INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

IoT-based Secure and Energy Efficient scheme for E-health applications

Mamoona Humayun[1]*, NZ Jhanjhi[2], Malak Z Alamri[1]

1 Department of Information systems, College of Computer and Information Sciences Jouf University, KSA
2 School of Computer Science and Engineering (SCE),, Taylor's University, Malaysia

OPEN ACCESS

Received: 08-06-2020

Accepted: 19-07-2020

Published: 07-08-2020

Editor: Dr. Natarajan Gajendran

Citation: Humayun M, Jhanjhi NZ, Alamri MZ (2020) IoT-based Secure and Energy Efficient scheme for E-health applications. Indian Journal of Science and Technology 13(28): 2833-2848. https://doi.org/10.17485/IJST/v13i28.861

***Corresponding author**.

mahumayun@ju.edu.sa

Funding: Deanship of Scientific Research, Jouf University, under the grant number, 40/222

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Background/objectives: This study presents a secure and energy-efficient scheme of patient's data transmission from wearable IoT sensors (WIS) to base station (BS). IoT sensors are widely used in the healthcare domain for real-time data collection and transmission. However, these sensors are resource-constrained in terms of computational power and storage due to which chances of security breaches and threats increase. Moreover, with time the energy level of IoT sensors also degrade that sometimes leads towards loss of sensitive patient data. **Purpose:** The purpose of this study is to provide secure data transmission between wearable sensors and base stations and increasing energy efficiency of resource-constrained wearable IoT sensors. **Method:** The proposed scheme was tested by creating a mathematical model and then creating a simulation setup using the Cooja Contiki simulator. **Findings:** The results show that the proposed scheme provides secure and energy-efficient data transmission from WISs to BS as compared to the existing approaches. Further, the proposed scheme addresses some key issues including availability, reliability, scalability, and limited patient mobility. **Novelty:** Our research presented a unique approach for e-health applications using the IoT, where we considered the lightweight and secure scheme providing multiple group node concept.

Keywords: Internet of Things (IoT); wearable IoT sensors (WIS); healthcare; Group node (GN); base station (BS); simulation

1 Introduction

Healthcare is one of the most significant fields for both individuals and governments. The increasing number of aged people, newly occurring diseases, and the cost of medical expenditure have made it one of the significant fields that need to be paid attention to. In the last few years, the advancement of IoT technologies and its use in the healthcare field has helped a lot in solving various healthcare problems by providing real-time patient monitoring, remote monitoring, and early and quick diagnosis of the problem (1,2). One of the significant advances that IoT has brought in the field of healthcare is the use of wearable sensors for monitoring real time health conditions of patients (3–5). These wearable sensors are attached to the human body for collecting vital information of patients such as blood pressure (BP), heart rate, temperature, etc. In case of any significant variation in captured data, it is sent to the BS that is responsible for sending it to the caregiver [6–8]. In this way, the patient data is collected in real-time, and quick first aid is provided in case of any emergency. Figure 1 shows the block diagram of wearable sensor usage in healthcare for patient monitoring. According to Figure 1, patient data is collected through the ultraviolet sensors attached to the human body, this collected data is sent to the BS that can be any smart devices capable of receiving data. BS send the collected data to the hospital server via healthcare cloud where a healthcare provider can access this data to take timely decision.

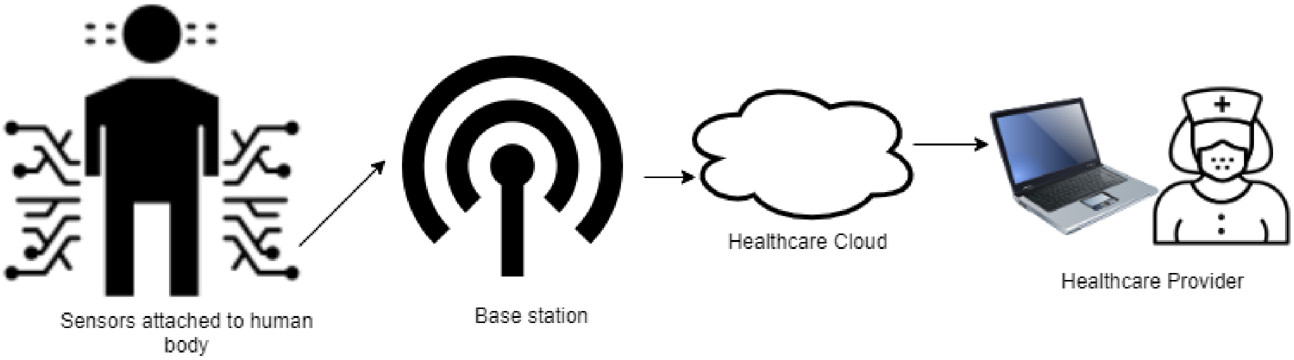


Fig 1. Real-time patient health monitoring through wearable sensors

IoT advancement has made a good revolution in the field of healthcare and modern healthcare systems also known as e-healthcare has brought a lot of ease for patients and healthcare providers [9,10]. However, one of the significant issues that still need to be addressed is the security of the patient's data. The data of the patient is sensitive and confidential and its unauthorized access sometimes leads towards disaster. Although end-to-end security of data is important, however; major security breaches occur when data is transmitted from wearable sensors to BS. The key reason behind these security breaches is resource-constrained IoT sensors. Wearable sensors have low computational and storage capacity due to which there are more chances of data loss and security breaches [11–13]. Hence, secure and efficient data transmission from wearable sensors to BS is a challenge that needs to be addressed.

To fill this gap, we have provided multiple group nodes (GN) concept that will serve as an interface between wearable sensors and BS. The GN in our case is having sufficient resources, it collects data from nearby sensors and transmits it to the BS. GN is also responsible for key authentication with BS. WISs do not need to communicate with BS rather they will directly communicate with GN and will use the same authentication key of GN. When an individual node communicates with BS directly, first it needs to establish a connection and then send data to the BS that is far from it. In the case of GN, individual nodes do not need to do key authentication, and distance among WIS and GN will also reduce. As distance is inversely proportional to energy, so decreasing the distance will increase energy efficiency. Further, a reduction in distance will also cause a reduction in security breaches. The reasons for introducing two GNs are: removing the distance between WISs and GN and sharing the burden of other GN in case of any failure. Further, the idea of single GN has already been proposed and evaluated in [14].

This paper is the extension of our previous work presented in [15]. We have already proposed a multi-group node concept in our review paper in which we have provided a multiple GNs based framework and also evaluated it using the Delphi technique. In this paper, we have set up an experimental environment through simulation by using the Cooja-Contiki simulator. In our experiment, we have tried to study and analyze the impact of multiple GNs on security and energy efficiency. The results are also compared with the previous scheme proposed by [14]. The structure of the paper is shown in Figure 2 .

2 Literature review

IoT has been widely used in the healthcare industry and a lot of research efforts are going on to address the issues and challenges associated with it. In this section, we will discuss some existing studies that have provided solutions for the transmission of patient's data from wearable sensors to BSs with a special focus on security and energy issues.

