. The internet of things as a novel approach will enable intra-communications between independent and autonomous objects that collaborate together to collect a complete picture of the services delivered to patients and enable the actuation towards tuning such services. The philosophy behind the architecture is to enable sensory platforms to operate and actuate independently and seamlessly with other sensory platforms in the same ecosystem without a common control algorithm that regulate and manages the operation of such devices. Accordingly, the network of sensors could accept foreign ad hoc sensors that could talk with any other sensor of the same type or of different type as long as the protocol of communication (e.g., standard MQTT protocol) is supported. The foreign node will discover the nodes and start the integration process with the network after a few minutes of being introduced to the network. For instance, in the model introduced above, the display unit is considered an object that can receive data from client nodes and display it. The edge proposed in the architecture is to abstract the layer between the sensory device and the display unit, and thus all sensory devices on the network have the capability to send their data to the display unit based on the display unit's request. From the user perspective, the user should ask the display unit to display specific parameters which in turn ask specific client devices to push back the requested data. This means that the network of sensors is formulated on an ad hoc basis with no need for a full logical connection between devices associated with the network.

The architecture model that is proposed in this paper is measured and benchmarked according to the following design principles:

- Power relative consumption
- Bandwidth relative consumption
- Switching relative consumption
- Service reliability

6.1. Power relative consumption

The system architecture enables a power-oriented environment through power aware protocols discussed in section 3 that control the state jump of the system through three different states (normal, emergency, sleep). Figure 11 shows the normal mode operation for the reference nodes used in the model presented in section 4, namely temperature node, pulse node and display node respectively. During normal operation, initially each device starts in normal mode, which could range from 0.2W in some devices to 1.1W in other devices. The range span depends on the type of processing platform, the application complexity and the circuit design [16]. However, the study in place does not consider the aforementioned parameters that are all related to hardware quality of design, but rather focuses on the impact of architecture and related protocols on energy savings as a result of power oriented intelligent operation and, accordingly, the impact on the battery life, which is a key factor in IoT applications.

