International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

RESEARCHERID
THOMSON REUTERS

[Sharma *et al.*, 9(11): November, 2020]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

AN IOT-BASED REMOTELY HEALTH MONITORING SYSTEM USING LOCATION PRIVACY MECHANISM FOR WBAN MODEL

Swati Sharma*[1] & Er. Shivani Rana[2]
*1&2HPTU, Himachal Pradesh

DOI: https://doi.org/10.29121/ijesrt.v9.i11.2020.2

ABSTRACT

In these days the demand of remote health monitoring rapidly increases due to in involvement of Wireless Body Area Network (WBAN) that is used for heal monitoring application in real-time scenario due to its capabilities of sensing and fast communication. It is a type of Wireless Sensor Network (WSN) model that consist of various tiny sensor nodes which are power by batteries and used routing algorithms to send a data packets from one node to other via the base station. But energy efficient and secure data transmission is an important factor for any remote location based health monitoring system. So, in this research, we proposed a Remote Location-based Health Monitoring (RLHM) system using the concept of Elliptical Curve Cryptography (ECC) as an encryption method for WBAN model. An intellectual and secure transmission in ECC-based RLHM system with WBAN is based on the location privacy preservation mechanism to support the network communication. The introduced ECC based intellectual and secure transmission mechanism as a routing protocol diminish the involvement of abnormal nodes between end to end nodes in the network to increase the efficiency. At the last of paper, the comparison of proposed ECC-based RLHM system with existing work in presented in respects of Quality of Service (QoS) like verification time, key size and message size and we noticed that the time of verification is reduced by existing in the WBAN model.

KEYWORDS: Location-based Health Monitoring (RLHM) system, Wireless Body Area Network (WBAN), Elliptical Curve Cryptography (ECC), Quality of Service (QoS).

1. INTRODUCTION

In the last few decade, the count of fragile persons such as physically disabled, seniors citizen and those suffering from the chronic or other diseases such as diabetics, arthritis, asthma, cancer etc. living in their own homes is increasing exponentially [1]. As per facing such problems by patients, there is a wide research area become open as an interest for efficient and effective ways to help the patient by remotely monitoring mechanism in their home [2]. This type of monitoring model has been shown that constant patient health monitoring can lead to 50% reduction in hospitalizations, 73% drop in emergency room visits, and 51% decrease in patient cost [3]. Also the wireless communication brought numerous benefits to our society in lot of matter and it is better option to adopt as a new technique in the Remote Location-based Health Monitoring (RLHM) system. Upgradation in the area of wireless technology has made this communication possible by the help of Bluetooth, WI-FI, 4G, and LTE and so on [4]. Recently, the concept of Wireless Sensor Network (WSN) for device to device communication and monitoring of environmental condition, healthcare system, automobile industry, telecom industry etc. has been a favorite area of research in past few decades [5]. Communication between machines and the human was next destination of the researcher and towards this step, the concept of RLHM system is an innovative. Low power, lightweight and miniature physiological sensors has made it possible to connect remotely the patient with doctor or other medical practitioners and this type of mechanism is known as Wireless Body Area Network (WBAN) [6]. The development of RLHM system is becoming standard care practices but some questions arises like how to offer quality patient care outside the hospital setting and security of patient location in a cost effective manner have become an interesting but challenging problem of WBAN [7].

Hence, the deployment of WBANs-based RLHM system in an Internet of Things (IoT) environment may well take care of the patients with secure way by securing their location using the concept of encryption technique for location privacy [8]–[10].

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

The secure and efficient WBAN technology allows the medical practitioners or doctors to respond to the patient from any remote location with secure location or without share own location. So that, in any type sudden emergency situation can be avoided and undated death rate will be controlled [11]. Nowadays, WBAN based health monitoring technology plays vital role for an average income family and reduces the medical bills by create an environment of RLHM system that is based on the Elliptical Curve Cryptography (ECC) concept for WBAN model that is shown in the below Fig. 1.