According to [14], the data of healthcare is sensitive therefore it needs more security to protect it from various cyber-attacks. Mainly security breaches occur when data is transmitted from resource-constrained WISs to BS. This research proposed a GN-based efficient and secure mechanism of healthcare data transmission between WISs and BS. The GN introduced in this paper serves as an interface between WISs and BS. GN is responsible for the key authentication process with BS and the same key

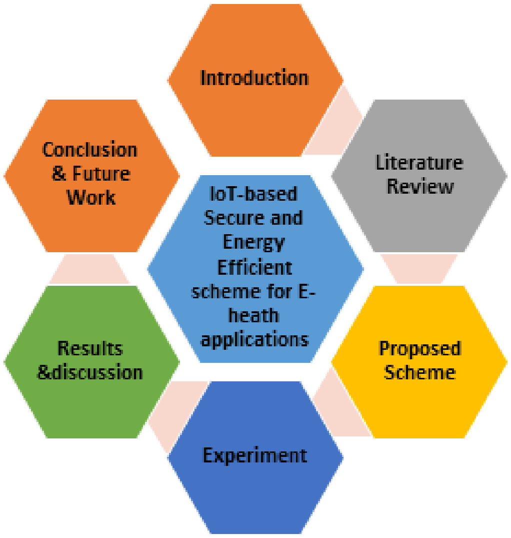


Fig 2. Paper structure

is used by all WISs. In this approach individual WIS does not need to communicate with BS rather they send the patient data to GN which is responsible for transmitting it to BS. The proposed scheme was tested through simulation that was performed using the Cooja-Contiki simulator. The results show that the proposed scheme provides more security and energy efficiency and is resistant against hacks due to the use of elliptic curve cryptography (ECC).

In paper [16], a lightweight authentication scheme for healthcare applications is provided. In this scheme, IoT sensors and BS authenticate each other for securing healthcare data. Nonces and Keyed-hash authentication technique is used to ensure the authenticity of exchanged data. To check the validity of the proposed scheme, a performance and security analysis was performed. However, the real-time testing of the proposed security protocol needs to be done. The analysis results show that the proposed scheme is energy efficient and resistant to various security threats.

In paper [17], the security requirements for body sensor networks (BSN) in current e-healthcare systems are addressed. Based on the discussed security requirements a secure IoT based healthcare system named BSN-care is proposed to address the identified requirements. The proposed architecture is composed of WISs and implantable sensors. These sensors collect a patient's health data and transmit it to the coordinator node called a local processing unit (LPU). This LPU can be any portable device such as a smartphone, PDA, tablet, etc. This LPU serves as a router between BSN node and server using a wireless communication channel. In case of any abnormality in the collected data, the patient is immediately notified. The analysis of the proposed scheme shows that it accomplish various security requirements.

Paper [18] provides the layered architecture of IoT, it describes possible cyber-attacks targeting each layer of IoT and the corresponding security requirements with a special focus on healthcare domain. Various development strategies are discussed to defend IoT from possible cyber-attacks. Thus the contribution of the paper is twofold: it discusses various types of attacks along with a defense mechanism. According to this paper, proper coordination between healthcare organizations and government is necessary for resolving security issues.

A comprehensive survey is provided in [19], it includes a review of the latest IoT-based healthcare technologies and existing network platforms and solutions. It also provides the details of existing security and privacy features of IoT-based healthcare system. Based on the detailed review of the current state-of-the-art, the paper provides a collaborative model for minimizing security risks and also discusses the role of recent technologies such as ambient intelligence, big data, and wearable in the healthcare domain. This paper also provides an overview of various IoT and e-healthcare regulations and policies across the world and provide some future research venues for IoT-based healthcare research.

In paper [20], existing IoT security and privacy risk factors in the healthcare sector are identified to provide a secure IoT-based healthcare environment that conforms to existing quality indicators. The paper provides a comparative analysis of related work along with a case study of a Malaysian government hospital. Based on the findings, a model is proposed that is claimed to serve as a basic principle for securing IoT-based healthcare systems from existing security risks.

Paper [21] analyze the performance of existing end-to-end security schemes in IoT-based healthcare systems. Based on findings, it provides a three-layer architecture for end-to-end secure communication for IoT-based healthcare. The proposed scheme was tested on two different scenarios: patient in-home and patient in the hospital room. A prototype was built for testing the proposed solution, the results were compared with existing approaches. The results show that the proposed scheme is more efficient in terms of energy efficiency and the cryptographic key generation. Further, it reduces communication overhead and communication latency.

Paper [22], have explored privacy protected collection and access of data in IoT-based healthcare applications and provided a framework named PrivacyProtector to maintain the privacy of patients' data. Further, it provides a secret sharing scheme for optimization of secret share size and supports the repair of exact-share in case if data is corrupted or altered. In the proposed scheme, data acquired from IoT sensors is stored on multiple cloud servers from where it is accessed by healthcare providers. If any data server gets compromised due to any reason, the privacy of the patient's data is still protected.

Paper [23] have presented an efficient and secure authentication architecture for IoT-based healthcare systems using smart gateways called SEA. It reduces the burden of resource-constrained IoT sensors by outsourcing some tasks, in this way the performance of sensor nodes improves. Due to smart gateways, IoT sensor nodes do not need to authenticate a remote healthcare provider. The inclusion of smart gateways reduces the burden of sensor nodes and improves security and efficiency. Further, the smart gateway provides some additional functionalities such as storing users' and sensors' information, local processing of sensors data, and by providing various data aggregation and interpretation techniques.

Paper [24] provides a lightweight authentication scheme to guarantee secure communication and protection of patients' data. An experimental setup was carried out for the processing of sensors signals by using a fuzzy inference system. Further, an improved intelligent model for patient monitoring was presented that automatically gathers and analyzes vital health parameters from the patient's body. The doctors can monitor the patients' health in real-time and can provide rescue in case of emergency. The proposed mechanism provides better authentication by reducing access time overhead and key generation time.

Paper [25] presents a security model for healthcare systems that provides secure data transmission in the IoT environment. The proposed model includes four processes: patient data is encrypted using a hybrid encryption scheme proposed in the model. Next, encrypted data is concealed in a cover image to produce stego image. Then embedded data is extracted and is decrypted for retrieval of the original image. The proposed model was implemented using simulation in MATLAB setup and results were satisfactory.

The above discussion is summarized in Table 1. It highlights that patients' data is sensitive and it needs to be protected against various security breaches. However, the key challenge faced in data transmission from wearable sensors to the BS is that IoT sensors attached to the patient's body are resource-constrained and their energy and computational power decrease with time. To overcome this problem, some burden on WISs need to be removed. This can be achieved by reducing the distance between WISs and BS and introducing a non-resource-constrained medium between WISs and BS. Before proceeding towards the solution of this problem, we provide a taxonomy of IoT-based healthcare system for a better understanding of the problem.

Table 1. Comparison of existing studies

Ref	Targeted Health App	Research method	Contribution	Pros	Cons	Evaluation parameters	Research Gaps
[14]	Wearable IoT sensors	Simulation	Provides a secure and energy-efficient scheme of healthcare data transmission between WISs and BS.	Provide a secure healthcare data transmission mechanism by reducing communication distance, improving security, and energy.	The GN is overburden and any problem or security breach at GN will lead to severe consequences.	Security Mobility Energy Communication distance	Overall data transmission is dependent on the group node. The failure of the Group Will affect overall network
[16]	Wearable and implantable sensors	Controlled experiment	Provided an energy-efficient and secure data exchange mechanism between IoT sensors and BS	Avoid replay attack & Impersonation Reduce communication and computational cost Session key establishment scalability	Validation is missing	Energy Security	Do not address some key issues like mobility, reliability, and availability