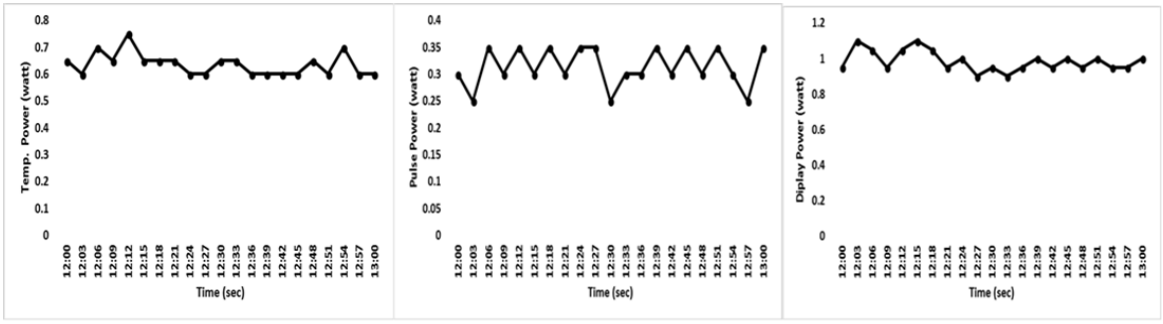


Figure 11. Power relative consumption in normal mode

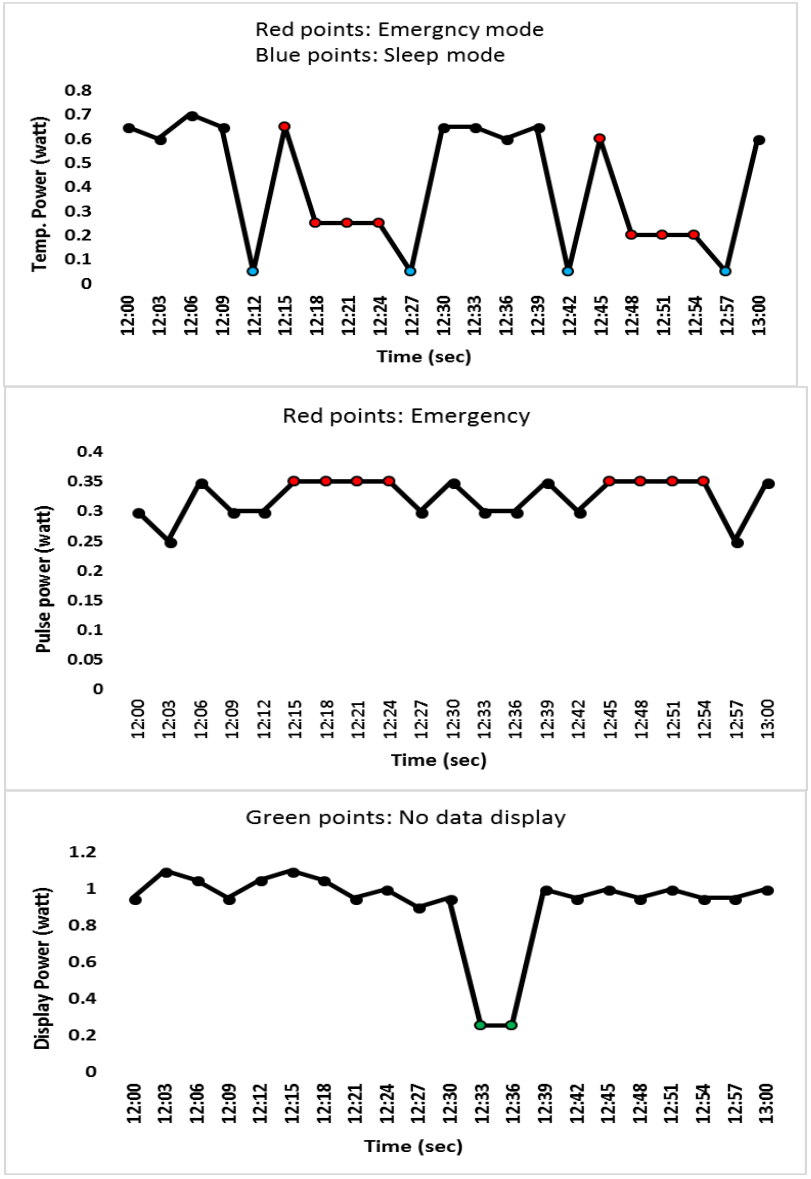


Figure 12. Power consumption

A lab experimental emulation test is run on a test model of three devices interacting with each other in an autonomous way based on protocols and architecture discussed in sections 3 and 4 respectively. The

model is composed of three devices (room temperature monitor (RT), human pulse monitor (HP), and common display unit (CDU)). A scenario is built on the model for a one-hour run, and the RT device is configured to go to sleep every 12 seconds as the only device allowed to sleep without impacting the core value of system operation. After 13 sec of operation, the temperature in the room exceeds the threshold level and the system change its state from normal to emergency mode and thus the power consumption on pulse node increases from average power consumption the 0.3W to average 0.7W as the rate of message transmission increases as a result of the operation as explained in the protocol explained in section 3. Once the emergency event is resolved, the system jumps back to the normal mode, and the CDC unit has the opportunity to go to sleep based on the synchronization protocol explained above, Figure 12 shows the display unit (CDU) power consumption rate decreases to 0.3W from 0.9W as a result of change of the CDU state from emergency back to normal.

The power relative consumption is then calculated based on the experimental scenario and the results are as follows:

$$\eta\text{Temp} = \frac{\text{area under the curve in emergency mode}}{\text{area under the curve in normal mode}} = \frac{X}{A} = \frac{0.36775}{0.62175} = 0.59 \quad (1)$$

$$\eta\text{Pulse} = \frac{\text{area under the curve in emergency mode}}{\text{area under the curve in normal mode}} = \frac{Y}{B} = \frac{0.31425}{0.30825} = 1.019 \quad (2)$$

$$\eta\text{Display} = \frac{\text{area under the curve in emergency mode}}{\text{area under the curve in normal mode}} = \frac{Z}{C} = \frac{0.94125}{0.98175} = 0.95 \quad (3)$$

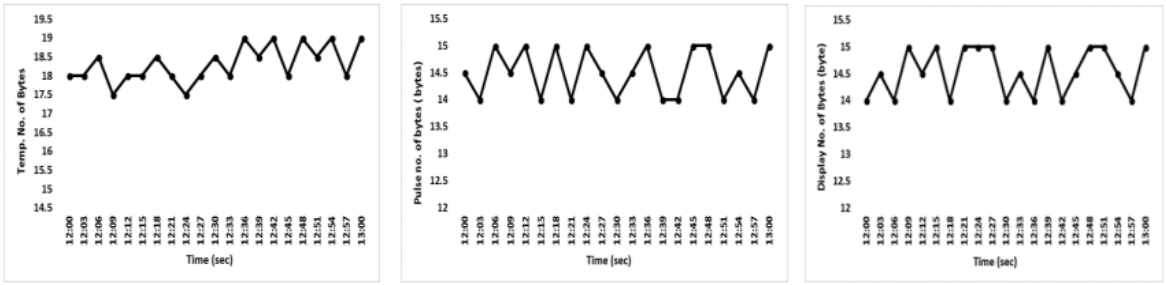
Where η is power relative consumption.