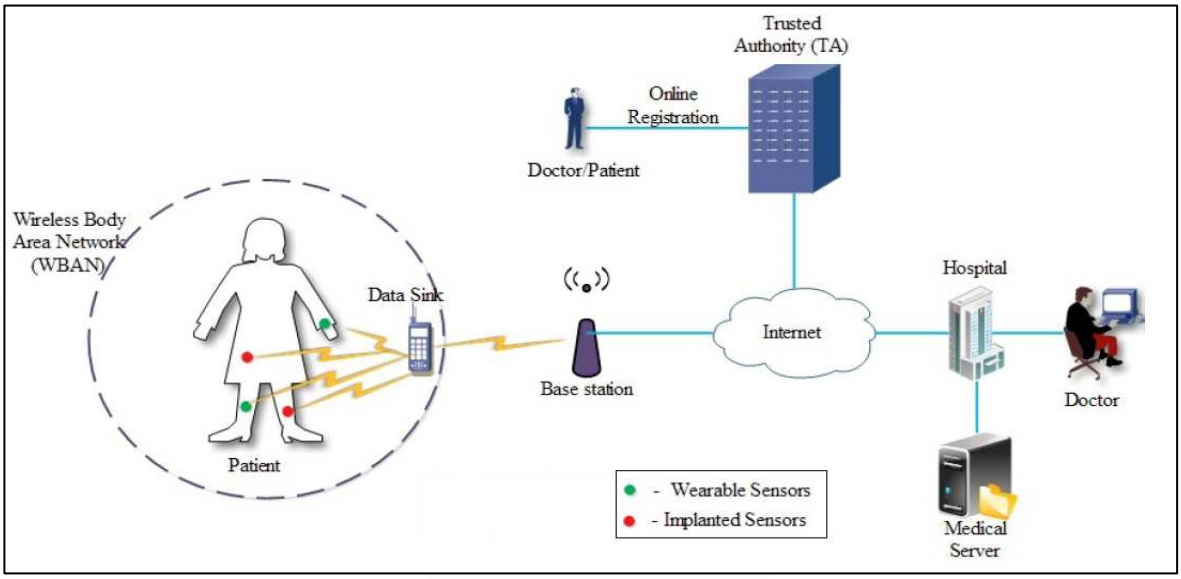


Fig 1: RLHM System Architecture

Fig 1 represents the architecture of proposed WBAN-based RLHM system with deployment of sensor nodes within the patient in or on body both. The main motivation behind the development of this model is the existing model drawbacks like their poor security constraint and we introducing a model using the concept of ECC as an encryption technique and the contributions are listed as:

- ❖ We introducing the concept of location privacy using the ECC encryption approach to secure the patient and doctor location.
- ❖ The concept of database management is used to store the location coordination of the patient and doctor or medical practitioner during the transmission of data packets from T_X-Patient to R_X-Doctor.
- ❖ To validate the proposed RLHM system with the help of WBAN, a comparison with the existing state of the art is performed based on the verification time on side of patients or doctors.

The main focus of this research article is to introduce ECC based RLHM system with the help of WBAN for secure and debauched communication in healthcare monitoring era. The remaining research article is organized as follows. In Sect. 2, survey of existing works are described. Sect. 3 describes the method and materials of proposed RLHM model and the simulation results and analysis are presented in Sect. 4. Finally, in Sect. 4, the conclusion with the future trends is discussed.

2. RELATED WORK

In this area lots of research works already done but since having many issues and challenging factors, so we presents a brief survey of existing models. ***P Vijayakumar et al.*** in 2019 had conducted a research on the efficient and secure anonymous authentication with location privacy for IoT-based WBANs. They proposed a framework with location privacy preservation for IoT-based WBANs using the concept of an efficient and secure anonymous authentication. The comprehensive analysis section shows that the proposed scheme overcomes the security weaknesses in the existing schemes and also provides low computation cost during anonymous authentication. ***S.***