Continued on next page

Table 1 continued

[17]	Body sensor network	Performance analysis	Provide an architecture for secure data transmission for body sensor networks by addressing various security requirements. It alerts the patient in case of any abnormality in the data received from sensors.	Address key security requirements including data privacy, data integrity, data freshness, authentication, Anonymity, and secure localization	Validation is missing	Computational overhead Privacy security	The paper only focus on security While various key parameters such as patient's mobility reliability, availability, scalability, communication overhead, and energy efficiency have not been addressed
[18]	Smart cities for healthcare applications	Review Paper	Discussed security attacks targeting different layers of IoT in the healthcare domain and also described the possible mitigation techniques.	Identified security requirements of all IoT layers to mitigate possible cyber attacks	Existing work is synthesized without any novel contribution	Security	General review provided, no novel contribution
[19]	IoT healthcare applications & services	Survey	Propose a collaborative security model for minimizing security risks in IoT-based healthcare systems.	Provide a review of the latest IoT-based healthcare technologies and existing network platforms and solutions Provide the details of existing security and privacy features of IoT-based healthcare system. Provides an overview of various IoT and e-healthcare regulations and policies	Existing work is synthesized without any novel contribution	Security Privacy	Just explored existing work without any novel contribution
[20]	Secure IoT-based healthcare environment	Review	Propose a model for secure IoT-based healthcare environment	Privacy and security risk factors identification Comparative analysis	Validation is missing	Security Privacy	Evaluation of the proposed model is missing
[21]	Healthcare IoT systems	Experiment	Provided end-to-end security scheme for IoT-Based healthcare system	Identified essential security requirements Performance analysis of existing end-to-end security solutions Prototype development	The cost-benefit analysis is missing	Latency Energy Security Key generation Computational overhead Performance	The main focus of the paper is security. However, some other key factors such as efficiency, throughput, and latency are not considered.

Continued on next page

Table 1 continued

(22)	IoT-based Healthcare system	Review	Provided a framework to preserve the privacy of patients' data	Support share repair Patients' data remain secure in case any security breach occurs on one or two cloud servers	The proposed scheme needs to be tested on real-time IoT-based healthcare application	Privacy Communication	Privacy is not being considered at the data acquisition stage and communication service provider stage
(23)	IoT-based Healthcare system	Prototype	Provided secure and efficient architecture for IoT-based healthcare systems using smart gateways	Improve sensors performance Secure key management Reduce communication overhead Provide reliable and scalable end-to-end security	The proposed scheme needs to be tested on real-time IoT-based healthcare application	Efficiency Security Communication latency Scalability Reliability	Some important issue like mobility, availability, and reliability are not been discussed
(24)	Healthcare monitoring system	Experiment	Proposed a model that integrates artificial intelligence to make the healthcare system smart and efficient	Real-time patient monitoring Protect patients information Reduce access time overhead Reduce key generation time	Real-time hardware implementation is missing	Reliability Accuracy Security	Patient mobility is not discussed and considered as all

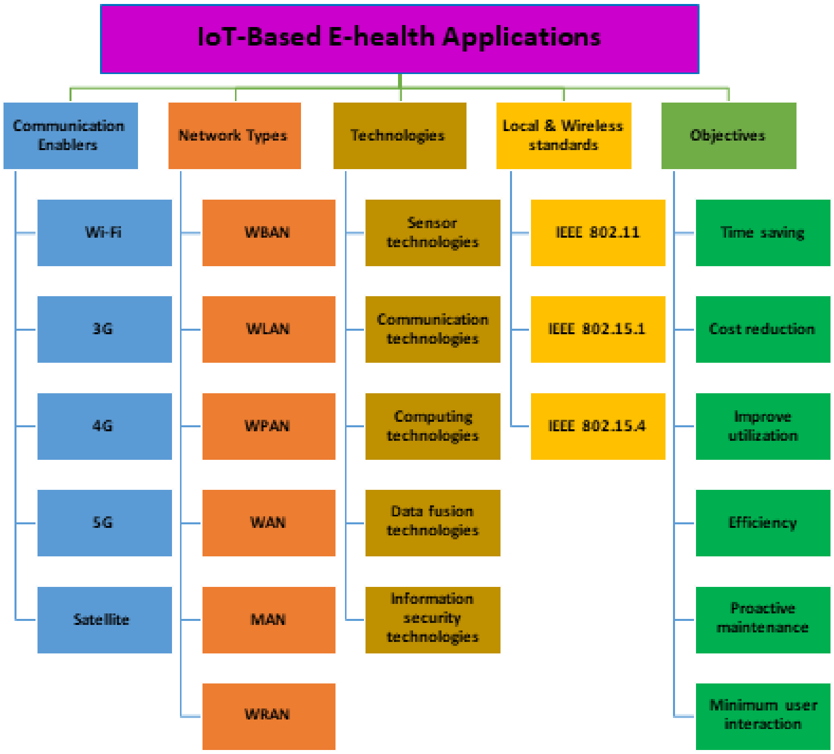


Fig 3. IoT-Based e-healthcare applications taxonomy

3 Proposed scheme

The wearable sensor is widely used technology and plays a key role in e-healthcare systems by providing real-time monitoring of patients. However, a key challenge associated with wearable IoT-sensors is their resource-constrained nature. This resource-constrained nature of IoT sensors makes them an ideal target of security attacks. Patient's data is very sensitive and unauthorized access to this data sometimes leads to disastrous consequences. Various solutions have been provided for the secure transmission of sensors data to the BS but still, the resource-constrained nature of IoT sensors becomes an obstacle. Below, we provide our framework that helps in the secure and efficient transmission of data from WISs to BS.

