International Journal of Safety and Security Engineering
Vol. 13, No. 6, December, 2023, pp. 1001-1014
Journal homepage: http://iieta.org/journals/ijsse

Advancing Public Health Monitoring through Secure and Efficient Wearable Technology

Sahar L. Qaddoori[1*], Ina'am Fathi[2], Modhar A. Hammoudy[2], Qutaiba I. Ali[2]

[1] Electronic Department, Electronics Engineering College, Ninevah University, Mosul 00964, Iraq
[2] Computer Engineering Department, Engineering College, Mosul University, Mosul 00964, Iraq

Corresponding Author Email: sahar.qaddoori@uoninevah.edu.iq

https://doi.org/10.18280/ijsse.130603

Received: 21 September 2023
Revised: 16 November 2023
Accepted: 29 November 2023
Available online: 25 December 2023

Keywords:
cyber security, WBAN, wearable device, continuous public health monitoring, energy consumption

ABSTRACT

Public health monitoring system, which are an integral part of diseases monitoring system and policies formulation, progressively rely on complex networks to collect and analyze the data then make the public health statistics. These systems play an essential role in detecting diseases outbreaks, constraining spread directions, and formulating polices for the public health. This manuscript proposes development a continuous health monitoring system, which is designed to monitor the individual health cases in real time. Where, the system is used to securely transfer the participating individual's data to a medical server, to ease early detection of abnormal health cases. Firstly, the most important contribution of this manuscript is the recommendation to implement a continuous health monitoring system as a public health service. In order to improve the proposed system, experimental analysis are conducted to focus on improving network performance and reducing price. These analyses include assessing different network protocols and their configurations to specify the most effective and reliable method to transfer data. While the second contribution is to develop a new wearable device characterized by its lightweight design and low power consumption. This device considers as one of the basic components for the proposed system. It is provided by different sensors to monitor numerous of health conditions and is able to quickly switch between sleep and wake up modes to conserve energy. These features make the proposed device an effective tool in monitoring public health. Furthermore, this manuscript suggests a security model designed especially for wearable devices with constrain resources to meet a serious need in the age of digital information security. The suggested security model assurances the secure handling and transferring the sensitive health data, which is considered the most important demand of public health monitoring system.

1. INTRODUCTION

The integration of modern wearable devices and Wireless Body Area Network (WBAN) considers an important tread in the arrival of a continuous public health surveillance system in real time [1-3]. These systems include the wearable devices designed to attached or be worn to the human body like smartwatches, fitness trackers, medical sensors, and etc. Where, these devices are capable of collecting countless of biological data, such as blood pressure, heart rate, temperature, activity levels, and others [4, 5]. They are equipped with sensors, processors and communication units, which are able to capture, analyze, and wirelessly transfer the health-related data [6]. While, WBAN networks, which are represented the interconnected networks of wearable devices, facilitate to exchange the health-related data either inside the network or through central monitoring system [7].

The corporation between wearable devices and WBAN networks in the public health monitoring system presents significant advantages. Because of the comfort and ease of these devices, they allow for uninterrupted monitoring and smoothly coordinating with daily events. In addition, they are available real time data that is crucial for medical intervention at suitable time and development the individual healthcare approaches [8, 9]. Where, WBAN network improve this ability by allowing continuous communications among the wearable devices, so it is enhanced an integrated environment to transfer and analyze healthcare data [10, 11]. This integration introduces for healthcare providers an inclusive visible to help them making overall clinic decisions. Furthermore, these techniques enabled the individuals to actively share in managing their health that leads to improve the health outcomes. On the other hand, the secure and effective implementation of the public health monitoring system is not without some challenges, such as issues surrounding data privacy, scalability, interoperability, and etc. [2]. So, the challenges solutions are necessary to fully achieve the potential of wearable technology in public health monitoring and to ensure the protection and proper use of sensitive health data.

The present sense of public health monitoring systems, which progressively depended on the wearable devices, reflects the intersection between the technology innovation and the healthcare requirements. The advancement in the

wearable devices facilitate to collect the data in real time, which is a vital for personalized health monitoring. But, the growing use these devices raises big concerns about the security of sensitive health-related data. So, greater emphasis has been placed on the necessity of developing secure and robust system capable of securing private health information in light of global health emergencies like the COVID-19 pandemic, which had enlarged the need for effective and secure solutions [12].

The wearable devices with WBANs integration promise to enable proactive, individualized, and efficient healthcare interventions. Thus, this paper focuses on leveraging the synergy of wearable devices and WBANs to establish an effective public health monitoring system.

Within the WBANs, communication occurs at three distinct tiers: intra-WBAN, inter-WBAN, and beyond-WBAN communications [13, 14]. Intra-WBAN communication, the first tier, comprises numerous sensors either worn or implanted in the human body. These sensors employ short-distance transmission techniques for the relay of physiological data. The second tier, inter-WBAN communication, involves the use of smartphones, laptops, and other intelligent electronic devices as intermediaries [15, 16]. These devices utilize wireless technologies such as 3G/4G/5G and WLAN to transmit data from the sensors to the terminal center, which represents the third tier of communication. Beyond WBAN, this terminal center typically consists of cloud servers where the collected data is stored and analyzed for various purposes including monitoring and diagnosis [17, 18].

Maintaining the security of medical data in continuous health monitoring systems represents a formidable challenge, necessitating the implementation of innovative and effective security strategies. These strategies must not only cater to health monitoring requirements but also guarantee the secure transmission and storage of health data [19]. However, due to the intrinsic limitations of WBANs in terms of resources (i.e., communication bandwidth and energy supplies are both scarce), most traditional security solutions designed for other networks simply cannot be applied directly or effectively to WBANs [10, 11]. As a result, security in the WBAN becomes an important research question raising unique design problems of these networks.

The aim of the manuscript is to create a continuous health monitoring system that makes use of wearable devices which securely transfer and store health data on a central, medical-based server. The principal contributions of this work are as follows:

(1) The proposal of a health monitoring system, envisaged as a public service, to provide accurate health information and facilitate the tracking of intervention effectiveness.

(2) The execution of experiments aimed at optimizing network performance and reducing costs within the proposed public health monitoring system. This involves an analysis of various network protocols and configurations to ascertain the most efficient and reliable methods for data transmission.

(3) The development and implementation of a wearable device characterized by its lightweight and low-power consumption features. This device is designed to efficiently alternate between sleep and wake-up modes, thereby conserving energy.

(4) The formulation of an innovative and efficient security model specifically tailored to meet the constraints of resource-limited wearable devices.

The structure of this paper is as follows: Section 2 presents related works, providing a comprehensive overview of the existing literature. Section 3 identifies the research gaps, setting the stage for the subsequent contributions of this study. The proposed public health monitoring system is described in detail in Section 4. Section 5 delineates the research methodology employed throughout the study. The selection and implementation of the platform are discussed in Section 6. Section 7 addresses potential security threats, detailing the proposed security model, its implementation, and a thorough security analysis. Network performance, analyzed through various network configurations and routing protocols, is elaborated upon in Section 8. A comparison with previous works is systematically tabulated in Section 9. The paper concludes with Section 10, summarizing the findings and outlining future research directions.

2. RELATED WORKS

Recently, WBAN has become as a major point in research, due to its effective application in public health monitoring system [20]. During the last five years, WBAN has witnessed a lot of research being conducted, covering a wide range of topics from design and challenges to implementation issues [16]. In addition, WBAN security has received increasing attention in public health monitoring applications, through the presentation and development of several security models.

Hassan et al. [21] presented a hybrid model that integrates both local and cloud-based components to monitor chronically ill patients at their homes. The cloud-based component is responsible for managing the huge data generated by the surveillance systems, while the local component becomes active in the event of an Internet or cloud system letdown. Using context-sensitive analysis technologies, the model monitors patients' physiological signs, surrounding conditions, and activities, effectively identifying health states in real time. It has been shown to be particularly effective in detecting emergency situations in patients with blood pressure disorders.

Al-Naggar and colleagues [22] developed an efficient system for real-time monitoring of different physiological signs, such as electrocardiogram, heart rate, respiratory rate, blood oxygen saturation, and temperature, using smartphones. Their design is powered by high performance, included features such as automatic alerts and warning transmissions, and improved security through multiple methods.