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

R. Chavva et al. in 2019 had conducted a research regarding to develop an energy-efficient multi-hop routing protocol for WBAN-based health monitoring system. Authors presented a joint scheduling and admission control problem with optimizing the both intra and beyond WBAN-based health monitoring system. A protocol in WBAN was design to transfers body sensing data from various sensors to sink or gateway node using multi-hop routing technique. The main objective of research is to prolong the average network life time of WBAN-based health monitoring system by reducing overall energy consumption on network during the data transmission. They select a parent sensor node based on their residual energy by the concept of using fuzzy logic approach to improve the efficiency of system. The simulation results show the efficiency of developed model is better as compere to the other state-of-art routing algorithms like SIMPLE and M-ATTEMPT but still need to identify the fail or malicious from the discovered route to reduce the drop rate. A model using the concept of priority based data packet balancing in queue for WBAN was designed by the ***A. Sahoo et al.*** in 2019 in IIT, Kanpur. The main objective of authors is to forward the most critical packets firstly based on the on demand and then give priority to non-critical packets transmission to control the emergency situation in WBAN-based any healthcare monitoring system. The designed protocol uses two separate queues of the data packets based on their priorities and threshold value. This novel routing protocol also consider the remaining time of critical packets for the comparison of same type of data packets. Author also introduced the facility of this protocol is that the on-demand packets can be transmitted earlier if there are no packets in both High Threshold Emergency Queue (HTEQ) and Low Threshold Emergency Queue (LTEQ). This research work has been more attractive over their counterparts in terms of QoS parameters such as throughput, ratio of packet delivery, transmission delay and energy consumption. A robust energy efficiency optimization algorithm based health monitoring system with concept of WBAN was developed by ***O. Amjad et al.*** in 2020. They use a summed up gamma dissemination that underpins different patient conditions during day by day life exercises and can effectively show both consistently and dynamic exercises. The streamlining issue expects to enhance every sensor transmit force and encoding rate to limit the EE (estimated in J/bits) by thinking about blackout likelihood and parcel retransmission. It is indicated that the detailed advancement issue is semi-carefully semi curved in every choice variable, and an elective streamlining approach is proposed to decide its answer.

Based on the analysis of existing research using the concept of WBAN-based area of healthcare system, we conclude some important and major point which helps to short out existing work problems.

- ✓ In this work, ECC based routing mechanisms which is introducing that improve the network security by preserving the location.
- ✓ Health monitoring purpose, network security as well as data transmission rate should be better, so, utilization encryption approach would be better option for WBAN-based RLHM system.

So in this work, we proposed ECC-based RLHM system with the help of WBAN architecture that can be easily generalized to other challenging such as routing and security problems and also improve the verification time of the model which helps to provide a better transmission.

3. METHOD & MATERIALS

We explain the methodology and algorithms which are used to design an ECC-based RLHM System with WBAN model. The proposed system consist of total eight biomedical sensor node named as EEG, ECG, EMG, BP, Pulse-Oximeter, Motion, Glucose and Temperature. The sensed data by sensor nodes are collected by the sink node for the further processing using the combination of ECC with proposed model. The procedural steps of proposed ECC-based RLHM system are defined as follows:

A. RLHM Model: Firstly design simulator for the simulation of proposed ECC-based RLHM system using the concept of graphical user interface in MATLAB 2016a software. The area of proposed RLHM system is defined by using the given formula of geometrical area calculation;

$$\boldsymbol{RLHM\ Area = Height(m) X\ Width(m)} \ldots\ldots \textbf{(1)}$$

Where, Height is the ECC-based RLHM system height (1000m) and Width is the ECC-based RLHM system width (1500) and the total RLHM area is shown in the Fig. 2.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