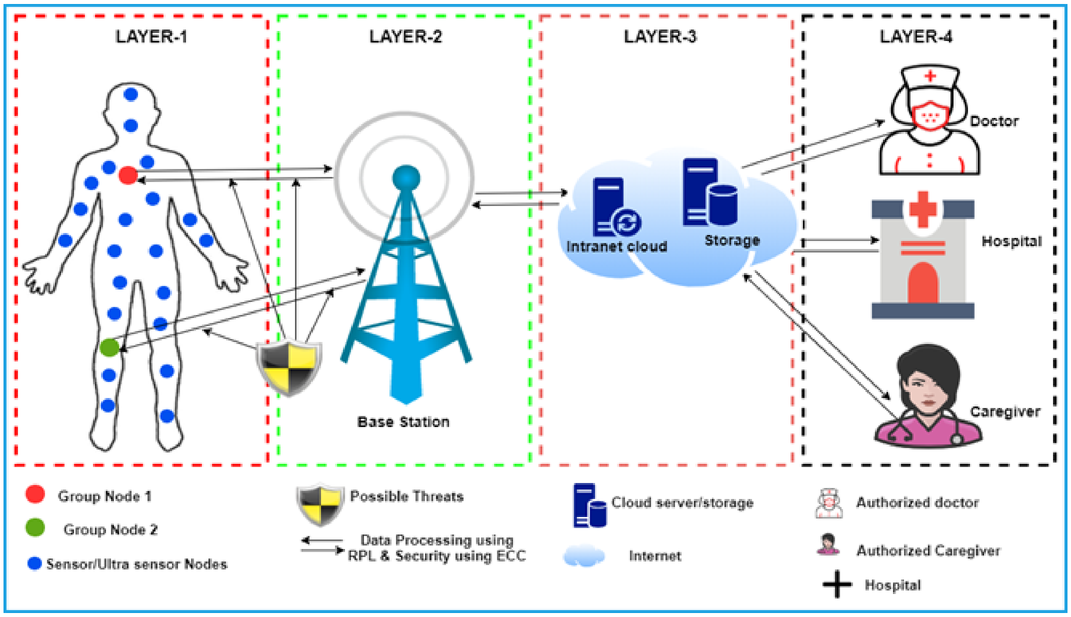


Fig 4. Proposed Framework

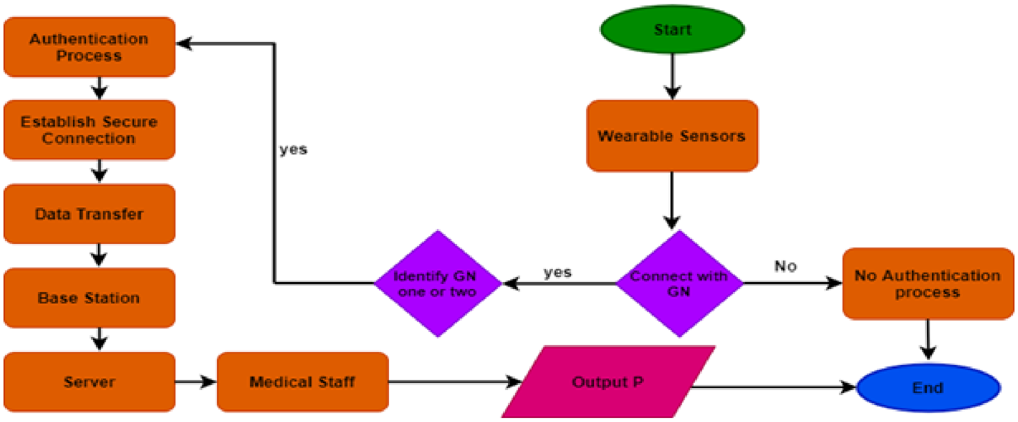


Fig 5. Proposed scheme flow diagram

The proposed framework consists of four layers. Layer 1 is the physical layer that involves patients with wearable IoT sensors for real-time monitoring of health parameters. We introduced two GNs concepts in this layer. These GNs are not resource-constrained and they serve as an interface between wearable sensors and BS. GNs collect data from nearby wearable sensors and send it to the BS. GNs are also responsible for key authentication with BS. Hence, individual nodes do not need to communicate with BS directly nor they need to involve in the key authentication process. This will improve their computational and energy level. The reason for involving two GNs is that one GN will replace other GN in case of any failure and thus the system will be more reliable. Layer 2 consist of BS that can be any smart device such as smartphone, tablet, PDA, etc. Layer 3 consists of a cloud that provides hosting services for healthcare data and application and layer 4 is the application layer through which care-providers can monitor patients' health. Figure 5 shows the flow diagram of our proposed scheme.

According to Figure 5, wearable sensors attached to the patient body need to connect with GN to transmit data. Once a sensor node is connected to GN, it identifies nearby GN for data transmission. These GNs are responsible for the authentication process and establishing a secure connection. GNs send the collected data to the BS from where it goes to sever. Medical staff can access this data from the server for monitoring a patient's health status and further actions. The algorithm of the proposed scheme is given below

Algorithm 1. Propose Scheme Algorithm

```
1:   Start
2:   Group Nodes initialization
3:   IoT Sensors initialization
4:   IoT Sensors registration with group node A
5:   IoT Sensors registration with group node B
6:   Receiving Key registration from group node
7:   Sensor node communicate with each other
8:   Node transfer the date to group node
9:   Group node transfer the data to base station
10:   if Registration not successful
11:   Go to step 4 or 5
12:   else
13:  Continue process
14:   End if
15:  End
```

4 Mathematical model

In this section, we describe and solve the proposed scheme mathematically. According to the proposed scheme w1, w2, w3….wn are wearable sensor nodes attached to human body. These nodes collect patient's vital information and send it to the BS as shown in Figure 6. Section 4.1 and 4.2 elaborate our objective function and how the proposed scheme help to improve energy and security.

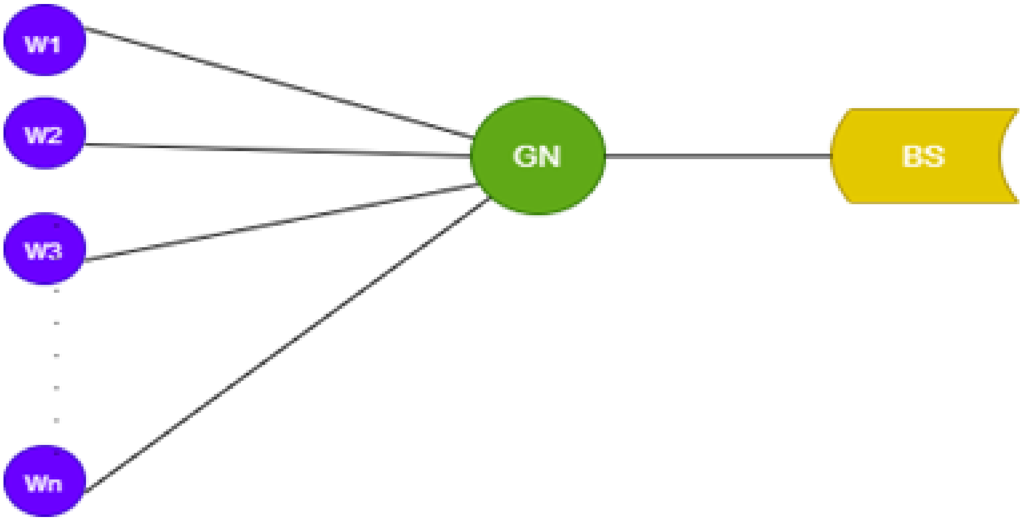


Fig 6. Mathematical model

4.1 Security improvement

According to our model security is dependent on computation, distance, and number of attempts. The mathematical model will be

$$y_1 = f(x_1, x_2\ , \ x_3)$$

$$y_1 = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \varepsilon$$

Where y_1 is a dependent variable that is security in our case

x_1 *and* x_2 *and* x_3 are independent variables where x_1 refers to the computation,x_2 refers to the distance and x_3 refers to the number of attempts

β_0 , β_1,β_2 , β_3 refers to the unknown coefficients

ε refers to the standard error of estimation

The relationship between the independent and dependent variable is inversely proportional which can be represented as

$y_1 \propto \frac{1}{x_1}$ which means security is inversely proportional to computation

$y_1 \propto \frac{1}{x_2}$ which means security is inversely proportional to the distance

$y_1 \propto \frac{1}{x_3}$ which means security is inversely proportional to number of attempts

$$While\ x_1 \propto x_2\ \propto x_3$$

According to our proposed model, there exist linear relationship between dependent and independent variables, below we list our decision variables and objective function

Decision variables:

X$_1$: total computation power used

X$_2$: communication distance between WIS and GN

X$_{3:}$ Number of attempts

Objective function: Max (y$_1$)

Constraints: WIS computation power and storage capacity is limited

To analyze the effect of change in independent variables on dependent variable, we need to find the partial derivatives as

$$y_1 = f\,(x_1, x_2\ , x_3)$$

$$f_{X_1} = \frac{\partial f}{\partial x_1} = \frac{\partial}{\partial x_1} f\,(x_1, x_2\ , x_3) = y_{1X_1} = \frac{\partial y}{\partial x_1} = D_{x_1} f$$

$$f_{X_2} = \frac{\partial f}{\partial x_2} = \frac{\partial}{\partial x_2} f\,(x_1, x_2\ , x_3) = y_{1X_2} = \frac{\partial y}{\partial x_2} = D_{x_2} f$$

$$f_{X_3} = \frac{\partial f}{\partial x_3} = \frac{\partial}{\partial x_3} f\,(x_1, x_2\ , x_3) = y_{1X_3} = \frac{\partial y}{\partial x_3} = D_{x_3} f$$

Let ρ=Group node ϖ= base station

Time taken by wearable sensors for computation= x_1

Computation time with ρ *is* $x_1 - \tau$ *where* τ *is a positive integer*

As $y_1 \propto \frac{1}{x_1}$ *and* $x_1 > x_1 - \tau\ \therefore \rho\ \Vdash y_1$