Rezaeibagha et al. [23] developed a wearable monitoring system leveraging the Internet of Things (IoT), which ensures the secure transmission of data frequently collected from IoT wearable sensors. In this system, the data sender, typically a patient, transmits their health data securely to their physician. The system employs an innovative authenticated homomorphic encryption technique to encrypt the data, thereby preventing the data collector, such as a cloud server, from decrypting and altering the collected data. However, this approach still allows the data collector to perform basic computations for statistical analysis.

Ryu and Kim [24] proposed a privacy-preserving authentication protocol for WBANs used in healthcare services. This protocol employs lightweight one-way hash functions and exclusive-or operations, yielding enhanced privacy and security features compared to similar protocols. It is both computationally and communicationally efficient and has been rigorously validated through formal security proofs using BAN logic and the ProVerif tool. Noor et al. [25]

introduced a novel framework, termed a secure channel-free certificateless signcryption scheme, based on a hyperelliptic curve for WBANs. This scheme meets various security requirements and is lightweight in terms of computational and communication costs. Unlike traditional signcryption schemes, it eliminates the need for a secure channel for key distribution and avoids issues related to certificate management and key escrow, also offering lower computation costs.

Ramaswamy and Gandhi [26] presented a trust model for secure communication in WBANs, focusing on node and data trust. Their proposed lightweight protocol, compared to non-cryptographic protocols, incurs low overhead and demonstrates superior performance in throughput, packet delivery ratio, and minimal delay. Extensive simulations have proven its effectiveness in preventing a range of attacks, including on-off attacks, selfishness attacks, sleeper attacks, and message suppression attacks.

3. RESEARCH GAPS

There are several research gaps in the field of public health monitoring systems, including: Scalability, Real-time data analysis, Security and Data privacy, Interoperability, User engagement, and Cost-effectiveness. These gaps are defined as follows respectively:

(1) Most public health monitoring systems are designed for a limited number of users or a small geographic area. One of the paper's aims is to handle a large number of users efficiently, making the system adaptable to varying user demands.

(2) Public health monitoring systems produce large volumes of data in real-time. The proposed system directly attends to the requirement underscored in this research gap by promptly identifying and addressing public health threats. This aligns with the necessity for efficient tools for real-time data analysis.

(3) Public health monitoring systems gather sensitive health data, and there is a need to confirm that this data is reserved secure and private. The employment of a new security model in the suggested system directly targets the security gap and data privacy.

(4) Public health monitoring systems often use different data formats and protocols, making it challenging to share data between systems. The secure transfer and storage of data in the suggested system contribute to treating the interoperability gap. By emphasizing continuous data exchange and suggesting a unified framework.

(5) Public health monitoring systems are only effective if users are engaged and motivated to use them. There is a need for user-centered design approaches to ensure that public health monitoring systems are user-friendly and meet the needs of their intended users. Where, the proposal of a health monitoring system as a public service underscores the importance of user engagement.

(6) Public health monitoring systems can be expensive to implement and maintain. By analyzing network protocols and configurations to identify efficient options, the system aligns with the objective to provide a cost-effective solution deployable in resource-constrained settings.

Addressing these research gaps will require collaboration between researchers, public health practitioners, and policymakers to develop innovative solutions that can improve public health monitoring and response.

4. PROPOSED SYSTEM DESCRIPTION

Generally, public health monitoring systems play a critical role in protecting the health of communities. By providing real-time data, accurate information, and tracking the effectiveness of interventions, these systems help to ensure that public health policies and practices are evidence-based and effective. In this manuscript, health monitoring service is presented as a public service, by gathering the participant's vital information and storing in a cloud server to get the general health statistics for the communities. It is possible to subscribe to this service by purchasing a particular equipment that captures the vital data of the individual then visiting the website for registration. Figure 1 depicts the proposed system's description. There are a variety of sensors that detect the participant's vital data and are incorporated on the embedded device known as a wearable device (more information about wearable device in section 6). It may be located anyplace near the participant's body (such as in the pocket) and has a wireless adaptor that allows to communicate with the nearest specialized gateway. Because the health monitoring service is a public service, so many specific gateways must be speared inside and outside the buildings. These gateways have indoor range (connected multiple Wearable devices inside the building) or outdoor range (connected multiple Wearable devices outside a building). Where, these gateways receive the participants' vital information from Wearable devices during a periodic basis (for example, every one minute) in order to collect them and then arrange them as a file to send it to the cloud server which responsible for this service on a constant schedule (e.g. every half hour). The cloud server receives the file from each gateway to extract the specific information for each participant and save it in the participant's database. Afterthought, the participants' vital data will be checked to get the statistics to know if there is any abnormal thing.

Based on Figure 2, the proposed health monitoring service passes through five stages which are explained as follows.

4.1 Registration phase

The participant visits the website for the first time at this phase to enter the information required to register and subscribe to the public health monitoring service. The following are the three types of registration information (as shown in Figure 3).

(1) The participant's personal information that are used to create a personal webpage, which are full name, age, date of birth, current residential address, current work address, mobile number, personal email, and personal photo.

(2) Information about the nearest healthcare center which are (full name, address, mobile number, e-mail).

(3) Information about the Wearable equipment (the manufacturer's identification number, the version of software used for installation, and the center where it was purchased).

After entering all information, a message will be sent to the participant's personal e-mail with an attached file that will be uploaded to the Wearable device. In addition, the user name and password are sent in the email that are needed to access the participant's webpage created by the cloud server and to download the program used for uploading the attached file on the Wearable device. Furthermore, a message will be sent to the health center's e-mail informing them of the new participant's details.