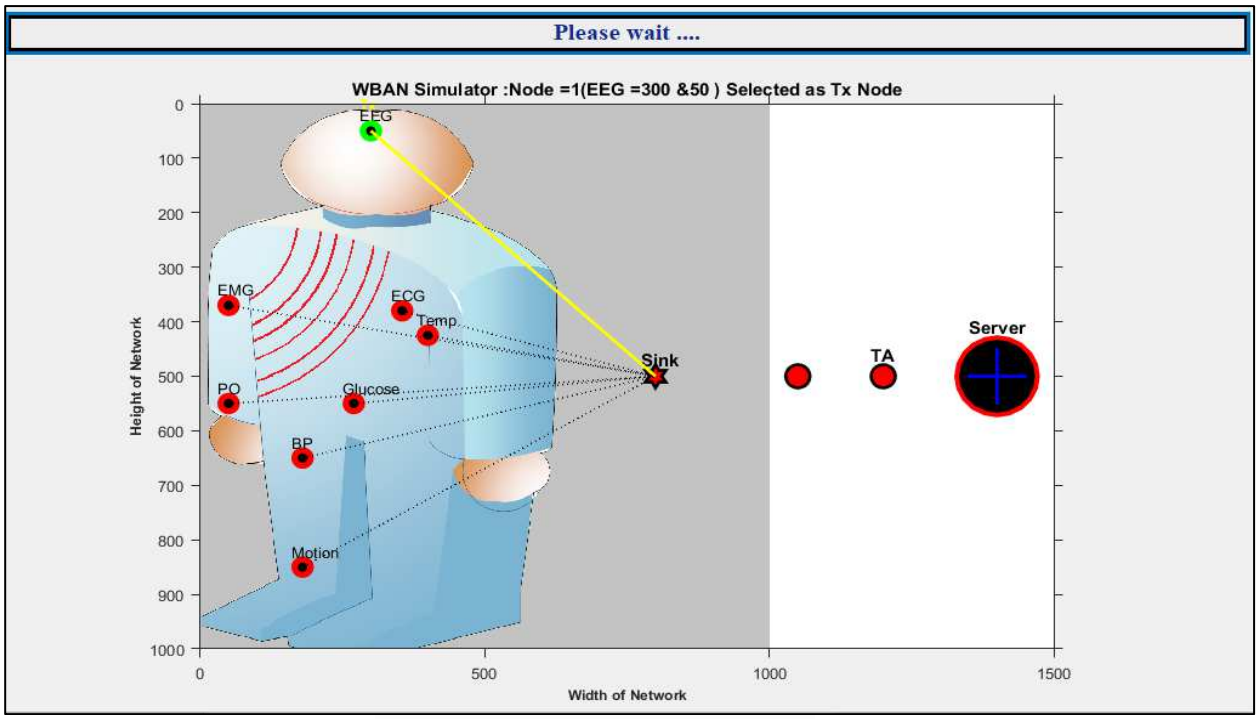
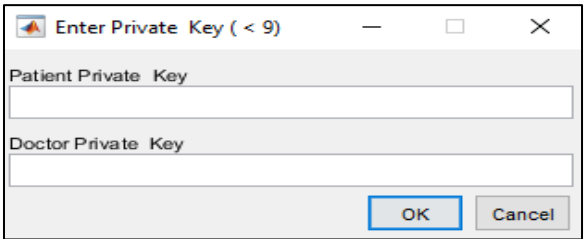


Fig 2: ECC-based RLHM Simulation Model

The develop simulation area of ECC-based RLHM system is shown in the Fig. 2 where total eight sensor nodes are implanted in the human or patient body on the specific geometrical location named as EEG, ECG, EMG, BP, PO, M, G and T.

Where, EEG → Electroencephalogram
ECG → Electrocardiograph
EMG → Electromyogram
BP →Blood Pressure
PO →Pulse-Oximeter
M →Motion
G →Glucose
T →Temperature

B. Routing in RLHM System: After the simulator development, we discover the route from the source (T_X-Patient) to destination (R_X-Doctor) via gateways and base station whether secure route is decided based on intermediates sensor nodes properties. Form the Fig. 2, in the Route (R), Biosensor Node-EEG is Source (T_X-Patient) and doctor location is Destination (R_X-Doctor). Here, sink node used the concept of ECC to encrypt the location on the patients and biosensors using the secret key.



ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Here, we apply the ECC encryption algorithm to secure the location by providing the patient and doctor private key, after that, we create a secure and energy efficient route from source (T_X-Patient) to destination (R_X-Doctor) via sink or base station node that is shown in the Fig. 3.

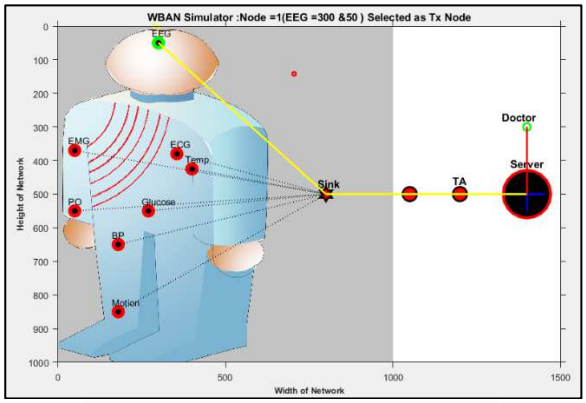


Fig 3: Route in ECC-based RLHM model

C. ***Quality of Service (QoS):*** After the simulation of the proposed ECC-based RLHM system, we calculate the QoS parameters in terms of verification time, we comparing with existing work on the basis of below given experimental setup in Table I.