Distance between wearable nodes w$_1$, w$_2$,w$_3$…….. w$_n$ to ϖ=x_2

Then Distance between wearable nodes w$_1$, w$_2$,w$_3$…….. w$_n$ to ρ=$x_2 - \zeta$ *where* ζ *is a positive integer*

As $y_1 \propto \frac{1}{x_2}$ *and*$x_2 > x_2 - \zeta\ \therefore \rho\ \Vdash y_1$

Number of attempts taken by wearable sensors=x_3

With ρ, x_3= $x_3 - \kappa$ *where* κ *is a positive integer*

As $y_1 \propto \frac{1}{x_3}$ *and* $x_3 > x_3 - \kappa\ \therefore\ \rho\ \Vdash\ y_1$

$y_1 = f(x_1, x_2\ , \ x_3)$ and $(x_1 + x_2\ +\ x_3\ )$ *improves* y_1 *upto* $\zeta + \tau + \kappa$ *by using* ρ

Hence prove that proposed scheme improves security

4.2 Energy efficiency improvement

According to our model energy is dependent on computation, distance, and number of authentications

The mathematical model will be

$$y_2 = f(z_1, z_2\ , z_3)$$

$$y_2 = \alpha_0 + \alpha_1 z_1 + \alpha_2 z_2 + \alpha_3 z_3\ + \varepsilon$$

Where y_2 is a dependent variable that is energy in our case

z_1 *and* z_2 *and* z_3 are independent variables where z_1 refers to the computation,z_2 refers to the distance and z_3 refers to the number of authentications

α_0 , α_1,α_2 , α_3 refers to the unknown coefficients

ε refers to the standard error of estimation

The relationship between independent and dependent variable is inversely proportional which can be represented as

$y_2 \propto \frac{1}{z_1}$ which means energy is inversely proportional to computation

$y_2 \propto \frac{1}{z_2}$ which means energy is inversely proportional to distance

$y_2 \propto \frac{1}{z_3}$ which means energy is inversely proportional to number of authentications

$$While\ z_1 \propto z_2 \propto z_3$$

According to our proposed model, there exist linear relationship between dependent and independent variables, below we list our decision variables and objective function

Decision variables:

Z_1: total computation power used

Z_2: communication distance between WIS and GN

$Z_{3:}$ Number of authentications

Objective function: Min (y_2)

Constraints: WIS computation power and storage capacity is limited

To analyze the effect of change in independent variables on dependent variable, we need to find the partial derivatives as

$$y_2 = f\,(z_1, z_2\ ,\ z_3)$$

$$f_{z_1} = \frac{\partial f}{\partial z_1} = \frac{\partial}{\partial z_1} f\,(z_1, z_2\ ,\ z_3) = y_{2_{z_1}} = \frac{\partial y_2}{\partial z_1} = D_{z_1} f$$

$$f_{z_2} = \frac{\partial f}{\partial z_2} = \frac{\partial}{\partial z_2} f\,(z_1, z_2\ ,\ z_3) = y_{2_{z_2}} = \frac{\partial y_2}{\partial z_2} = D_{z_2} f$$

$$f_{z_3} = \frac{\partial f}{\partial z_3} = \frac{\partial}{\partial z_3} f\,(z_1, z_2\ ,\ z_3) = y_{2_{z_3}} = \frac{\partial y_2}{\partial z_3} = D_{z_3} f$$

Time taken by wearable sensors for computation= z_1

Computation time with $\rho\ is\ z_1 - \theta\ where\ \theta\ is\ a\ positive\ integer$

As $y_2 \propto \frac{1}{z_1}\ and\ z_1 > z_1 - \theta\ \therefore \rho\ \Vdash\ y_2$

Distance between wearable nodes w$_1$, w$_2$,w$_3$…….. w$_n$ to ϖ=z_2

Then Distance between wearable nodes w$_1$, w$_2$,w$_3$…….. w$_n$ to ρ=$z_2 - \lambda\ where\ \lambda\ is\ a\ positive\ integer$

As $y_2 \propto \frac{1}{z_2}\ and z_2 > z_2 - \lambda\ \therefore \rho\ \Vdash y_2$

Number of authentications by wearable sensors=z_3

With ρ, z_3= $z_3 - \xi\ where\ \xi\ is\ a\ positive\ integer$

As $y_2 \propto \frac{1}{z_3}\ and\ z_3 > z_3 - \xi\ \therefore\ \rho\ \Vdash\ y_2$

$y_2 = f(z_1, z_2\ ,\ z_3)$ and $(z_1 + z_2\ +\ z_3\ )\ improves\ y_2\ upto\ \theta + \lambda + \xi\ \ by\ using\ \rho$

Hence prove that proposed scheme improves energy

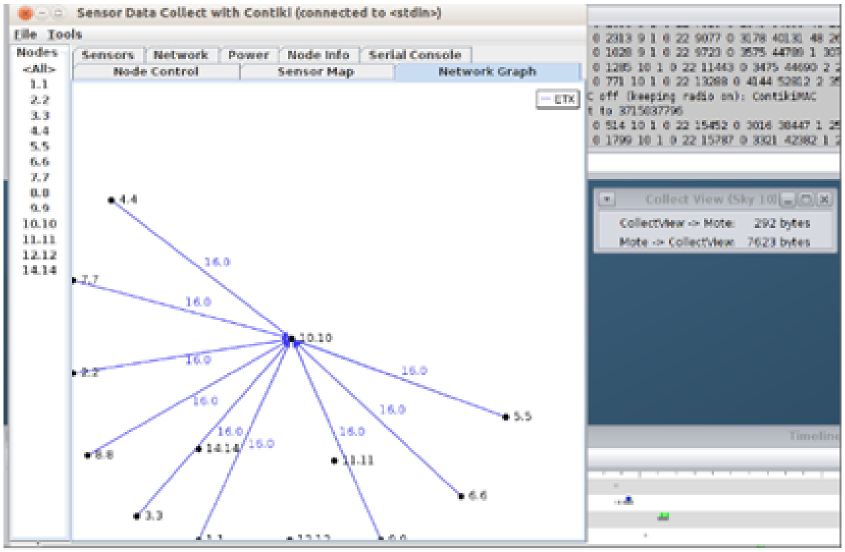
5 Simulation setup

To test our research, we followed two folds means, where we verify our model using mathematical modeling as depicted in the earlier section, besides of that research results has been tested using simulations by adopting a very well-known simulator in the research community Cooja simulator based on Instant Contiki, which is widely used for the same type of IoT based researches (26–30). Since this research linked with the E-health, and indoor patient-oriented environment, where the normal range of the sensor nodes used with patients from 5 to 20. We used our simulation using 25 number of nodes in the simulation area of 150 X 150 meters to avoid the interference. This research used two group nodes concepts by extending the one group node concept presented in (14,31). We use the Unit Disk Graph Medium (UDGM) model with a distance loss model, where links are supposed symmetric, while other wireless environment parameters are ignored (32,33). The random node distributions topology was considered with the patient body. Nodes in the network can transfer data packets to either group node depend on its deployment location. The data transfer considered continuously with a 1-second delay. The data packet default size is 127 bytes. Initial node energy for all nodes was assumed as 2 J. The following Table 2 describes the simulation parameters.

Table 2. Simulation Parameters.