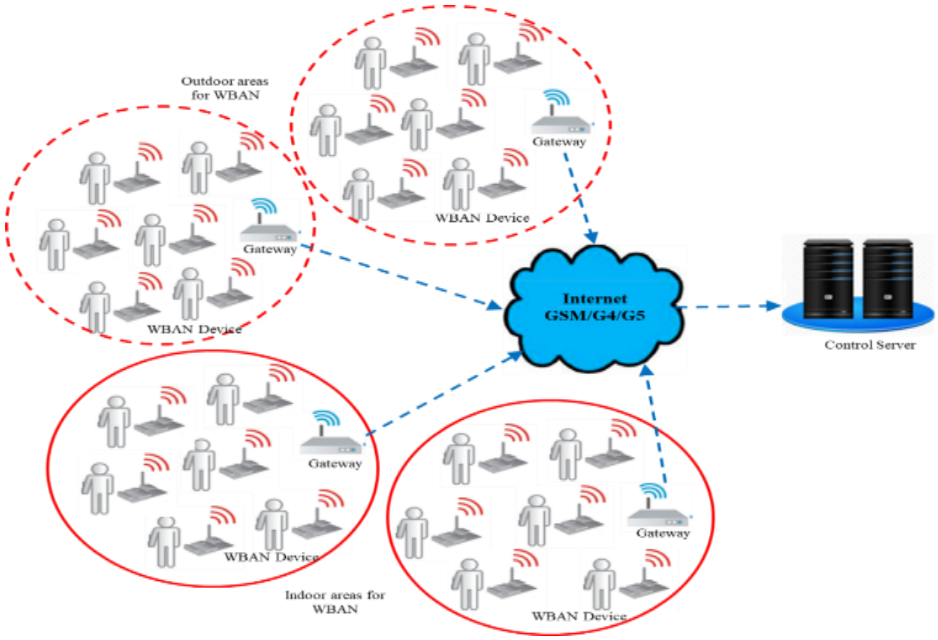

Figure 1. The proposed health monitoring system framework

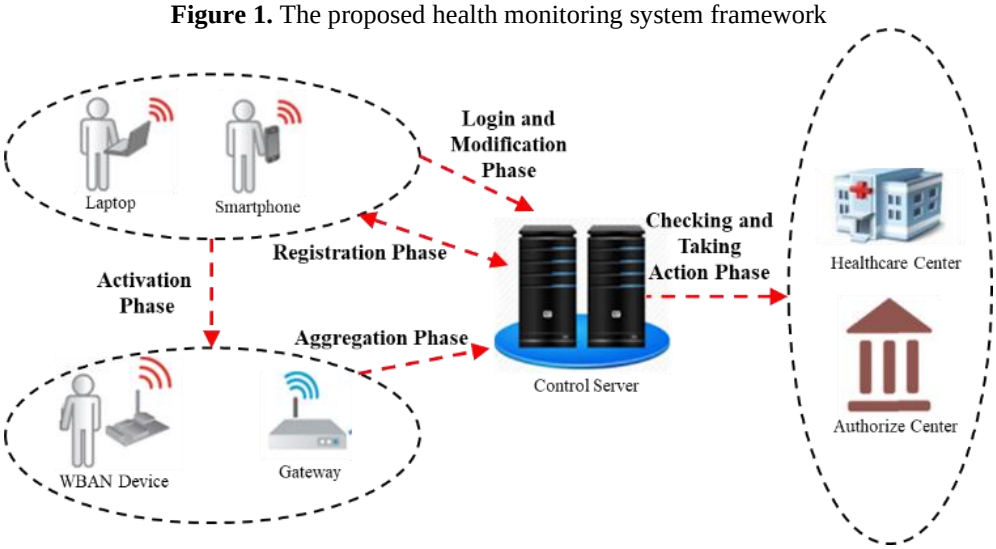

Figure 2. The phases of the proposed public health monitoring system

Registration Information Page

User's Personal Information:
Full Name:
Age: Date of Birth:
Weight: Height:
Current Residential Address:
Current Work Address:
Mobile Number:
Personal Email:
Personal Photo:

Healthcare Center Information
Healthcare Center Name:
Address:
Mobile Number:
E-mail:

Wearable Device Information
Manufacturer's Identification Number:
Software Version:

Figure 3. The registration information webpage

4.2 Activation phase

After the successful completion of the registration process in the previous phase, the Wearable device's file will be sent to the participant's personal e-mail for uploading on the purchased Wearable device. After the uploading process, the Wearable device's wireless adapter will be activated in order to detect the nearest specific gateway within the region and communicate it to begin transferring the participant's vital data. The participant ID is encoded with the vital data supplied in packet to transfer through the wireless network.

4.3 Aggregation phase

After activating the Wearable device by uploading the file given by the cloud server, the device will interact with the closest specific gateway to submit the participant's vital data. The information which have been exchanged between the Wearable device and the specific gateway are (as shown in Figure 4).

Timestamp 13 bytes	User ID 8 bytes	Vital data 7 bytes

Figure 4. The data exchanged between Wearable device and specific gateway

(1) A Timestamp (13 bytes): which is the time for each packet that contained vital information and will be sent to the closest specific gateway.

(2) The user identification (ID) number (8 bytes): which is a unique number added for each Wearable device so that it may be used to store the participant's vital information in the aggregator file.

(3) Vital information (7 bytes): which are the readings of the different sensors that measure the participant's vital data such as body's temperature, heart rate, and so on. The size of the participant's vital is depended on the number of sensors connected to the Wearable device and the size of the data that generated from each sensor.

The closest specific gateway will be gathered the participant's vital data in the table form and delivered them to the cloud server during this phase as a file. Where the specific gateway collects the vital data of the participants associated with it during a specific period and arranges this information in the table form, where each row in the table contains all information of a specific participant. Each row is divided to multiple columns as follows: the first column of the table contains the identification number of the participant associated with that specific gateway, and the second column represents the first packet's information received from the same participant's ID, and the third column represents the second packet's information received from the same participant's ID, and so on. The numbers of columns for each participant depended on the number of vital data received before the gateway is sent the aggregator file to the cloud server (as shown in Figure 5).

User ID	**Vital Data 1**	**Vital Data 2**	----------	**Vital Data 6**
User ID1	Vital Data 1	Vital Data 2		Vital Data 6
User ID2	Vital Data 1	Vital Data 2		Vital Data 6
User IDn	Vital Data 1	Vital Data 2	----------	Vital Data 6

Figure 5. The structure of the received aggregator file by cloud server

4.4 Login and modification phase

After obtaining the user name and special password, the participant may access the participant's webpage, which was built using the information provided during the registration process, to check the statistics of the participant's vital data since utilizing this service, as well as the healthcare professional's opinion on them. Furthermore, during this phase, the participant's or the healthcare center information can be updated or changed in order to be updated on the cloud server and the participant's webpage. However, if the information of the Wearable device utilized are changed, the cloud server will re-send a new file to be uploaded on the Wearable device (by returning to the activation phase again).

4.5 Checking and taking action phase

The system users can access their wearable body sensor data and other resources globally, resulting in reduced diagnosis costs, enhanced services, better analytical reports, and faster care delivery. After the participant's vital data have been saved in his database into the cloud server, the statistical figures will be updated in the participant's webpage, then it will be checked using the artificial intelligent technologies to know if there is any abnormal thing in the participants' vital data. If the abnormal thing is found in the individual participant's vital data, the cloud server will send a message to the healthcare center to do the suitable action. While, if the abnormal is found in the general statistics for the participants' vital data, an alarm will be sent to the authorized center.

5. RESEARCH METHODOLOGY

In this section, the key steps involved in building a secured public health monitoring system based on wearable devices are outlined. Each of these steps plays a crucial role in ensuring the security and effectiveness of the monitoring system. The proposed methodology includes the following steps:

(1) Platform Selection step refers to choose the suitable platform or framework to implement the secured public health monitoring system, where it includes considering some aspects like software and hardware requirements (more description about this step is shown in section 6).

(2) System Immunization step refers to develop and implement a security model of public health monitoring system for protecting against various threats and vulnerabilities. In this step, the techniques like encryption, and digital signature are used to build a robust model (more description about this step is shown in section 7).

(3) Performance Analysis step involves assessing the different routing protocols performance and network configurations which will be used in the proposed health monitoring system. Some performance metrics are measured in order to select the most effective and reliable routing protocol and network configuration for the system (more description about this step is shown in section 8).

In selecting the methodology for constructing the secured public health monitoring system based on wearable devices, the outlined steps were carefully chosen due to their vital roles in fortifying the system's security and operational efficacy. The decision to include these steps stems from their critical contributions to the overall system's robustness and functionality. This methodology has been chosen to ensure a well-rounded approach that prioritizes both security and system performance, consequently establishing a robust and effective public health monitoring system.

6. PLATFORM SELECTION

Examples of body-worn or wireless wearable devices include smartwatches, wristbands, smart glasses, smart jewelry, electronic garments, skin patches, and more [27]. On the contrary, the envisioned gadget is meticulously developed from scratch, boasting a simplistic design. It embraces an open-source approach, is budget-friendly, and aims to consistently acquire, compile, and transmit diverse

physiological data to enhance overall well-being.

The electronic architecture of the wearable health monitoring device revolves around the NodeMCU microcontroller, serving as the primary processing hub. NodeMCU, an ESP8266-based microcontroller board, equipped with built-in Wi-Fi connectivity, is ideal for this purpose, see Figure 6.

The device incorporates two primary sensors: the MAX30100 sensor for monitoring heart rate and SPO2 levels, and the DALLAS DS18B20 sensor for gauging body temperature. These sensors interface with the NodeMCU microcontroller via the I2C and OneWire protocols, respectively.

The MAX30100 sensor utilizes red and infrared LEDs to measure the patient's heart rate and SPO2 levels. It employs a photodetector to capture reflected light, varying in intensity with the heartbeat. SPO2 levels are calculated by assessing the oxygenated hemoglobin in the blood.

The DALLAS DS18B20 temperature sensor gauges body temperature by detecting changes in the resistance of a temperature-sensitive metal wire. It is a one-wire digital temperature sensor known for high accuracy and resolution.

The NodeMCU microcontroller collates data from the sensors and transmits it to the cloud using Wi-Fi connectivity (as depicted in Figure 6). It is powered by the Esp8266 Power Supply Rechargeable Dual Lithium Battery Charger Shield Module (3.7V), to ensure a stable power supply and to offer efficient charging of two lithium batteries. It also includes protection circuits for overcharge and over-discharge and incorporates a power-on/off switch for convenient control.

