An Improved Remotely Health Monitoring System based on IoT Communication using Location Privacy Mechanism for WBAN Model

Oshin Behl #1, Er. Pallavi Garg #2
Student #1, Assistant Professor #2
#SIRDA Institute of Engineering & Technology Sundernagar Distt-Mandi, Himachal Pradesh-175021

Abstract: Due to the participation of Wireless Body Area Network (WBAN), which is employed for heal monitoring application in a real-time situation due to its sensing and quick transmission capabilities, the need for remote health monitoring is rapidly increasing these days. It's a Wireless Sensor Network (WSN) concept made up of a number of small sensor nodes that are powered by batteries and employ routing algorithms to deliver data packets from one node to the next via the base station. However, for any remote location based health monitoring system, energy efficiency and secure data transfer are critical. As a result, in this study, we suggested an Improved Remote Health Monitoring (IRHM) system for the WBAN model that uses the notion of Elliptical Curve Cryptography (ECC) as an encryption mechanism. In an ECC-based IRHM system with WBAN, an intellectual and secure transmission is based on a location privacy preservation method to allow network communication. The introduced ECC-based intellectual and secure transmission mechanism as a routing protocol reduces the involvement of anomalous nodes among both end-to-end nodes in the network, increasing efficiency, and the concept of Artificial Neural Network (ANN) combined with Genetic Algorithm (GA) is used to ensure security communication protocol. To create a secure and energy-efficient route between TX and RX nodes, calculate the Quality of Service (QoS) parameters to validate the proposed model, and if QoS is not acceptable, the concept of ANN with GA is used as an Artificial Intelligence (AI) technique to identify the routes fails nodes and prevent location data. At the end of the study, we compare the proposed ECC-based IRHM system to prior work in terms of Quality of Service (QoS), such as verification time, key size, and message size, and we find that the WBAN model reduces verification time.

Index Terms: *Improved Remotely Health Monitoring (IRHM) System, Wireless Body Area Network (WBAN), Location Privacy Mechanism, Elliptical Curve Cryptography (ECC), Genetic Algorithm (GA), Artificial Neural Network (ANN), Quality of Service (QoS)*