Parameter	Value
Number of Nodes	25
G. Node	2
Routing Protocol	RPL Protocol
Area	150 * 150 m
Simulation Time	3600 Seconds
Transmission Range	50 meters
Interference Range	100 meters
Packet Interval	60 Seconds
Data Packet Size	127 Bytes
Topology	Random
Initial Energy of the nodes	2 J

The simulation used was the main source to collect the results in this case, we used the Cooja Contiki the most common and popular simulator being used for the simulations in IoT. This simulator is used for several different purposes, including the energy efficiency, security attacks, such as version number, rank attacks, etc. this can help to get the information for different aspects as well. The sample screen of the sensor data collection is shown in Figure 7 along with other details.



```
0 2313 9 1 0 22 9077 0 3178 40131 48 2
0 1628 9 1 0 22 9723 0 3575 44789 1 30
0 1285 10 1 0 22 11443 0 3475 44690 2 2
0 771 10 1 0 22 13288 0 4144 52812 2 3
C off (keeping radio on): ContikiMAC
t to 3715037796
0 514 10 1 0 22 15452 0 3016 38447 1 2
0 1799 10 1 0 22 15787 0 3321 42382 1 2
```

CollectView -> Mote: 292 bytes
Mote -> CollectView: 7623 bytes

Fig 7. Simulation Sensor Data Collections sample

6 Result and discussion

The common authentication mechanism is depicted in Figure 8 , the authentication mechanism normally goes in two phases such as authentication phases and key establishment phase.

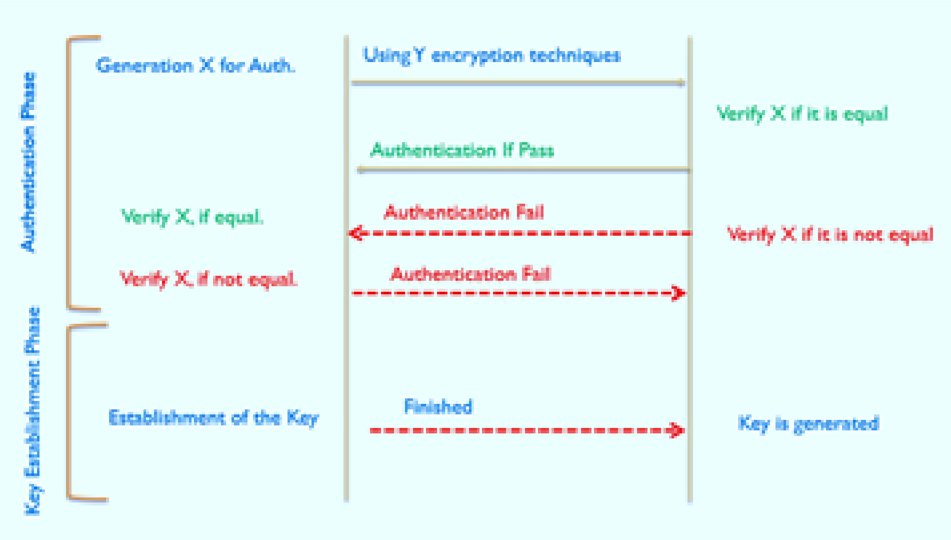


Fig 8. Common Authentication mechanism

In the first phase, it uses specific encryption techniques, which later needs to be verified, in case of successful verification it goes to the second phase of key generation, and in other ways around it ended up with authentication failure state.

Our proposed scheme is mainly considering to the two folds aims, including security and lightweight approach, we used the Elliptic Curve Cryptography (ECC) for the security and lightweight requirements. Further, we have adopted the key generation mechanism from[34]

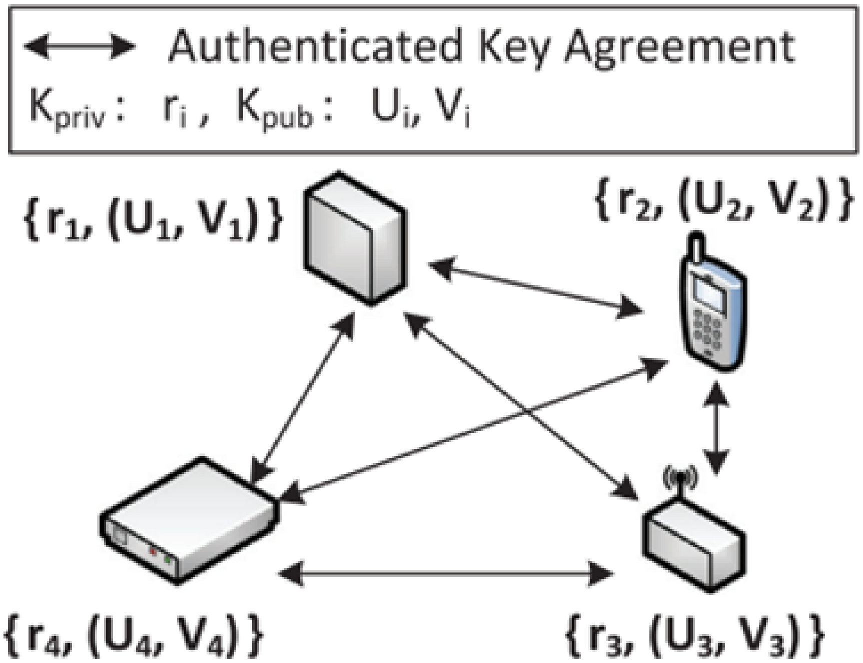


Fig 9. Authentication Key Agreement (AKA)[34]

Our proposed scheme uses the AKA mechanism for the key generation as shown in Figure 9 , which can handle easily to generate the using Key Generation Center (KGC), nodes use ECC symmetric key approach to maintain the secure and lightweight approach. The recent state of the art results presented in (35–37) has elaborated the IoT based lightweight schemes and suggested the use of ECC as well.

Extensive simulation has been done to reach out conclusion, conducted simulation was focused on the performance parameters including the energy efficiency and security of the scheme. The research draws several results considering the main performance parameter, by deploying the nodes without group node GN, and deploying of one GN and later with two GN. Besides, we compare our results with recently presented secure and lightweight schemes (14,31). Our results show an overall significant performance over them. The simulation results are shown below in four different ways including the different cases such as A) random topology without GN concepts, B) random topology with one GN, C) random topology with two GN, and D) random topology with two GN comparing results with the existing group-based approach by Maria, et al.

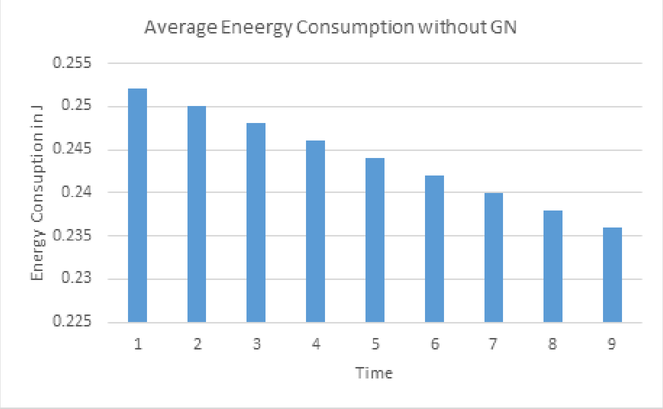


Fig 10. Average Energy Consumption without GN

Figure 10 shows the energy consumption for our proposed scheme with approach A, where the data was transferred directly to the base station rather to use the group node concept. This approach bypasses the group node, as illustrated in our proposed model. This shows that the energy consumption is higher, and it requires multiple iterations from each node to the base station. This enhances the chances of the exploitation for the security and uses more energy due to the data transmission distance since the distance is directly proportional to the energy, higher the distance requires higher energy. Since mostly we use ultra-sensors which are highly resources constrained, and not able to handle the heavy/costly encryption schemes as well. Our proposed scheme considers these issues and proposed multiple group node concept. This will reduce the data transmission distance and to reduce the data iterations as well as authentication registration iterations to reduce the network exploitation to enhance the overall network security.