The electronic design of the wearable health monitoring device is uncomplicated and efficient, facilitating ease of use and maintenance. High-quality sensors and the NodeMCU microcontroller guarantee precise and dependable data collection, while Wi-Fi connectivity and cloud storage enable remote monitoring of participants' health.

Wearable devices necessitate comprehensive testing to guarantee reliability, accuracy, and user-friendliness. This testing involves both single-user and multiple-user assessments. Single-user testing entails individual evaluation to assess functionality, accuracy, and user-friendliness, see Figure 7. Multiple-user testing assesses the device's ability to collect and analyze data from various users, ensuring accurate performance in group settings. Table 1 presents vital data collected from individuals of diverse ages and genders, forming a sub-dataset for general health statistics. Rigorous testing for both single and multiple users ensures that wearable devices are effective, accurate, and reliable for public health monitoring systems.

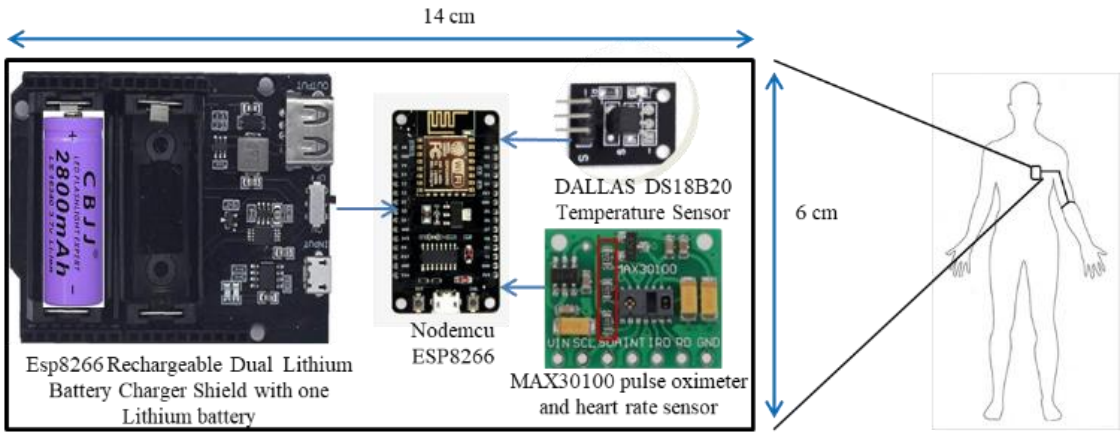

Figure 6. The framework of the proposed wearable health monitoring device

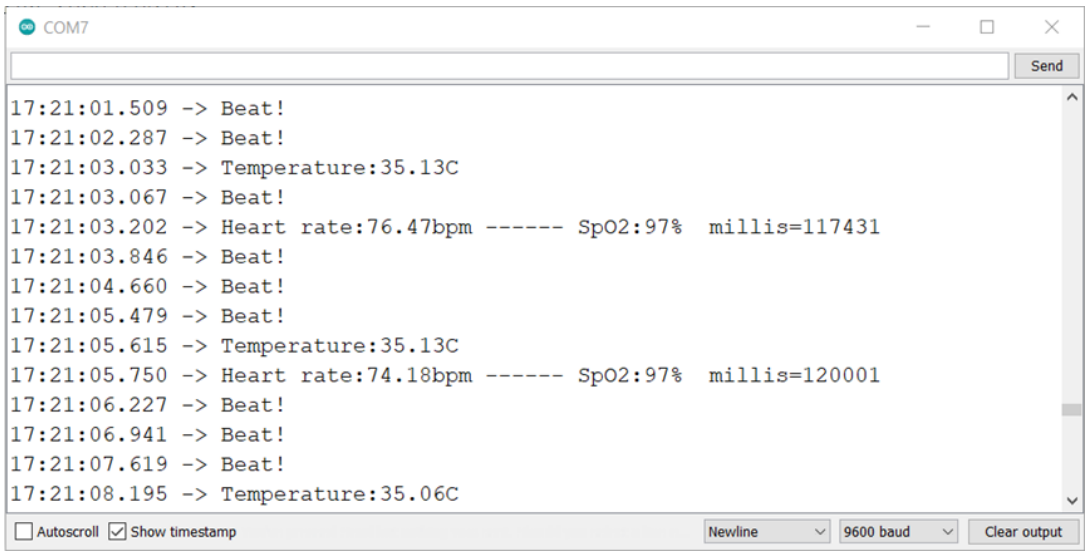

Figure 7. Testing the wearable device for single user

Table 1. Collection of vital data gathered from individuals with varying ages and genders

No	Gender	Age	Weight (kg)	Height (cm)	Spo2%	Heart Rate (beat/min)	Temp ©
1	Male	22	75	173	96	110	36.7
2	Male	21	70	187	96	98	36.1
3	Male	25	72	170	97	87	36.3
4	Male	24	80	178	97	74	36.8
5	Male	57	85	171	96	87	36.3
6	Male	63	82	177	96	85	36.2
7	Female	20	53	157	97	78	36.6
8	Female	14	36	142	98	80	36.4
9	Female	47	82	162	97	93	36
10	Female	53	86	160	97	90	36.5

7. SYSTEM IMMUNIZATION

In this section it will be focused on improving the public health monitoring system security by implementing a security model to protect against the described attacks and vulnerabilities. Then, the security analysis is declared to ensure that the proposed security model is effective. The goal is to fortify the system's defenses and safeguard it against security breaches, ensuring its integrity and confidentiality.

7.1 Possible threats

Wireless Body Area Networks (WBANs) used in public health monitoring systems are susceptible to various security threats. Table 2 shows some of the most common threats with their description and possible defense mechanisms [28, 29].

While no single defense mechanism can guarantee absolute security against all these threats, it is crucial to employ multiple defense mechanisms in combination to create a robust security posture.

7.2 Suggested security model

The public health monitoring system involves human body information; therefore, security and privacy are very important, which must be considered when designing a wearable device. This section went from illustrating the security model for the proposed system. The proposed public health monitoring service uses the connectionless protocol which is UDP (User Datagram Protocol), so the proposed security model must be suited this type of protocol and must be lightweight to be applied on the limited resources devices. To secure the information which will be exchanged between the wearable device and the specific gateway, the following procedures are used as shown in Figure 8:

(1) Include a Timestamp each once when the vital data packet is sent to secure the connection against reply assaults.

Encrypt the vital data with timestamp and participant ID using the symmetric key algorithm like Advanced Encryption Standard 256 (AES256) algorithm which is lightweight than asymmetric key algorithms to be implemented on the limited resources devices. The selection of AES-256 is grounded in its well-established reputation for providing a high level of security. In the context of our proposed health monitoring system, AES-256 serves as a robust defense against various potential attacks. The secret key for the used algorithm is encoded in the file that is uploaded on the Wearable device during the activation phase. So, the participant and the nearest specific gateway don't know the secret key only the cloud server know this key to decrypt the encrypted data.

Where, the key pre-distribution scheme is used in the proposed security model by distributing the secret keys in the Wearable nodes before the communication.

(2) Include a copy of timestamp and participant ID outside the encrypted data because the nearest specific gateway requires these information.

Table 2. Some of the most common threats with their description and possible defense mechanisms

Attack Type	Description	Defense Way
Data interception and eavesdropping	An attacker may intercept and eavesdrop on data transmitted between devices in a WBAN. This can allow them to access sensitive data, such as health records or personal information.	Use encryption.
Denial of Service (DoS) attack	A DoS attack can overload the network with traffic, making it unavailable to legitimate users. This can disrupt the normal functioning of the WBAN and compromise its ability to monitor health data.	Implement rate limiting, traffic shaping, and other traffic management techniques.
Man-in-the-middle (MitM) attack	An attacker can intercept data transmitted between devices in a WBAN and modify it before forwarding it to the intended recipient.	Use end-to-end encryption.
Matching Attack	When the message is small in size as in case of WBAN, attacker generates a pool of keys. He tries to decrypt the message content by applying different key values and find the meaningful values.	Use stronger encryption techniques, key management and distribution mechanisms, and message authentication codes (MACs).
Message corruption	Message corruption is one of active attack based on eavesdropping which capture the information first, modify and reintroduce in transmission again.	Use the encryption and MAC algorithms.
Replay Attack	An attacker with a malicious intent can capture a message, replay it at a later time with or without changing its contents. Such bogus messages are induced into the network to drain the energy of the system. It may also lead to take wrong decisions.	Use a combination of the source node ID and the timestamp. Use sequence numbers in the messages. Also, cryptographic techniques such as digital signatures.