However, we can measure the whole proposed system's power relative consumption as the ratio between the total dissipated energy for sum all nodes in both modes (emergency mode/normal mode).

$$\text{The total dissipated energy in both modes} = \frac{0.36775+0.31425+0.94125}{0.62175+0.30825+0.98175} = 0.849 \quad (4)$$

6.2. Bandwidth relative consumption

The number of bytes represents the throughput that the proposed system produces. The throughput is a measure of how many units of information a system can process in a given amount of time. The value of the number of bytes increases and decreases depending on the proposed system in which mode, changing in time and type of scenario. Figure 13 shows the relationship between the number of bytes and time per second when the temperature system is responsible for transmitting data to other devices.



(a) Temperature System (b) Pulse System (c) Display System

Figure 13. Bandwidth relative consumption in normal mode

Bandwidth relative consumption was calculated in this section by measuring the number of bytes for each system. As the number of bytes increases, the bandwidth decreases. Figure 14 shows the values of bandwidth relative consumption in emergency mode. In the temperature curve, drop value that happen at the three points as the node enters the emergency case (Don't send data). So, at 12:15 seconds, the number of bytes decreased but the pulse curve, at the moment it started to send data, so acheived high value of bytes.

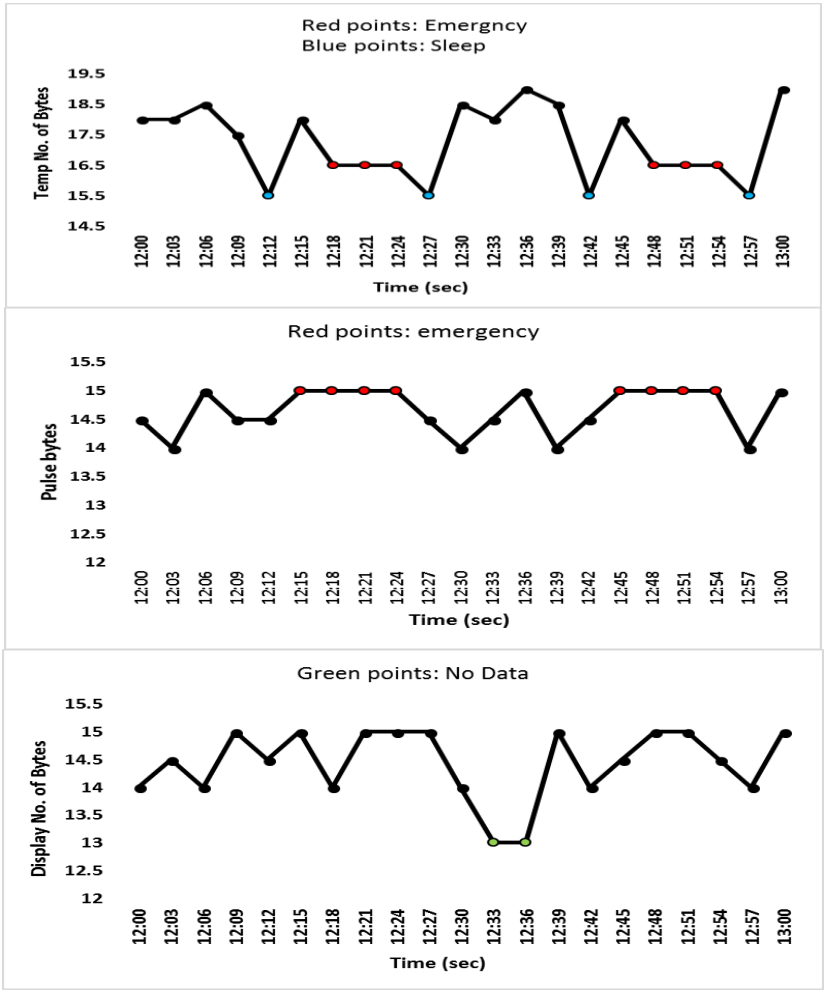


Figure 14. Bandwidth relative consumption in emergency mode

$$\eta(\text{Temp.}) = \frac{\text{area under the curve in emergency mode}}{\text{area under the curve in normal mode}} = \frac{17.205}{18.38} = 0.93 \quad (5)$$