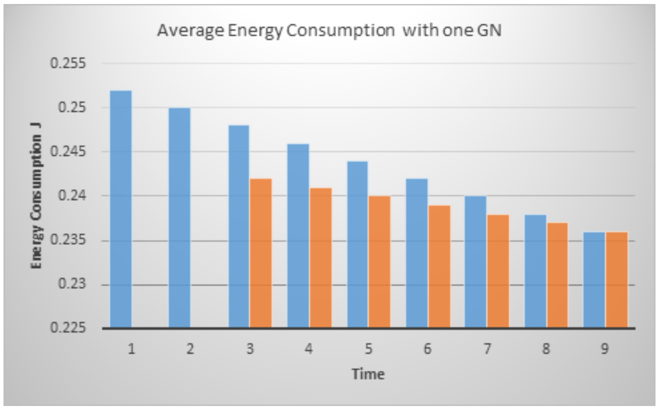


Fig 11. Average Energy Consumption with one GN

Figure 11 shows the energy consumption for our proposed scheme with approach B, where the data was transferred directly to the base station, compared with the use of one GN. The GN reduces the distance of each node, and nodes can be able to transfer the data to the GN rather to the base station. As depicted a significant difference compared with no GN. It shows almost 50% less energy consumption compared to the approach A. At the same time, it enhances the security level of the network by reducing the iterations of nodes, GN can register for authentication for nodes and can share the key with them.

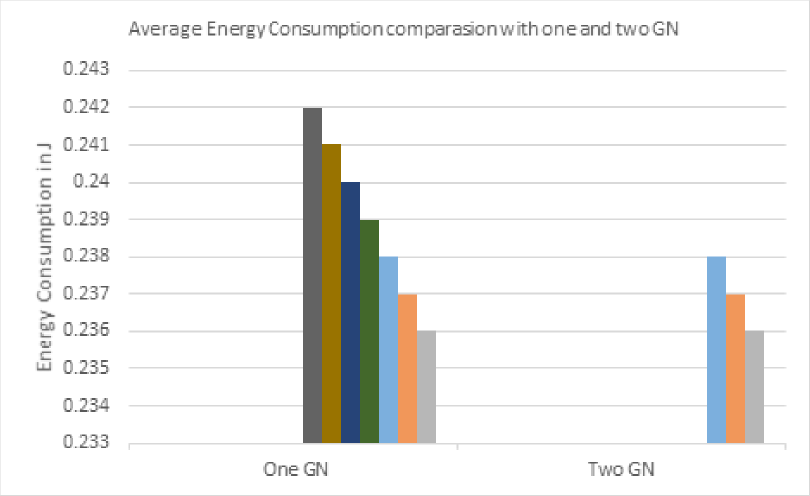


Fig 12. Average Energy Consumption Comparison among two GN

Figure 12 shows the energy consumption for our proposed scheme with approach C, where the data was transferred using the two GN either one, this approach is adopted to further reduce the communication distance during data transfer. The multi GN reduces further communication distance and enhances further energy consumption. This leads to security as well on the same principles. The nodes in the body area network are divided into two clusters, and each cluster is being handled with its respective GN and then GN can transfer the data to the Base station and so on. This shows further approximately 15% significant improvement of the results compared to the one GN as shown in Figure 12.

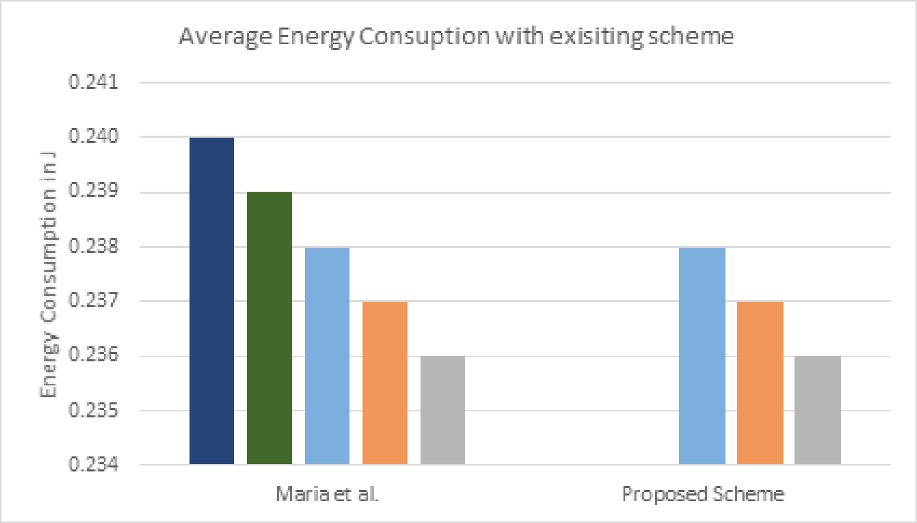


Fig 13. Average Energy Consumption Comparison with Marita et al.

Figure 13 shows the average energy consumption for our proposed scheme with approach D, where the data was transferred using the two GN has been compared with the existing approach [14,31]. This comparison shows a significant 10% improvement with our proposed scheme. This further strengthens the presented concept of GN. However, we found that this approach is only feasible for the indoor E-Health applications, while the research reveals that the same significant improvement level is not noticed for outdoor E-Health applications. We found that the two GN concept can be adapted for indoor E-health applications for better security and lightweight use.

The results of our proposed schemes are compared with the recently presented work (14,31) who presented the group node concept for the E-health applications and covers the indoor patients. Our results showed a significant improvements over the schemes presented in (14,31).

7 Conclusion

This paper presents a secure and energy-efficient scheme of patient's data transmission for indoor E-health applications using IoT. IoT sensors are widely used in the healthcare domain for real-time data collection and transmission. However, these are vulnerable due to the resource-constrains, which requires specific secure and lightweight schemes to overcome this. To address these issues, our proposed scheme presented a concept of the multi-group node to reduce the data transmission distance to enhance the energy consumption, as well as to reduce the possible exposure, and iterations of the nodes for the registration and key authentication. The key authentication registration can be done by the group nodes and one common key can be shared with the nodes in the network. Our proposed scheme will have an edge over using the elliptic curve cryptography (ECC) approach which will be resilient against several attacks for E-health applications. The proposed study was tested with 4 different cases, including without GN, with one GN, with two GN and finally compared our achieved results with the existing research work. The presented research is supported by our presented scheme with a mathematical model and extensive simulation results. The results show a significant improvement in energy efficiency while using a multi-group node concept. It outperforms as well when compared with the existing group node approaches approximately 10% higher.

Acknowledgment

This research has been funded by the Deanship of Scientific Research, Jouf University, under the grant number, 40/222. We acknowledge their cooperation and support to complete this research.