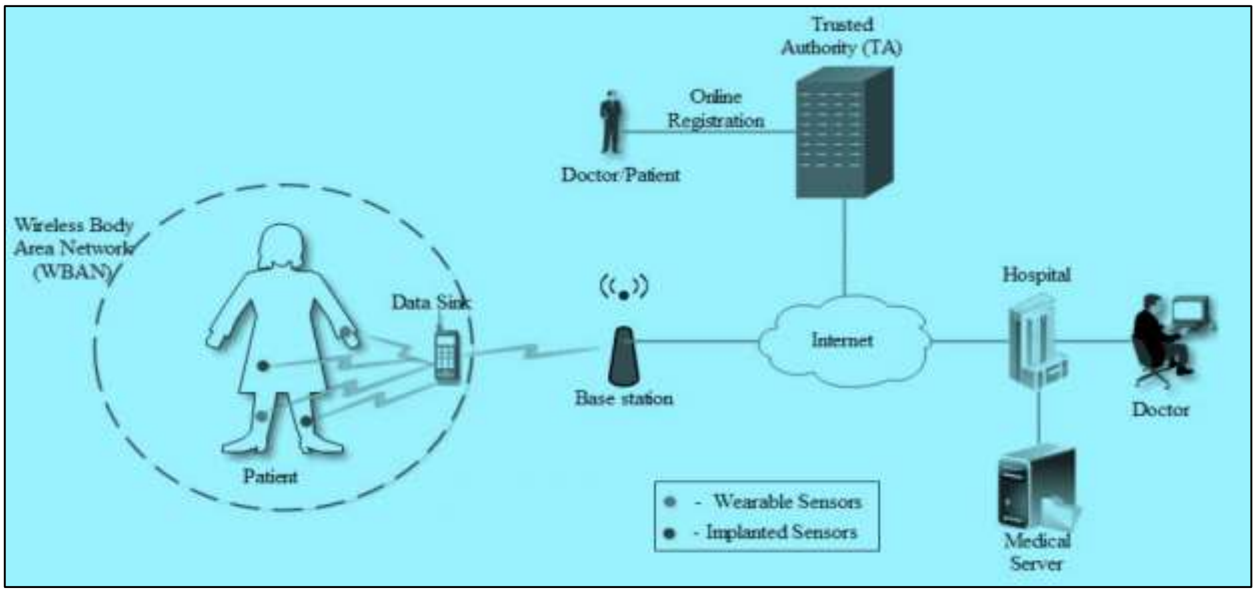
I. INTRODUCTION

The number of frail people living in their own homes, such as the physically challenged, senior citizens, and those suffering from chronic or other ailments such as diabetes, arthritis, asthma, cancer, and so on, has increased tremendously in the previous decade [1]. As a result of patients' experiences with such issues, a large study area has opened up as an interest in finding efficient and effective ways to assist patients through remote monitoring mechanisms in their homes [2]. Constant patient health monitoring has been found to lead to a 50 percent reduction in hospitalizations, a 73 percent reduction in emergency department visits, and a 51 percent reduction in patient costs [3]. Wireless communication has also provided several benefits to our society in a variety of areas, and it is a better alternative to use as a new approach in the Improved Remote Health Monitoring (IRHM) system based on the Location Privacy Mechanism for WBAN. Bluetooth, WI-FI, 4G, and LTE, among other advancements in wireless technology, have made this communication feasible [4]. In recent decades, the notion of Wireless Sensor Network (WSN) for device-to-device communication and monitoring of environmental conditions, healthcare systems, automobile industries, and telecom industries, among others, has been a popular topic of research [5]. The researcher's next goal was to communicate between robots and humans, and the notion of the IRHM system was an innovative move in that direction. Wireless Body Area Network (WBAN) [6] is a form of mechanism that allows a patient to be connected remotely with a doctor or other medical practitioners using low-power, lightweight, and small physiological sensors. The creation of the IRHM system is becoming routine care practices, but several problems remain, such as how to provide excellent patient care outside of the hospital environment and secure patient location in a cost-effective manner [7]. As a result, in an Internet of Things (IoT) environment, the deployment of a WBANs-based IRHM system may well take care of patients in a safe manner by encrypting their location utilizing the notion of encryption approach for location privacy [8]–[10].

WBAN technology allows medical practitioners or physicians to reply to patients from any distant place, with or without sharing their own location, in a safe and efficient manner. So that any form of unexpected emergency scenario may be avoided and the fatality rate can be kept under control [11]. Nowadays, WBAN-based health monitoring technology plays an important role in helping low-income families save money on medical costs by establishing an IRHM The proposed WBAN-based IRHM system is depicted in Figure 1 with sensor nodes deployed both within and on the patient's body. The fundamental objective for developing this model is to address existing model flaws such as insufficient security constraints, and we introduce a model that uses the notion of ECC as an encryption mechanism, with the following contributions:

- In the WBAN paradigm, we introduce the idea of location privacy by securing the patient and doctor locations using the ECC encryption technique.
- We utilized the concept of location privacy mechanism to create a reactive routing protocol in WBAN model with the combination of security by introducing an ECC technique.
- The concept of GA with ANN as an artificial intelligence technique is used in this research to detect the malicious or fail nodes during IoT-based communication.

To validate the proposed IRHM model, compare with existing state of the art using Quality of Service (QoS) parameters in terms of the Verification time, Encryption Time, Decryption system based on the Elliptical Curve Cryptography (ECC) idea for the WBAN model depicted in Fig. 1



- Time, Key Size and Message Size is performed. With the concept of database management to store the location coordination of the patient and doctor or medical practitioner.

The major goal of this study is to offer an ECC-based IRHM system that uses WBAN to provide safe and encrypted communication in the healthcare monitoring age. The rest of the study paper is arranged as follows: The survey of existing works is presented in Sect. 2. Sect. 3 covers the suggested IRHM model's technique and materials, while Sect. 4 presents the simulation results and analysis. Finally, in Sect 5, the conclusion is stated along with future tendencies.