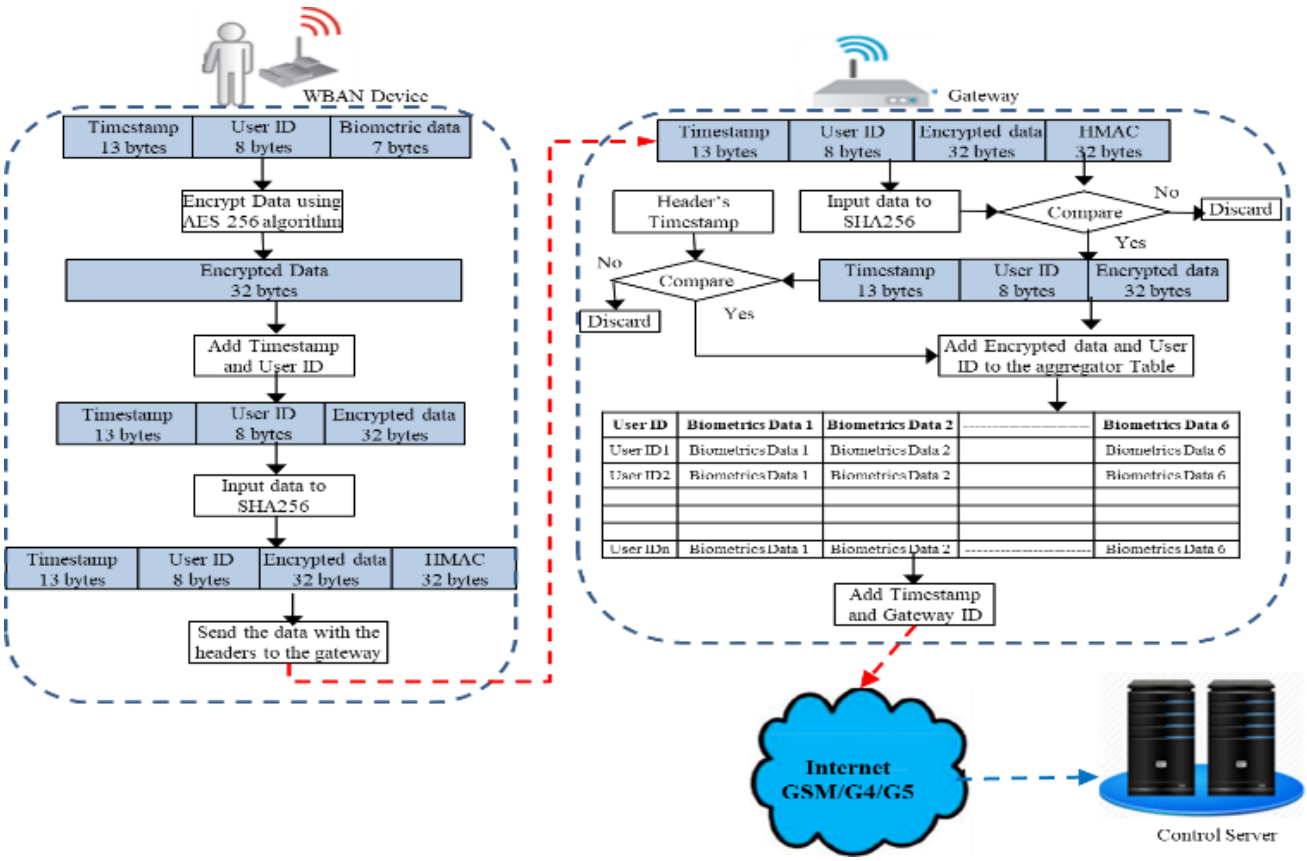

Figure 8. The structure of the data exchanged between wearable device and gateway

(3) Include the Hash-Based Message Authentication Code (HMAC) to guarantee that the information is valid and protected against the modified attacks. This is done by using the keyless hash algorithm like secure hash algorithm 256 (SHA256). This algorithm will be applied on the encrypted data and the copy of timestamp and user ID. Then the generated HMAC will be added to the sent packet to the nearest specific gateway.

(4) For further security, the aggregator file is encrypted, and all information relevant to each participant which are encrypted independently (as shown in step 2). As, GSM / 5G technology (Global System for Mobile communication) is used to transfer the aggregator files between the specific gateways and the cloud server, and this form of data is highly secure.

The proposed security model likes the Pretty Good Privacy (PGP) protocol which is used to secure email communications. But the proposed model is used to secure individual packets of data. PGP employs cryptographic techniques to provide end-to-end encryption and digital signatures for securing data packets in transit. In our scenario, the data packet is encrypted and decrypted using the secret key which is embedded securely in the wearable device and only known by the administrator of the medical server, ensuring that only the intended medical server can decrypt and access the data. Additionally, the sender can digitally sign the data packet to verify the integrity and authenticity of the data. The proposed security model with the encryption and digital signature algorithms make the model a flexible protocol to protect individual data packets in different communication networks.

7.3 Security model implementation

To implement the described security model in the previous subsection on on NodeMCU (ESP8266), the Arduino framework is utilized to provide a suitable environment for programming microcontrollers. The software and programming language requirements are described in the following:

(1) The Arduino IDE (Integrated Development Environment) is the basic software which is utilized to write, compile, and uploading the instruction code s to NodeMCU (ESP8266). Where, it provides a simple and in-built interface for Arduino framework. The Arduino core for ESP8266 is needed to support and program the NodeMCU (ESP8266) boards. A variant of C++ with Arduino-specific extensions is used as the programming language.

(2) Timestamp is generated in the proposed security model using the millis() function provided by the Arduino framework to return the number of milliseconds since the NodeMCU board started running. The function is called as follows:

```
unsigned long currentTimestamp = millis();
```

(3) AES-256 Encryption Algorithm is employed by calling the Crypto library specifically the AES.h module. This algorithm uses the encryption key (a 256-bit key) to encrypt the data. To ensure confidentiality during data transferring, the following sub code encrypts the data in place:

```
#include <Crypto.h>
#include <AES.h>
byte aesKey[] = {...}; // Your 256-bit AES encryption key
AES256 aes;
void encryptData(byte* data, size_t dataSize) {
aes.setKey(aesKey, sizeof(aesKey));
aes.encrypt(data, dataSize); }
```

This function takes the data to be encrypted and encrypts it in place, ensuring confidentiality during data transmission.

Table 3. The security analysis to demonstrate the proposed security scheme's effectiveness against possible attacks

Attack Type	Attack Target	Defense Way Based on Proposed Security Model
Data interception and eavesdropping	The data being transmitted or communicated between two parties.	Use AES 256 algorithm.
Denial of Service (DoS) attack	Disrupt or interrupt the normal functioning of a system or network by overwhelming it with excessive traffic, requests, or other malicious activities.	Implement rate limiting, traffic shaping, and other traffic management techniques.
Man-in-the-middle (MitM) attack	The communication between two parties.	Use AES 256 algorithm.
Matching Attack	The key of cryptographic technique by using a fake key.	Use AES 256 algorithm, key management and distribution mechanisms, and Hash Message Authentication Code algorithm (HMACs).
Message corruption	The integrity of a message or data being transmitted.	Use the AES 256 and HMAC algorithms.
Replay attack	The integrity and authenticity of a message or data being transmitted.	Use a combination of the source node ID and the timestamp. Use AES 256 and HMAC algorithms.

(4) To generate SHA-256 HMAC, the Hash library is utilized, specifically the sha256.h module. To generate a unique signature for the encoded data, the HMAC key is used along with the SHA-256 hashing algorithm. To ensure data integrity, the following sub code uses simply the encrypted data as input, computes the HMAC using the SHA-256 algorithm, and produces a secure signature:

```
#include <Hash.h>
#include <sha256.h>
byte hmacKey[] = {...}; // Your HMAC key
void generateHMAC(byte* data, size_t dataSize, byte* hmacResult) {
 Sha256.initHmac(hmacKey, sizeof(hmacKey));
 Sha256.print(data, dataSize);
 Sha256.getHmac(hmacResult); }
```

This function takes the encrypted data as input, computes the HMAC using the SHA-256 algorithm, and produces a secure signature to ensure data integrity.