References

1) Farahani B, Firouzi F, Chakrabarty K, Iot H. Healthcare IOT. In: and others, editor. Intelligent Internet of Things. Springer. 2020;p. 515–545. Available from: https://doi.org/10.1007/978-3-030-30367-9_11.
2) Satija U, Ramkumar B, Manikandan MS. Real-Time Signal Quality-Aware ECG Telemetry System for IoT-Based Health Care Monitoring. *IEEE Internet of Things Journal*. 2017;4(3):815–823. Available from: https://dx.doi.org/10.1109/jiot.2017.2670022.
3) Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*. 2020;50:102407–102407. Available from: https://dx.doi.org/10.1016/j.jisa.2019.102407.
4) Greco L, Ritrovato P, Xhafa F. An edge-stream computing infrastructure for real-time analysis of wearable sensors data. *Future Generation Computer Systems*. 2019;93:515–528. Available from: https://dx.doi.org/10.1016/j.future.2018.10.058.
5) Indrakumari R. The growing role of Internet of Things in healthcare wearables. *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach 2020*;p. 163–194. Available from: https://doi.org/10.1016/B978-0-12-819593-2.00006-6.
6) Hathaliya J, Sharma P, Tanwar S, Gupta R. Blockchain-based remote patient monitoring in healthcare 4.0. In: and others, editor. 2019 IEEE 9th International Conference on Advanced Computing (IACC). IEEE. 2019;p. 87–91. Available from: https://doi.org/10.1109/IACC48062.2019.8971593.
7) Muthu B. IOT based wearable sensor for diseases prediction and symptom analysis in healthcare sector. *Peer-to-Peer Networking and Applications*. 2020;2020:1–12. Available from: https://doi.org/10.1007/s12083-019-00823-2.
8) Jayatilleka I, Halgamuge MN. Chapter 1 - Internet of Things in healthcare: Smart devices, sensors, and systems related to diseases and health conditions. In: and others, editor. Real-Time Data Analytics for Large Scale Sensor Data. Elsevier. 2020;p. 1–35. Available from: https://doi.org/10.1016/B978-0-12-818014-3.00001-2.
9) Kaur H, Atif M, Chauhan R. An Internet of Healthcare Things (IoHT)-Based Healthcare Monitoring System. *Advances in Intelligent Computing and Communication 2020*;p. 475–482. Available from: https://doi.org/10.1007/978-981-15-2774-6_56.
10) Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, et al. BHEEM: A blockchain-based framework for securing electronic health records. In: and others, editor. 2018 IEEE Globecom Workshops (GC Wkshps). IEEE. 2018;p. 1–6. Available from: https://doi.org/10.1109/GLOCOMW.2018.8644088.
11) Hathaliya JJ, Tanwar S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*. 2020;153:311–335. Available from: https://dx.doi.org/10.1016/j.comcom.2020.02.018.
12) Hathaliya JJ, Tanwar S, Evans R. Securing electronic healthcare records: A mobile-based biometric authentication approach. *Journal of Information Security and Applications*. 2020;53:102528–102528. Available from: https://dx.doi.org/10.1016/j.jisa.2020.102528.
13) Salih FI. IoT security risk management model for healthcare industry. *Malaysian Journal of Computer Science*. 2019;p. 131–144. Available from: https://doi.org/https://doi.org/10.22452/mjcs.sp2019no3.9.
14) Almulhim M, Islam N, Zaman N. A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications. *International Journal of Computer Science and Network Security*. 2019;19(1):107–120. Available from: https://expert.taylors.edu.my/file/rems/publication/109566_5572_1.pdf.
15) Humayun NZM, Jhanjhi, Malak Z, Alamri. Smart Secure and Energy Efficient Scheme for E-Health Applications using IoT: A Review. *IJCSNS International Journal of Computer Science and Network Security*. 2020;(6):20–20.

16) Khemissa H, Tandjaoui D. A lightweight authentication scheme for e-health applications in the context of internet of things. In: and others, editor. 9th International Conference on Next Generation Mobile Applications, Services and Technologies. 2015. Available from: https://doi.org/10.1109/NGMAST.2015.31.

17) Gope P, Hwang T. BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. *IEEE Sensors Journal*. 2016;16:1368–1376. Available from: https://dx.doi.org/10.1109/jsen.2015.2502401.

18) Alromaihi S, Elmedany W, Balakrishna C. Cyber security challenges of deploying IoT in smart cities for healthcare applications. In: and others, editor. 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). IEEE. 2018. Available from: https://doi.org/10.1109/W-FiCloud.2018.00028.

19) Islam SR. The internet of things for health care: a comprehensive survey. *IEEE Access*. 2015;3:678–708. Available from: https://doi.org/10.1109/ACCESS.2015.2437951.

20) Zakaria H. IoT Security Risk Management Model for Secured Practice in Healthcare Environment. *Procedia Computer Science*. 2019;161:1241–1248. Available from: https://doi.org/10.1016/j.procs.2019.11.238.

21) Moosavi SR. Performance analysis of end-to-end security schemes in healthcare IoT. *Procedia computer science*. 2018;130:432–439. Available from: https://doi.org/10.1016/j.procs.2018.04.064.

22) Luo E. Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Communications Magazine*. 2018;56(2):163–168. Available from: https://doi.org/10.1109/MCOM.2018.1700364.

23) Moosavi SR. SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science*. 2015. Available from: 10.1016/j.procs.2015.05.013.

24) Zouka HAE, Hosni MM. Secure IoT communications for smart healthcare monitoring system. *Internet of Things*. 2019;p. 100036–100036. Available from: https://dx.doi.org/10.1016/j.iot.2019.01.003.

25) Elhoseny M. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access*. 2018;6:20596–20608. Available from: https://doi.org/10.1109/ACCESS.2018.2817615.

26) Dunkels A. Contiki: The Open Source OS for the Internet of Things. 2003. Available from: http://www.contikios.org/index.html.

27) Ali H. A Performance Evaluation of RPL in Contiki :a Cooja Simulation based study. Sweden. 2012. Available from: https://bit.ly/37MlnNI.

28) Romdhani I, Al-Dubai AY, Qasem M, Ghaleb B. Cooja Simulator Manual. United Kingdom. Edinburgh Napier University. 2016.

29) Bagula B, Erasmus Z. IOT emulation with Cooja. In: and others, editor. ICTP-IoT Workshop. 2015. Available from: https://bit.ly/2NulRyZ.

30) Dunkels A, Gronvall B, Voigt T. Contiki - a lightweight and flexible operating system for tiny networked sensors. In: 29th Annual IEEE International Conference on Local Computer Networks. 2004;p. 16–18. Available from: https://doi.org/10.1109/LCN.2004.38.

31) Almulhim M, Zaman N. Proposing secure and lightweight authentication scheme for IoT based E-health applications. *20th International Conference on Advanced Communication Technology (ICACT)*. 2018;p. 481–487. Available from: https://doi.org/10.23919/ICACT.2018.8323802.

32) Rezaei E. Energy Efficient RPL Routing Protocol in Smart Buildings. Waterloo, Ontario, Canada. 2014. Available from: http://hdl.handle.net/10012/8544.

33) Mehmood T. COOJA Network Simulator: Exploring the Infinite Possible Ways to Compute the Performance Metrics of IOT Based Smart Devices to Understand the Working of IOT Based Compression & Routing Protocols. 2017. Available from: arXiv:1712.08303v1.

34) Marcos A, Simplicio, et al. Lightweight and escrow- Less authenticated key agreement for the IoT. *Computer Communications*. 2017;98:43–51. Available from: https://doi.org/10.1016/j.comcom.2016.05.002.

35) Almusaylim ZA, Zaman N. A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). *Wireless Networks*. 2019;25:3193–3204. Available from: https://dx.doi.org/10.1007/s11276-018-1712-5.

36) Almusaylim ZA, Alhumam A, Jhanjhi NZ. Proposing a Secure RPL based Internet of Things Routing Protocol: A Review. *Ad Hoc Networks*. 2020;101:102096–102096. Available from: https://dx.doi.org/10.1016/j.adhoc.2020.102096.

37) Diro A, Reda H, Chilamkurti N, Mahmood A, Zaman N, Nam Y. Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication. *IEEE Access*. 2020;8:60539–60551. Available from: https://dx.doi.org/10.1109/access.2020.2983117.