Table I: System Setup

Number of Biosensor Nodes	**8 [EEG, ECG, EMG, BP, Pulse-Oximeter, Motion, Glucose, Temperature]**
Height of RLHM System	**1000m**
Width of RHM System	**1500m**
Simulation Tool	**Communication Toolbox in MATLAB Software**
Simulation Time	**10 to 100 ms**
Evaluation Parameter	**Verification time, Encryption Time, Decryption Time, Key Size and Message Size**

The simulation results of proposed ECC-based RLHM system is described in the below section of paper.

4. RESULTS AND DISCUSSION

In this section, we describe the simulation results of the proposed ECC-based RLHM system the WBAN model on basis of the Table I experimental scenario and compare with existing work by ***P Vijayakumar et al.*** in 2019 [12] work. In the point of view of wireless communication in proposed ECC-based RLHM system, we presents the QoS parameters in terms of the Verification time, Encryption Time, Decryption Time, Key Size and Message Size.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

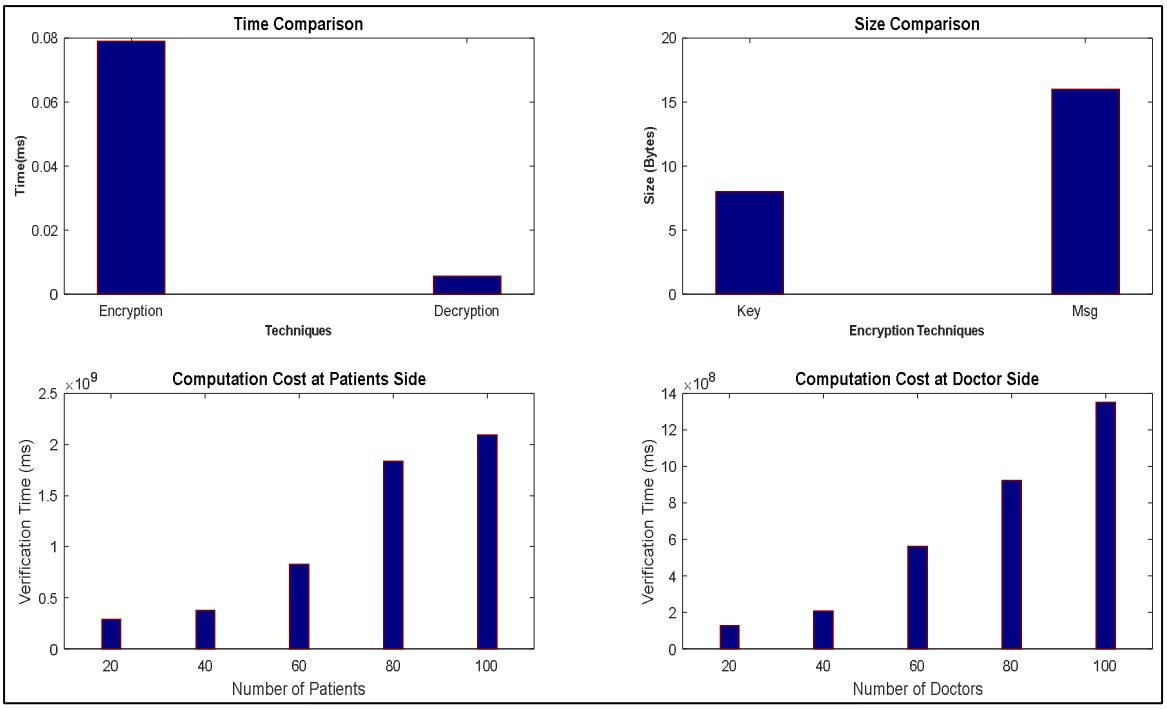


Fig 4: QoS Parameters of the ECC-based RLHM Model

According to the above figure, we observed that the throughput of proposed ECC-based RLHM system is improved by utilization of ECC approach as an encryption technique and the comparison with existing work is shown in the below Fig. 5. Firstly, we create a comparison table for patients and doctor and we consider both from 1 to 100.