$$\eta(\text{Pulse}) = \frac{\text{area under the curve in emergency mode}}{\text{area under the curve in normal mode}} = \frac{14.5975}{14.4925} = 1.007 \quad (6)$$

$$\eta(\text{Display}) = \frac{\text{area under the curve in emergency mode}}{\text{area under the curve in normal mode}} = \frac{14.455}{14.53} = 0.99 \quad (7)$$

However, we can measure the whole proposed system's bandwidth relative consumption as the ratio between the total dissipated energy for sum all nodes in both modes (emergency mode/normal mode).

$$\text{The total dissipated energy in both modes} = \frac{17.205+14.5975+14.455}{18.38+14.4925+14.53} = 0.975 \quad (8)$$

6.3. Calculation the execution time for each scenario

The values in the following Table 1 show calculations and measurements of the scenario time (execution time) per millisecond for the different scenarios that may occur for each system (node). Where the readings are taken according to the device that is working, which sends the data and the device to which it is connected, as well as in terms of different modes of devices (sleep mode - emergency mode - normal mode). Also, as shown in table 1, take into account where the receiver device may be responsive or not and takes readings in each case.

Table 1. Execution scenario

Steps	Execution Time (ms)
Temperature Display time in normal mode	1312
Temperature Display time in sleep mode	10000
Pulse node display time in emergency mode (positive response to interrupt of temperature node)	1793
Pulse node display time in emergency mode (negative response to interrupt of temperature node)	1304
Pulse node display time in Normal mode (DHT do not send an interrupt)	1011
Display node display time in case DHT do not send an interrupt	1312
Display node display time in case pulse node in emergency (positive response)	11017
Display node display time in case pulse node in emergency (Negative response)	2020

6.4. Switching relative consumption

Table 2 shows the latency interrupt, which means the time consumed when a system switches from a scenario to another. The types of interruption that may occur to which the proposed system is determined by the type of sensor it contains. The causes of this interruption are either because of the increase in temperature (this happens in the emergency mode) or the arrival of the heartbeat at abnormal values (this also happens in the case of emergency mode). In addition to these two cases, there is the third case in which the temperature sensor doesn't send any data (this happens in sleep mode). This means the entry of the sensor to another mode, whether (emergency mode, sleep mode and normal) or vice versa. These values are taken on the condition of a particular person at a given moment, but vary according to the situation of each person or patient and the circumstances surrounding it and the place in it.

Table 2. Time consumed when system switch from one scenario to another

Measured Parameter	From Scenario	To Scenario	Switch time	Interrupt
Temperature Display	Display every 3 sec	Display every 1 sec	65 sec	Temperature exceeds 25
Temperature Display	Display every 3 sec	Normal or Emergency modes	5 sec	Temperature sleep mode
Pulse Display	Display every 3 sec	Display every 3sec	140 sec	BPM>150& <20

7. CHALLENGES FACED BY THE PROPOSED IoT HEALTHCARE.

IoT healthcare systems hold immense potential to revolutionize healthcare delivery, but they also face several significant challenges and limitations that need to be addressed. Though the proposed work supplies better results, there are still a few limitations that can be improved, such as:

- **Limited battery life:** Battery-powered devices may require frequent charging or replacement, adding to logistical challenges and potentially impacting the user experience.
- **Data security and privacy:** Healthcare data is highly sensitive and vulnerable to breaches. IoT systems collect and transmit vast amounts of personal health information (PHI), making them attractive targets for cyberattacks.
- **Cost and Scalability:** Deployment and Maintenance Costs is the initial investment in purchasing, deploying, and maintaining IoT devices can be substantial. Also, Scalability Challenges: Scaling up an IoT system to accommodate a larger user base can be complex and require significant infrastructure upgrades.
- **Limited device reliability:** Technical issues and malfunctions in sensors or devices can disrupt data collection and compromise the reliability of the system.

By acknowledging these challenges and actively working towards solutions, we can ensure the responsible and ethical development and implementation of IoT healthcare systems that truly benefit patients and healthcare providers. It's important to remember that while the technical aspects of IoT are crucial, understanding and addressing the challenges is equally important for successful real-world applications.