II. RELATED WORK

Many research efforts have previously been done in this field, however due to the numerous challenges and demanding elements, we give a quick assessment of existing models. ***P Vijayakumar et al.*** published a study in 2019 on efficient and safe anonymous authentication for IoT-based WBANs with location privacy. They suggested a system for IoT-based WBANs that preserves location privacy utilizing the notion of efficient and secure anonymous authentication. The suggested technique solves the security flaws of current schemes while simultaneously providing cheap computing cost during anonymous authentication, according to the complete analysis part. In 2019, ***S. R. Chavva et al.*** published a study on developing an energy-efficient multi-hop routing protocol for WBAN-based health monitoring systems. The authors presented a combination scheduling and admission control challenge with the goal of improving a WBAN-based health monitoring system both within and outside the hospital. Using a multi-hop routing mechanism, a protocol in WBAN was designed to send body sensing data from multiple sensors to a sink or gateway node. The major goal of this study is to extend the average network life of a WBAN-based health monitoring system by lowering total network energy consumption during data transmission. They choose a parent sensor node depending on their leftover energy using a fuzzy logic method to increase the system's efficiency. The simulation results suggest that the proposed model is more efficient than existing state-of-the-art routing algorithms such as SIMPLE and M-ATTEMPT, but that it still needs to detect fail or malicious routes to lower the drop rate. In 2019, ***A. Sahoo et al.*** developed a model for WBAN based on the notion of priority-based data packet balancing in queue at IIT Kanpur. The authors' major goal is to regulate the emergency scenario in any WBAN-based healthcare monitoring system by forwarding the most essential packets first on demand and then giving precedence to non-critical packets transmission. The proposed protocol divides data packets into two queues based on their priority and threshold values. For the comparison of similar types of data packets, this unique routing protocol additionally considers the remaining time of crucial packets. The author also said that if there are no packets in both the High Threshold Emergency Queue (HTEQ) and the Low Threshold Emergency Queue (LTEQ), on-demand packets can be forwarded earlier (LTEQ). In terms of QoS measures such as throughput, packet delivery ratio, transmission latency, and energy usage, this study effort outperformed its peers. In 2020, ***O. Amjad et al.*** created a comprehensive energy efficiency optimization algorithm-based health monitoring system based on the WBAN idea. They employ a summed gamma distribution that underpins various patient circumstances throughout day-to-day living activities and can successfully demonstrate both static and dynamic workouts. By considering blackout possibility and package retransmission, the streamlining problem aims to improve every sensor transmit force and encoding rate in order to reduce the EE (measured in J/bits). 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.

We conclude several essential and major points based on the study of current research utilizing the idea of WBAN-based area of healthcare system, which helps to shorten existing work challenges.

- In this paper, we provide ECC-based location preserving routing algorithm that increase network security by retaining location of patients and doctors.
- Because network security and data transmission rate are important for health monitoring, an encryption solution would be a preferable choice for a WBAN-based IRHM system and here the concept of ANN and GA is used for this purpose.

So, in this paper, we offer an ECC-based IRHM system based on WBAN architecture that can be readily adapted to other tough problems such as routing and security, as well as enhance the model's verification time, resulting in improved transmission after studying existing works in the WBANs field.

III. METHOD & MATERIALS

The technique and algorithms utilized to create an ECC-based IRHM System with WBAN model are explained. EEG, ECG, EMG, BP, Pulse-Oximeter, Motion, Glucose, and Temperature are among the eight biomedical sensor nodes included in the proposed system. The data gathered by sensor nodes is collected by the sink node for further processing The functional simulation area of the proposed ECC, ANN and GA-based IRHM system is illustrated in Fig. 2, where total eight sensor nodes are deployed named as EEG: Electroencephalogram, ECG: Electrocardiograph, EMG: Electromyogram, BP: Blood Pressure, PO: Pulse-Oximeter, M: Motion, G: utilizing the suggested model and ECC. The following are the steps in the proposed ECC-based IRHM system's procedure:

A. IRHM Model: To begin, create a simulator for the proposed ECC-based IRHM system in MATLAB 2016a using the graphical user interface idea. The suggested IRHM system's area is calculated using the supplied geometrical area calculation formula:

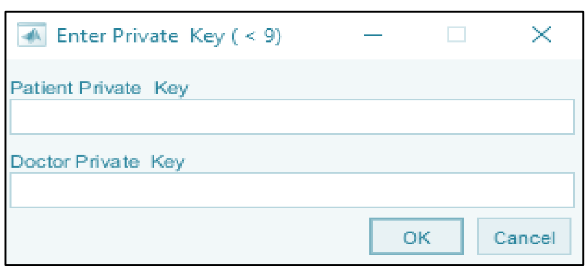
$$\boldsymbol{IRHM\ Area = Height(m)X\ Width(m)}\ \ldots\ldots\ \mathbf{(1)}$$

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

Glucose T: Temperature in the human or patient body on certain geometrical locations.

Route discovery mechanism in IRHM System: Following the simulator's construction, we determine if a secure path from the source (T_X-Patient) to the destination (R_X-Doctor) through gateways and base stations is determined based on the features of intermediate sensor nodes. In Fig. 2, the Biosensor Node-EEG is the Source (T_X-Patient), and the doctor's position is the Destination (R_X-Doctor). The secret key was utilized by the sink node to encrypt the location of the patients and biosensors using the ECC principle.

We use the ECC encryption technique to protect the location by supplying the patient and doctor private keys, and then we build a safe and energy-efficient path from the source (T_X-Patient) to the destination (R_X-Doctor) via a sink or base station node, as illustrated in Figure 3.



After that, discover the route from the source (T_X-Patient) to destination (R_X-Doctor) via gateways and Base Station (BS) whether secure route is decided based on intermediates sensor nodes properties using concept of WBAN with IoT. Biosensor Node is act as 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. Here, ECC encryption algorithm will be used to secure the location by providing the patient and doctor private key, after that, create a secure and energy efficient route from source (T_X-Patient) to destination (R_X-Doctor) via sink or base station node. Based on the above mentioned mechanism, create a secure and energy efficient route from T_X and R_X node and calculate the QoS parameters to validate the proposed IRHM model and if QoS is not acceptable then the concept of ANN with GA is used as an AI technique to identify the fails nodes in the route and prevent location data. Here, we used the Levenberg-Marquardt approach based neural network in MATLAB to train the model for the classification of any affected nodes in the network during data transmission. Basically, neural network is used as a classifier based on the network's nodes properties and if any node having no appropriate properties then we consider it as abnormal nodes (to be affected). Details of used neural networks are as follows:

Input Layer:	Node's Energy Consumption
Hidden Layer:	10
Output Layer:	Normal and Affected Nodes
Training Ratio:	70%
Validation Ratio:	15%
Testing Ratio:	15%
Epochs:	100
Evaluation:	MSE (Mean Square Error)
Data Selection:	Random

Based on the above mentioned parameters and data division ratio, we train the proposed IRHM system using the given algorithm:

Algorithm 1: GA for Optimization

Required Input:	FR ← Final Route from N_S to N_D
	N_{PROP} ← Mobile Sensor Nodes Properties
Obtained Output:	ON_{PROP} ← Optimized Mobile Sensor Nodes Properties

1. **Start Properties Optimization**
2. **To optimized the FR, GA Algorithm is used**
3. **Set up basic parameters of ABC:**
   Population of Population (P) – Number of Sensor Nodes

Final Route (FR) – Route from N_S to N_D

Fitness Function: $F(f) = \begin{cases} 1; & if\ N_{PROP} < Threshold_{PROP} \\ 0; & Otherwise \end{cases}$

In the fitness function, N_{PROP} : is properties of current sensor nodes which are in FR and $Threshold_{PROP}$ is the threshold properties of all communicating sensor nodes which is define on the basis of energy

1. Calculate Length of Route in terms of R Length
2. **Set, Optimized Nodes Properties, ON_{PROP} = []**
3. **For i in rang of R Length**
4. F_S = FR (i) = N_{PROP} // Selected Data
5. F_T = $Threshold_{PROP}$ // // Mean of Data
6. $F(f) = Fit\ Fun\ (F_S, F_T)$
7. ON_{PROP} = GA (F(f), FR (i))
8. **End – For**
9. **Returns:** ON_{PROP} as an Optimized Mobile Sensor Nodes Properties
10. **End – Function**