In the overall integration, the timestamp, encrypted data, and HMAC are then combined into a secure message for transmission, ensuring a comprehensive security model for the proposed health monitoring system.

7.4 Security analysis

The data collected through WBAN is susceptible to both internal and external attacks. To ensure confidentiality and integrity, one solution is to encrypt or sign the collected data. However, the computational complexity of this process makes it challenging to apply in real IoT-based (Internet of Thing) health monitoring devices. Despite some efforts to develop secure and efficient IoT schemes, there is still a gap in achieving secure data analysis in modern health monitoring. Table 3 presents a non-mathematical security analysis to demonstrate the proposed security scheme's effectiveness against different known attacks with a high level of confidence.

It is important to note that no defense mechanism can provide absolute security, and multiple defense mechanisms should be used in conjunction to provide a strong security posture. Overall, a comprehensive security analysis should be an ongoing process that is integrated into the overall design and implementation of the public health monitoring system. By conducting regular security assessments and implementing appropriate security controls, the system can be protected from potential threats and vulnerabilities, and ensure the privacy and security of vital data.

8. PERFORMANCE ANALYSIS

Recently, there are several wireless technologies which can be adopted for deploying proposed the public health monitoring system such as Wi-Fi, Bluetooth, ZigBee and etc. Application requirements determine the type of wireless technology that could be adopted for better performance. For example, for the proposed system, there are a number of requirements that determine the type of technology used, and the most important of these requirements are: transmission range, cost, power consumed, amount of data, and other requirements. So, compromising between these elements greatly affects choosing the most wireless technology for the application.

For such applications like our proposed system, Mobile Ad Hoc Networks (MANET) are the most widely used wireless networks which can be adopted for building inter-WBAN data collection infrastructure. As explained previously in section 4, the public health monitoring system consists of a group of sensor systems that move within a specific area and send data periodically. This system can best be deployed using Mobile Ad Hoc Networks (MANET) for many reasons. Firstly, ease of deployment as it permits them to be set up rapidly and effectively in crisis circumstances or in zones without existing infrastructure. Secondly, because they self-organize and can quickly adjust to changes in the network's topology or node failures, MANETs can also be very resilient. So, this feature makes them an ideal decision for public health monitoring systems which require reliable and real time data transmission. Finally, from perspective of security, MANETs can be a best choice due to its ability to use advanced encryption and authentication methods to guard against unauthorized access and malicious attacks, making them highly secure.

However, in order to find the settings that are most conducive to achieving optimal network performance and cost effectiveness by a public health monitoring system, it is necessary to go through a series of experiments. Such investigation may require the analysis of different protocols and configuration methods for the network. Routing protocols are one key factor in the performance of inter-WBAN communications. The choice of a suitable routing protocol can affect energy efficiency, latency, reliability, and system throughput.

Consequently, which routing protocol is most suitable for a particular application depends on performance evaluation. So based on our earlier research [30], OLSR was chosen as the system's routing protocol. OLSR is a proactive, table driven routing protocol utilized in MANETs that can give a few

advantages over other routing protocols, including:

(1) Less overhead for the network: OLSR restricts the amount of control traffic in the network by only flooding updates to a slice through nodes in the network. This relieves network congestion and saves bandwidth.

(2) Fast convergence: OLSR is a self-establishing routing protocol, so nodes constantly maintain an overall view of the network topology. It not only includes fast route calculation, it can also help shorten delay and packet loss in the network.

(3) The selection of a multi-point relay (MPR): OLSR utilizes a MPR algorithm for the selection that decides a subset of nodes called MPRs, which are responsible for forwarding traffic on behalf of their neighboring nodes. This reduces the quantity of nodes that need to get and forward traffic, which serves to reduces power utilization and increasing network efficiency.

(4) scalability: OLSR can be supposed to be ideal for large networks because it is designed to minimize control traffic and reduce the amount of processing required at each node. This assists with guaranteeing that the protocol can scale to provide networks with large number of nodes.

(5) Security: OLSR can utilize signature to verify routing messages and not allow malicious nodes from disturbing the network. So it can support secure routing.

Compared to other routing protocols, such as Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), OLSR can provide faster convergence, lower overhead, and improved scalability [30].

The evaluation of the simulated WBAN system is conducted in different scenarios which are created based on different update intervals, and various IEEE 802.11g Wireless Local Area Network (WLAN) standard speeds in order to estimate the maximum number of served nodes (i.e., system capacity). To ensure simulation simplicity and accurate results, some assumptions for implementing the simulated WBAN system are made. These assumptions include mobile and stationary nodes, and assuming a processing speed of 2000 packet/sec for each NodeMCU node. The simulation settings for the simulation test requirements are listed in Table 4, and the simulation model is shown in Figure 9.

Table 4. The simulation settings for the simulation test requirements

Parameters	Settings
Simulation time (h) for each scenario	5
Network Span Area (m)	30*30
WLAN Data Rate (Mbps)	54
Wearable nodes processing speed (packet/sec)	2000
No. of nodes	variable (50% stationary & 50% mobile)
Update interval (Minute)	1
Packet length (byte)	85
Node mobility speed (km/h)	5
OLSR Settings	Message Interval (Hello and TC): 2 seconds TC redundancy: 2 Willingness: 3 Link Quality Level: 2 MID (Message Identifier) value range: 128-255 Multi-interface support: enabled MID validity time: 300 seconds TC Interval Scaling Factor: 2

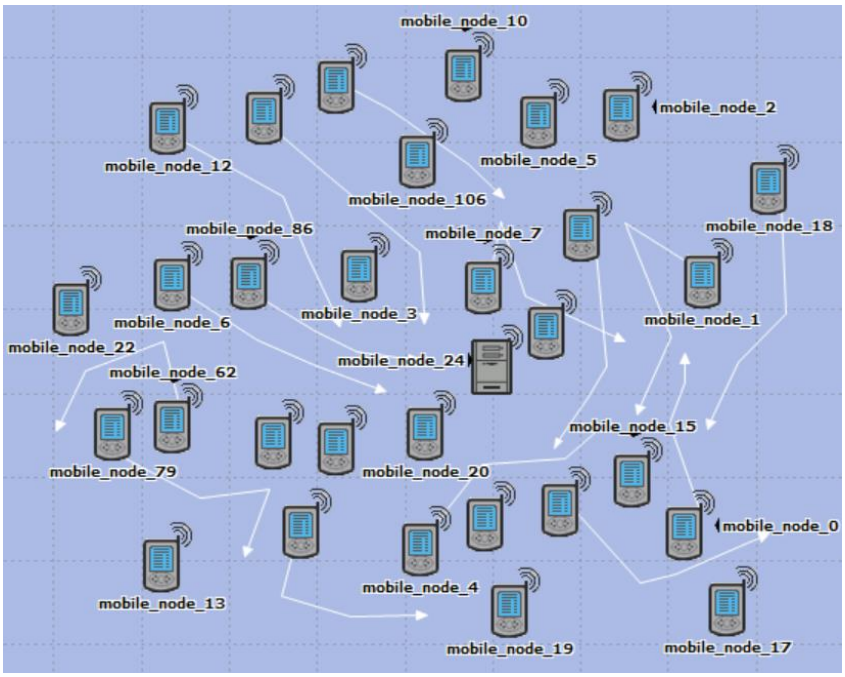

Figure 9. The simulation model

Table 5. The different results after running many simulation scenarios

Parameter	Value
Recommended IEEE802.11g Data Rate	54 Mbps
Maximum number of served nodes without packet loss	218
Average response time (ms) (form the node to the gateway)	7
WLAN traffic/Node (Kbps)	805 (95% of it is the routed traffic received from other nodes)
CPU Utilization of each node (without security activities)	5.5%

The different results after running many simulation scenarios are listed in Table 5. These results reflects the system performance in terms of response time, network load and node resources utilization while working in the most appropriate system settings.