8. CONCLUSIONS

The healthcare system has minimized complication and complexity with the environment of IoT. This paper surveys advances in IoT healthcare technologies and presents various healthcare system framework of architecture, protocols, and algorithms in which the proposed architecture ensure that each individual device is autonomous and can work independently with the surrounding environment, increase the efficiency of systems operation and enhance the reachability of different type of devices on the same patient or across several patients by the physician. The idea that has been proposed in this system requires some basic hardware which can easily be procured.

In the future, further on proposing to make some additional changes to the system and on applying the same concept if we scale up the number and diversity of devices to include more complimentary ones like pulse oximeters, body temperature or blood pressure devices that need to communicate together intelligently and autonomously in the same patient or across patient categories.

REFERENCES

[1] S. M. Riazul Islam, Daehan Kwak, Mahmud Hossain and Kyung-sup KWAK , "The Internet of Things for Health Care: A Comprehensive Survey," The journal for rapid open access publishing (IEEE Access),vol. 3,pp. 678-708,2015.

[2] Al-Fuqaia, A., Gutierrez, M., Yousuf, M., and Salahi, "The role of the Internet of Things in healthcare: a survey", IEEE Communications Surveys & Tutorials, vol.3,2015.

[3] Mark Kung, ,Gartner Research vice president, Chapter one, Leverage of IoT, April 2017.

[4] Siobhan Babu, K. Srikanth and I. Lakshmi Narayana, "IoT for Healthcare" , International Journal of Science and Research (IJSR), vol. 5, pp. 322-326, 2016.

[5] Bayadir A. Issa and Qabeela Q. Thabit, "Review in IoT for Healthcare in Our Life" , Iraqi Journal for Electrical and Electronic Engineering, pp.9-19, June 2022.

[6] David Niewonly, "How The Internet of Things is Revolutionizing Healthcare", Freescale Semiconductors, 18 oct 2013.

[7] Dr PM Murali, G.Ramachandran and S.Vaishnodevi, "A HEALTHCARE APPLICATION OF IOT TECHNOLOGIES" , International Journal of Scientific Research and Review, Vol.7,pp.523-526, 2018.

[8] Hamza Aldabbas, Dheeb Albashish, Khalaf Khatatneh and Rashid Amin, "An Architecture of IoT-Aware Healthcare Smart System by Leveraging Machine Learning" , The International Arab Journal of Information Technology, Vol. 19, pp.160-171, March 2022.

[9] Ajit A. Chavan and Mininath K. Nighot, "Secure and Cost-effective Application Layer Protocol with Authentication Interoperability for IoT," Procedia Computer Science (ELSIVER), pp. 646 – 651, 2015.

[10] Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci and Silvana Andreescu, "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges", in IEEE International Conference on Services Computing, pp. 285-292, 2015.

[11] Dominik Samociuk and Blazej Adamczyk, "Secure gateway for Internet of Things with internal AAA mechanism," Institute of Informatics Silesian University of Technology Akademicka, vol. 28, pp. 17-35, 2017.

[12] Abdullah A. Al-Atawi, Faheem Khan and Cheong Ghil Kim, " Application and Challenges of IoT Healthcare System in COVID-19", Sensors, vol. 22, 2022.

[13] Ms. Shinde Sayali P and Ms. Phalle Vaibhavi, "A Survey Paper on Internet of Things based Healthcare System, " International Advance d Research Journal in Science, Engineering and Technology, vol. 4, pp.131-133, 2017.

[14] Rita Zgheib, Emmanuel Conchon and Remi Bastide , "Engineering IoT Healthcare Applications: Towards a Semantic Data Driven Sustainable Architecture, " Research Gate, pp. 1-12, 2016.

[15] Pooja M. and Deepthi Das, "Comparative Analysis of IoT based Healthcare Architectures", International Journal of Computer Applications (0975 8887), vol. 161, pp. 33-37, March 2018.

[16] Vaneeta Bhardwaj, Rajat Joshi1 and Anshu Mli Gaur, "IoT-Based Smart Health Monitoring System for COVID-19", SN Computer Science 3:137, pp.1-11, 2022.

[17] David Lake, Rodolfo Milito, Monique Morrow and Rajesh Vargheese, "Internet of Things: Architectural Framework for eHealth Security," Journal of JCT, vol. 3 & 4, pp. 301-328, 2013.