Algorithm 2: ANN for IRHM Model Training

Required Input:	FR ← Final Route from N_S to N_D
	ON_{PROP} ← Optimized Sensor Nodes Properties
	Cat ← Target/Category in terms of Normal and Abnormal Sensor Nodes
	N ← Carrier Neurons Number
Obtained Output:	OR and F ← Optimized and Validated Route from N_S to N_D with Fail Nodes

1. **Start Routing Optimization**
2. **To optimized the FR, ANN is used**

Index = Find index of N_{PROP} in FR
If index of route is normal then
    OR(i) = FR (index)
Else
    Mark as faulty route
End – If
Call and set the ANN using OR properties as training data (T), number of N_{SN} as group (G) and Neurons (N)
Set, MANET_Structure = NEWFF (T, Group, N)
MANET_Structure = TRAIN (MANET_Structure , T, G
Current Sensor Nodes, N_C = Properties of current node in MANET
Sensor Nodes Characteristics = SIM (MANET_Structure, N_C)
If Sensor Nodes Characteristics is valid then
    OR = Validated
Else
    OR = Need Correction or mark as Black Hole and Gray Hole Nodes
    If drop rate is maximum
        Marked as BHA
    Else if drop some and transmit some data packets
        Marked as GHA
    End – If
End – If
Returns: OR as an Optimized and Validated Route from N_S to N_D with Black Hole and Gray Hole Nodes
End – Function

B. Quality of Service (QoS): We determine the QoS various performance metrics of verification time after simulating the proposed ECC-based IRHM system and compare them to prior work using the 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 IRHM System	**1000m**
Width of IRHM System	**1500m**
Simulation Tool	**Communication** **Network** **Optimization** **Classification**
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, ANN and GA-based IRHM system is described in the below section of paper.

IV. RESULTS AND DISCUSSION

In this part, we explain the simulation findings of the proposed ECC-based IRHM system using the WBAN model and compare them to previous work by ***P Vijayakumar et al.*** in 2019 [12]. We describe the QoS parameters in terms of Verification time, Encryption Time, Decryption Time, Key

Size, and Message Size in the proposed ECC-based IRHM system from the perspective of wireless communication.