As shown in Table 5, we can analyze the simulation outcomes as follows:

(1) Recommended IEEE802.11g Data Rate (54 Mbps): This data rate is the maximum theoretical throughput for an IEEE 802.11g network. It's important to note that in real-world scenarios, it is rarely achieved the full 54 Mbps due to various factors like interference, signal strength, and network congestion. Nonetheless, it provides a reference point for network capacity.

(2) Maximum number of served nodes without packet loss (218): This metric is crucial for network scalability. The fact that 218 nodes can be served without packet loss suggests that the network's design and capacity planning are robust. However, the number of nodes increases, network performance might degrade due to contention for the limited available bandwidth.

(3) Average response time (ms) (from the node to the gateway) (7 ms): A 7 ms average response time indicates relatively low latency, which is desirable in most networking scenarios. Low latency is particularly important for real-time applications like voice and video calls. However, it's essential to ensure this low latency is maintained even as the network load increases.

(4) WLAN traffic/Node (Kbps) (805 Kbps, with 95% being routed traffic): This data indicates the average traffic load per node. A traffic load of 805 Kbps per node is relatively high, especially if most of it is routed traffic from other nodes. It's essential to monitor network congestion and ensure that QoS (Quality of Service) mechanisms are in place to prioritize critical traffic, especially for real-time applications.

(5) CPU Utilization of each node (without security activities) (5.5%): A CPU utilization of 5.5% without security activities is relatively low. It suggests that the nodes are not overly burdened with processing network traffic. However, it's crucial to consider that security activities, such as encryption and authentication, may significantly increase CPU utilization, so it's important to assess this metric.

To calculate the node lifetime, we need to estimate the average current consumption of the node over time, and then divide the battery capacity by the average current consumption to get an estimate of the node's lifetime [31]. In this paper, the node was assumed to operate on a fixed duty cycle, where it stays active for a fixed amount of time and then goes to sleep for the remaining time. The active time and sleep time are constant and do not change based on the network conditions or traffic patterns. Duty cycling can significantly affect the node's lifetime as it allows the node to save energy by reducing the time it spends in the active mode. Table 6 shows how the estimated node lifetime changes with different duty cycles, based on the parameters (Transmission mode current=140 mA, Sleep mode current=0.5 mA) and using the following relation [32].

As it can be seen, reducing the duty cycle can significantly extend the node's lifetime. However, it also reduces the node's active time and may increase the latency of the transmission. Therefore, it's important to strike a balance between the energy consumption and the desired performance of the system and 10% duty cycling value fits the performance and power consumption of this system.

Table 6. The estimated node lifetime changes with different duty cycles

Duty Cycle	Active Time	Sleep Time	Average Current Consumption	Estimated Node Lifetime
1%	0.6 s	59.4 s	1.45 mA	1929.31 hours (80.39 days)
5%	3 s	57 s	7.15 mA	402.10 hours (16.75 days)
10%	6 s	54 s	13.75 mA	203.64 hours (8.48 days)
20%	12 s	48 s	26.25 mA	101.82 hours (4.24 days)
50%	30 s	30 s	65 mA	40.31 hours (1.68 days)
90%	54 s	6 s	116.75 mA	22.15 hours (0.92 days)

*Average current consumption = (Transmission time*Transmission mode current) + ((1 - Transmission time)*Sleep mode current)*

9. COMPARISON WITH THE PREVIOUS WORKS

Comparisons between previous research on wearable device public health monitoring systems may be difficult due to differences in system design and implementation, differences in experimental setups, lack of standardised metrics for evaluation, and the rapidly changing wearable technology landscape. These factors add complexity that makes it difficult to compare the effectiveness of previous studies, highlighting the significance of careful consideration when interpreting and extrapolating their findings.

In Table 7, the comparative analysis uses a number of critical factors as criteria for comparing and contrasting different health monitoring systems. These criteria were carefully chosen because they are important in determining how well and how suitably various health monitoring systems perform. The Design Level criterion, for example, measures how sophisticated and complex the system's architecture is, which affects its functionality and adaptability. Performance Analysis of Networks examines how efficient the network is, which is critical for smooth data transmission. These factors were selected based on their significance in determining the overall reliability, efficiency, and security of the respective systems. The Adopted Platform factor explores the technology infrastructure that supports the system, impacting its compatibility and scalability. Finally, the Security Features criterion highlights the strength and effectiveness of measures put in place to safeguard sensitive health data.

After analysing the comparisons with pertinent literature in

detail, our analysis highlights how well the suggested system performs in offering a continuous health monitoring solution, especially in the context of public health services. The analysis of routing protocols and network configurations provides insightful information that helps select protocols and configurations that maximise energy efficiency and network performance. The wearable device, which is low-power and lightweight, stands out for its comfortable and extended wear, which improves user experience. At the same time, the effective security model guarantees the safe transmission and storage of health data. Each of these constituents makes a distinct contribution to the all-encompassing synopsis provided in Table 8, which enumerates the system's salient features and, taken as a whole, underscores its competence in furnishing a comprehensive solution for public health monitoring. The results indicate not only increased efficacy in health data monitoring and transmission but also offer a structure that encourages broad implementation, guaranteeing improved health outcomes for individuals in heterogeneous communities. By giving precedence to energy efficiency, network performance, and data security, our system sets a standard for future advancements, clearing the path for more easily accessible, dependable, and secure public health monitoring systems.

Table 7. Comparison with the related works

Ref. No.	Design Level	Performance Analysis of Networks	Adopted Platform	Security Features
[21]	System level & device level	N/A	N/A	N/A
[22]	System level & device level	N/A	Arduino Mega & Nano with smartphone	N/A
[23]	System Level	N/A	N/A	A novel cryptographic accumulator based on novel authenticated additive homomorphic encryption
[24]	System Level	N/A	N/A	A privacy-preserving authentication protocol
[25]	System Level	N/A	N/A	A secure channel free certificateless signcryption scheme
[26]	N/A	Throughput, Packet Delivery Ratio, and Minimum delay	N/A	A trust model for secure communication in WBAN based on node trust and data trust
Our work	System level & device level	Throughput, Packet end to end delay, and power consumption	Node MCU	AES256-SHA256- confidentiality, integrity and authentication– key generation and distribution (based on PGP protocol)

Table 8. Main features and performance of the proposed public health monitoring system

Setting	Parameter	
Network Type	Wireless Mesh Network	
Ad hoc routing protocol	OLSR	
Mobility of the Wearable nodes	Mobile nodes	
Hardware implementation of the Wearable device	ESP8266, 32bit microcontroller, 80MHz CPU speed, 32KiB memory size	
Wi-Fi standard	IEEE802.11g, 54 Mbps	
Wearable device size	14*6 cm	
Wearable device radial transmit range	Less than 20 meters (indoor) Less than 100 meters (outdoors)	
Wearable device weight	80 grams	
Estimated cost/ Wearable device	5–10$	
Average Wearable device lifetime	203 hours	
Network performance	Network load/node (Kbps)	805
	Average response time (ms)	7
Supported security methods	AES256-SHA256- confidentiality, integrity and authentication– key generation and distribution (based on PGP protocol)	
Possible threats detected	Data interception and eavesdropping, DoS attack, Man-in-the-middle attack, Matching attack, Message Corruption attack, and Replay attack	
CPU Utilization of each node (including security activities)	30%	

10. CONCLUSIONS

In conclusion, this manuscript showcases significant advancements in public health monitoring systems, leveraging data analytics and technology. The widespread adoption of electronic health records and digital tools by public health agencies has revolutionized data collection, analysis, and real-time sharing, substantially enhancing disease surveillance and response accuracy. Our research specifically focuses on the development of a continuous health monitoring system, emphasizing secure data storage on a medical server to detect anomalies. Key contributions include proposing a public health service, optimizing network performance and cost-effectiveness through the analysis of network protocols and configurations, creating a lightweight, energy-efficient wearable device, and suggesting an efficient security model for resource-constrained wearables. The system's efficacy and security features position it as a promising solution for public health monitoring using wearable devices. Looking ahead, future integrations could involve additional health sensors,

such as ECG sensors, consolidating multiple health parameters into a single device, optimizing time efficiency, and broadening health issue identification within communities. Furthermore, the establishment of a robust public health monitoring system holds critical importance in safeguarding communities' health and enabling swift responses to outbreaks and other health threats. These implications highlight the potential for wider societal benefits and substantial advancements in scientific methodologies and healthcare practices.