Table II: Comparison of Verification Time

No.	Patients		Doctors	
	Existing	Proposed	Existing	Proposed
20	110	80	60	35
40	260	105	130	58
60	420	230	260	156
80	570	510	340	256
100	730	580	450	375

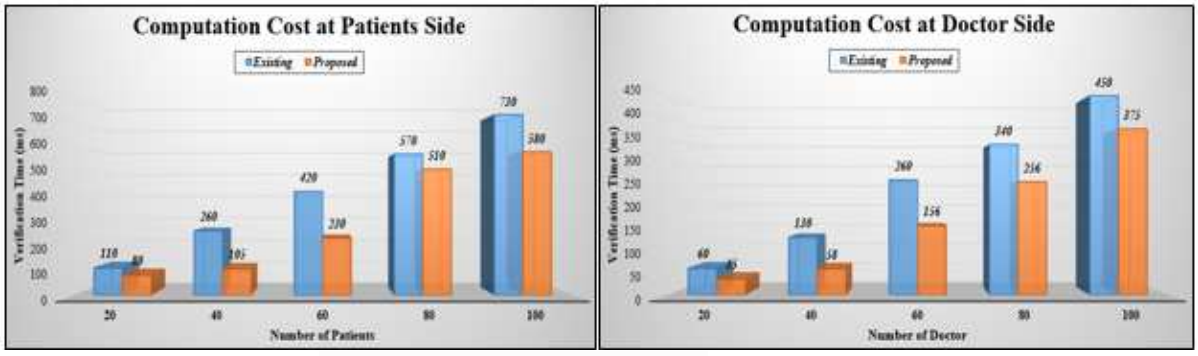


Fig 5: QoS Parameters Comparison of Verification Time

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

The comparison of the QoS parameters in term of the verification time on both side, patient as well as doctor side is given the above Table II and Fig. 5. Finally, from the analysis, we observed that the utilization of ECC is a beneficial step towards development of a secure WBAN-based intellectual and energy efficient transmission mechanism as a RLHM system and the encryption time as well the size of key is also reduced as compare to the existing architecture and the model is also secure to encrypt an decrypt the location of patient as well as doctors or medical practitioners.

5. CONCLUSION AND FUTURE WORK

In this paper, An IoT-based RLHM using location privacy mechanism for WBAN model is proposed for secure communication. Here we used the ECC as an encryption technique to encrypt or decrypt the patients or doctor location. We know that the ECC-based RLHM system is an emerging field of research within the domain of healthcare but the secure communication is a big concern that is solved in this research by utilizing the concept of encryption technique with the improvisation in the routing technique. The main aim of research is to minimize the verification time with secure and fast data transmission through the trust of the route in WBAN model in both patients as well as doctors side. The performance of the proposed WBAN-based RLHM system is much better than existing work in respects of verification time and also we calculate the size of key and size of message. The data transmission also becomes more secure by encrypting the location of patients and the effect of attackers is reduces in the WBAN but need to speed up the data transmission rate with the energy minimization concept. So, in future, the idea of optimized deep learning will be utilized as a classifier to prepare ECC-based RLHM system in WBAN model for handling the privacy issues and reliability issues in medical data with natural computing based Meta heuristic algorithm.