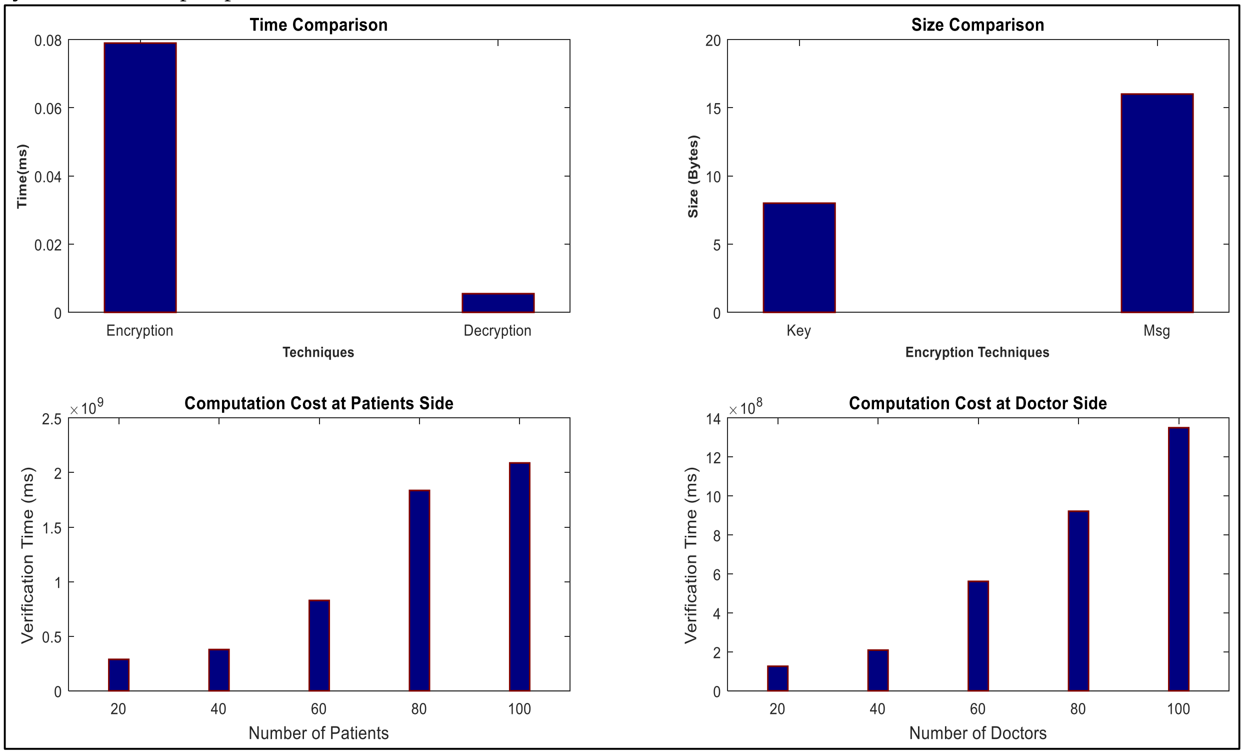


Fig 4: QoS Parameters of the ECC-based IRHM Model

According to the above figure, we observed that the throughput of proposed ECC-based IRHM 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.

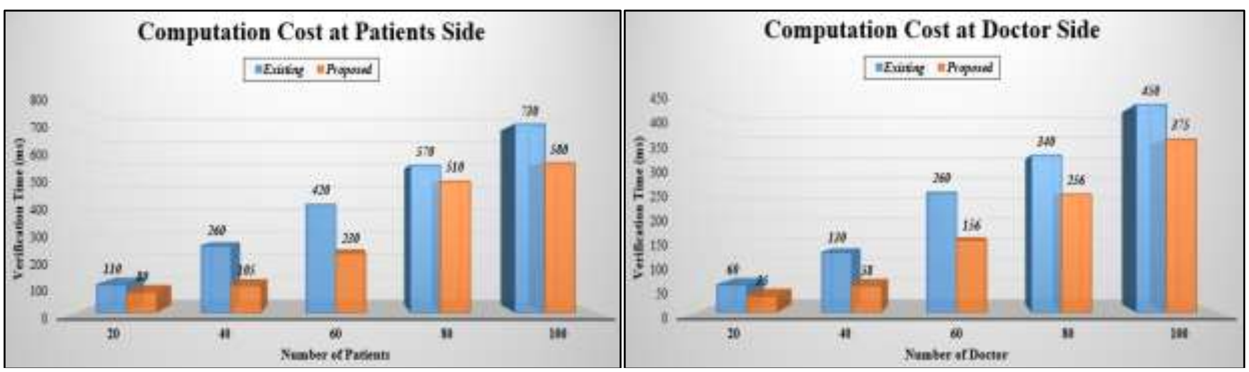


Fig 5: QoS Parameters Comparison of Verification Time

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 IRHM 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.

V. CONCLUSION AND FUTURE WORK

An IoT-based IRHM with a location privacy mechanism for the WBAN model is suggested in this study for safe communication. To encrypt or decode the patients' or doctor's location, we employed the ECC as an encryption mechanism. We know that the ECC-based IRHM system is a new field of research in the world of healthcare, but secure communication is a major worry that is addressed in this study by combining the notion of encryption with a routing technique improvement. The major goal of this study is to reduce verification time by using a secure and fast data transfer method in the WBAN paradigm, which will benefit both patients and physicians. For the network security purpose, the concept of ANN along with the GA is used to find out the fail node during the simulation. In terms of verification time, the proposed IRHM system outperforms previous work, and we also compute the size of the key and the size of the message. By encrypting the location of patients, data transmission becomes more secure, and the impact of attackers is reduced in the WBAN, but the data transmission rate must be sped up using the energy minimization principle. As a result, in the future, the notion of optimal deep learning will be used as a classifier to construct an ECC-based IRHM system in the WBAN model to handle privacy and reliability concerns in medical data using a natural computing-based Meta heuristic algorithm.

VI. 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.
[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.