REFERENCES

[1] Sama, N.U., Zen, K., Humayun, M., Jhanjhi, N.Z., Rahman, A.U. (2022). Security in wireless body sensor network: A multivocal literature study. Applied System Innovation, 5(4): 79. https://doi.org/10.3390/asi5040079

[2] Zhong, L., He, S., Lin, J., Wu, J., Li, X., Pang, Y., Li, Z. (2022). Technological requirements and challenges in wireless body area networks for health monitoring: A comprehensive survey. Sensors, 22(9): 3539. https://doi.org/10.3390/s22093539

[3] Punj, R., Kumar, R. (2019). Technological aspects of WBANs for health monitoring: A comprehensive review. Wireless Networks, 25(3): 1125-1157. https://doi.org/10.1007/s11276-018-1694-3

[4] Bhatti, D.S., Saleem, S., Imran, A., Iqbal, Z., Alzahrani, A., Kim, H., Kim, K.I. (2022). A survey on wireless wearable body area networks: A perspective of technology and economy. Sensors, 22(20): 7722. https://doi.org/10.3390/s22207722

[5] Arefin, M.T., Ali, M.H., Haque, A.F. (2017). Wireless body area network: An overview and various applications. Journal of Computer and Communications, 5(7): 53-64. https://doi.org/10.4236/jcc.2017.57006

[6] Salayma, M., Al-Dubai, A., Romdhani, I., Nasser, Y. (2017). Wireless body area network (WBAN) a survey on reliability, fault tolerance, and technologies coexistence. ACM Computing Surveys (CSUR), 50(1): 1-38. https://doi.org/10.1145/3041956

[7] Qu, Y., Zheng, G., Ma, H., Wang, X., Ji, B., Wu, H. (2019). A survey of routing protocols in WBAN for healthcare applications. Sensors, 19(7): 1638. https://doi.org/10.3390/s19071638

[8] Jin, Y. (2019). Low-cost and active control of radiation of wearable medical health device for wireless body area network. Journal of Medical Systems, 43: 1-11. https://doi.org/10.1007/s10916-019-1254-0

[9] Poongodi, T., Rathee, A., Indrakumari, R., Suresh, P. (2020). IoT sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition. In: Peng, SL., Pal, S., Huang, L. (eds) Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Intelligent Systems Reference Library, vol 174. Springer, Cham. https://doi.org/10.1007/978-3-030-33596-0_5

[10] Ananthi, J.V., Jose, P. (2021). A perspective review of security challenges in body area networks for healthcare applications. International Journal of Wireless Information Networks, 28(4): 451-466. https://doi.org/10.1007/s10776-021-00538-3

[11] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal, 18(2): 113-122. https://doi.org/10.1016/j.eij.2016.11.001

[12] Wang, W.H., Hsu, W.S. (2023). Integrating artificial intelligence and wearable IoT system in long-term care environments. Sensors, 23(13): 5913. https://doi.org/10.3390/s23135913

[13] Haider, Z., Jamal, T., Asam, M., Butt, S., Ajaz, A. (2020). Mitigation of wireless body area networks challenges using cooperation. International Journal of Security and Its Applications, 14(1): 15-30. http://dx.doi.org/10.33832/ijsia.2020.14.1.02

[14] Hussain, S., Ullah, S.S., Uddin, M., Iqbal, J., Chen, C.L. (2022). A comprehensive survey on signcryption security mechanisms in wireless body area networks. Sensors, 22(3): 1072. https://doi.org/10.3390/s22031072

[15] Elayan, H., Shubair, R.M., Kiourti, A. (2017). Wireless sensors for medical applications: Current status and future challenges. 2017 11th European Conference on Antennas and Propagation (EUCAP), Paris, France, pp. 2478-2482. https://doi.org/10.23919/EuCAP.2017.7928405

[16] Yaghoubi, M., Ahmed, K., Miao, Y. (2022). Wireless Body Area Network (WBAN): A survey on architecture, technologies, energy consumption, and security challenges. Journal of Sensor and Actuator Networks, 11(4): 67. https://doi.org/10.3390/jsan11040067

[17] Khan, S.R., Mugisha, A.J., Tsiamis, A., Mitra, S. (2022). Commercial Off-the-Shelf Components (COTS) in realizing miniature implantable wireless medical devices: A review. Sensors, 22(10): 3635. https://doi.org/10.3390/s22103635

[18] Alrashidi, M., Nasri, N. (2021). Wireless body area sensor networks for wearable health monitoring: Technology trends and future research opportunities. International Journal of Advanced Computer Science and Applications, 12(4): 506-512. https://doi.org/10.14569/IJACSA.2021.0120464

[19] Singh, A.K., Anand, A., Lv, Z., Ko, H., Mohan, A. (2021). A survey on healthcare data: A security perspective. ACM Transactions on Multimidia Computing Communications and Applications, 17(2s): 1-26. https://doi.org/10.1145/3422816

[20] Liu, Q., Mkongwa, K.G., Zhang, C. (2021). Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. SN Applied Sciences, 3(2): 1-19. https://doi.org/10.1007/s42452-020-04058-2

[21] Hassan, M.K., El Desouky, A.I., Elghamrawy, S.M., Sarhan, A.M. (2018). Intelligent hybrid remote patient-monitoring model with cloud-based framework for knowledge discovery. Computers & Electrical Engineering, 70: 1034-1048. https://doi.org/10.1016/j.compeleceng.2018.02.032

[22] Al-Naggar, N.Q., Al-Hammadi, H.M., Al-Fusail, A.M., Al-Shaebi, Z.A. (2019). Design of a remote real-time monitoring system for multiple physiological parameters based on smartphone. Journal of Healthcare Engineering, 2019: 5674673. https://doi.org/10.1155/2019/5674673

[23] Rezaeibagha, F., Mu, Y., Huang, K., Chen, L. (2020). Secure and efficient data aggregation for IoT monitoring systems. IEEE Internet of Things Journal, 8(10): 8056-8063. https://doi.org/10.1109/JIOT.2020.3042204

[24] Ryu, H., Kim, H. (2021). Privacy-preserving

authentication protocol for wireless body area networks in healthcare applications. Healthcare, 9(9): 1114. https://doi.org/10.3390/healthcare9091114

[25] Noor, F., Kordy, T.A., Alkhodre, A.B., Benrhouma, O., Nadeem, A., Alzahrani, A. (2021). Securing wireless body area network with efficient secure channel free and anonymous certificateless signcryption. Wireless Communications and Mobile Computing, 2021: 5986469. https://doi.org/10.1155/2021/5986469

[26] Ramaswamy, S., Gandhi, U.D. (2022). Trust-based data communication in wireless body area network for healthcare applications. Big Data and Cognitive Computing, 6(4): 148. https://doi.org/10.3390/bdcc6040148

[27] Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., Hassan, M., Seneviratne, A. (2017). A survey of wearable devices and challenges. IEEE Communications Surveys & Tutorials, 19(4): 2573-2620. https://doi.org/10.1109/COMST.2017.2731979

[28] Hussain, S., Kumar, M. (2021). Secured key agreement schemes in wireless body area network-A review. Indian Journal of Science and Technology, 14(24): 2005-2033.

[29] Ali, A., Khan, F.A. (2015). Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art. Journal of Medical Systems, 39: 1-14. https://doi.org/10.1007/s10916-015-0272-9

[30] Ali, Q.I. (2016). Green communication infrastructure for vehicular ad hoc network (VANET). Journal of Electrical Engineering, 16(2): 10-10.

[31] Ibrahim, Q. (2016). Enhanced power management scheme for embedded road side units. IET Computers & Digital Techniques, 10(4): 174-185. https://doi.org/10.1049/iet-cdt.2015.0135

[32] Ali, Q.I. (2016). Event driven duty cycling: An efficient power management scheme for a solar-energy harvested road side unit. IET Electrical Systems in Transportation, 6(3): 222-235. https://doi.org/10.1049/iet-est.2015.0036