REFERENCES

[1]. Samanta, Amit, and SudipMisra. "Energy-efficient and distributed network management cost minimization in opportunistic wireless body area networks." IEEE Transactions on Mobile Computing 17.2 (2018): 376-389.
[2]. Rahmani, Amir M., Tuan Nguyen Gia, BehailuNegash, Arman Anzanpour, ImanAzimi, Mingzhe Jiang, and PasiLiljeberg. "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach." Future Generation Computer Systems 78 (2018): 641-658.
[3]. Shamsan Saleh, A. M., Ali, B. M., Rasid, M. F. A., & Ismail, A. (2014). A survey on energy awareness mechanisms in routing protocols for wireless sensor networks using optimization methods. Transactions on Emerging Telecommunications Technologies, 25(12), 1184-1207.
[4]. Liu, Qi, et al. "A speculative approach to spatial-temporal efficiency with multi-objective optimization in a heterogeneous cloud environment." Security and Communication Networks9.17 (2016): 4002-4012.
[5]. Khalid, Adia, Nadeem Javaid, Mohsen Guizani, MusaedAlhussein, Khursheed Aurangzeb, and ManzoorIlahi. "Towards dynamic coordination among home appliances using multi-objective energy optimization for demand side management in smart buildings." Ieee Access 6 (2018): 19509-19529.
[6]. Gravina, Raffaele, ParastooAlinia, Hassan Ghasemzadeh, and Giancarlo Fortino. "Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges." Information Fusion 35 (2017): 68-80.
[7]. Iqbal, Muhammad, Muhammad Naeem, AlaganAnpalagan, Ashfaq Ahmed, and Muhammad Azam. "Wireless sensor network optimization: Multi-objective paradigm." Sensors 15, no. 7 (2015): 17572-17620.
[8]. Klemm, Maciej, and Gerhard Troester. "Textile UWB antennas for wireless body area networks." IEEE Transactions on Antennas and Propagation 54, no. 11 (2006): 3192-3197.
[9]. Moraes, Jermana L., Matheus X. Rocha, Glauber G. Vasconcelos, José E. Vasconcelos Filho, Victor Hugo C. De Albuquerque, and Auzuir R. Alexandria. "Advances in photopletysmography signal analysis for biomedical applications." Sensors 18, no. 6 (2018): 1894.
[10]. Zang, Weilin, Fen Miao, Raffaele Gravina, Fangmin Sun, Giancarlo Fortino, and Ye Li. "CMDP-based intelligent transmission for wireless body area network in remote health monitoring." Neural computing and applications 32, no. 3 (2020): 829-837.
[11]. Chavva, Subba Reddy, and Ravi Sankar Sangam. "An energy-efficient multi-hop routing protocol for health monitoring in wireless body area networks." Network Modeling Analysis in Health Informatics and Bioinformatics 8, no. 1 (2019): 21.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[12]. Vijayakumar, P., Obaidat, M. S., Azees, M., Islam, S. H., & Kumar, N. (2019). Efficient and secure anonymous authentication with location privacy for IoT-based WBANs. IEEE Transactions on Industrial Informatics, 16(4), 2603-2611.
[13]. Sahoo, Anita, Tusharkanta Samal, and Bivasa Ranjan Parida. "Priority based Packet Balanced Queue MAC protocol in Wireless Body Area Network." In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-6. IEEE, 2019.
[14]. Amjad, Osama, Ebrahim Bedeer, Najah Abu Ali, and Salama Ikki. "Robust Energy Efficiency Optimization Algorithm for Health Monitoring System with Wireless Body Area Networks." IEEE Communications Letters 24, no. 5 (2020): 1142-1145.
[15]. Argyriou, Antonios, Alberto Caballero Breva, and Marc Aoun. "Optimizing data forwarding from body area networks in the presence of body shadowing with dual wireless technology nodes." IEEE Transactions on Mobile Computing 14, no. 3 (2014): 632-645.
[16]. Islam, Md Zahidul, Sazzad Hossain Rafi, and Md Murad Miah. "Remote Health Monitoring System using Wireless Body Area Network." Global Journal of Research in Engineering (2019).
[17]. Nidhya, R., and S. Karthik. "Security and privacy issues in remote healthcare systems using wireless body area networks." In Body Area Network Challenges and Solutions, pp. 37-53. Springer, Cham, 2019.
[18]. Asam, M., Jamal, T., Ajaz, A., Haider, Z., & Butt, S. A. (2019). Security Issues in WBANs. arXiv preprint arXiv:1911.04330.
[19]. Tan, H., & Chung, I. (2019). Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor. IEEE Access, 7, 151459-151474.
[20]. Aktas, F., Ceken, C., & Erdemli, Y. E. (2018). IoT-based healthcare framework for biomedical applications. Journal of Medical and Biological Engineering, 38(6), 966-979.