Journal of Integrated
SCIENCE & TECHNOLOGY

Healthcare monitoring system with blockchain technology encompassing energy harvesting and delays in a Wideband Network

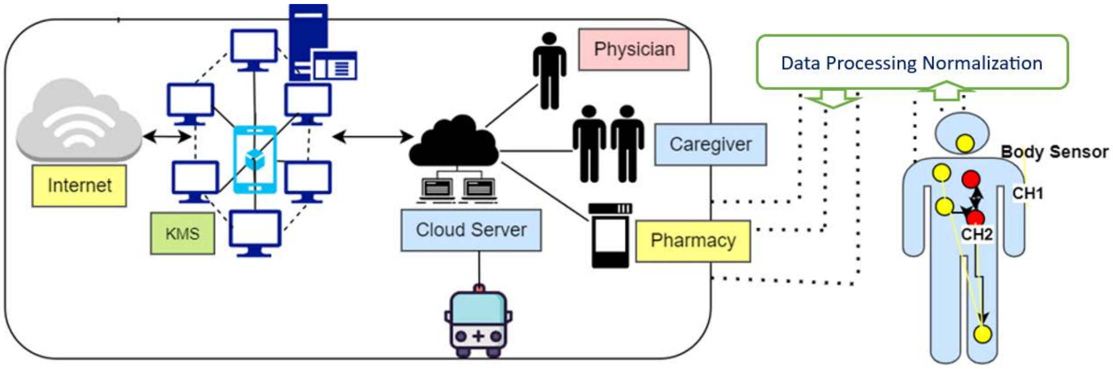
Puneeta Singh,* Shrddha Sagar

School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh. India.

Received on: 12-Nov-2023, Accepted and Published on: 16-Jan-2024

Article

ABSTRACT



The study of WBANs enables people to be monitored for their healthcare. WBAN connects to the Internet of Things to create a logistic, remote healthcare monitoring system that allows for the diagnosis of a variety of medical conditions. The three main problems in the WBAN IoT environment are the attributes of service, privacy, and efficient energy. Existing solutions for these three problems fall short because nodes are resource-constrained, which causes latency and reduces energy use. This study introduces the B-DEAH system in the WBAN-IoT setting. Dual sinks are used with body and environment sensors for periodic and emergency packet transfer. This study involves several procedures, and each process is detailed as follows: It is suggested to register keys for patients using an expanded form of the PRESENT method. Using the spotted hyena optimizer, cluster nucleation, and central node selection are carried out. The MOORA algorithm is then used to build cluster-based routing. The elliptic curve cryptography used as an algorithm is used to deploy and authenticate the patient block agent (PBA) for data transmission. Classifier, queue manager, channel selector, and security manager are the three entities employed in PBA. A unique function controls each entity, and packets are divided into three categories via two ways deep reinforcement learning (TS-DRL): emergency, non-emergency, and incorrect data. Each packet is placed in a different queue, known as the emergency, periodic, and faulty queue. Reyni entropy is employed to manage each queue. Utilize a vector optimization-based channel selection technique, periodic fragments are delivered by a different channel without any interference.

Keywords: WBAN, Blockchain, delay, transaction, IoT

INTRODUCTION

A sensor network that helps with creative patient healthcare monitoring is a medical body area network (MBAN). is another name for WBANs. Recent years have seen many studies in area network to monitor the patients.[1–3] The QoS for a patient is not met by the present wide band area network (WBAN).[4] In WBANs, QoS provisioning is a crucial factor that is accomplished by overcoming difficulties: energy efficiency, mobility prediction (adaptiveness), and security.[5] In WBAN communications are divided into many communications layers: Inter, Intra, and beyond wireless body area network.[6,7] With the help of IoT and WBAN combination easy to monitor the patient data.[8] IoT sensors are to be used efficiently because of the nature of their resources limited, however, difficult to solve this issue. Difficult to sink the communication between the sensor node and the sink node. Critical packets are discarded leading to regular loss packets.[9] The issue of energy usage can be addressed in part via clustering. Those nodes deployed in the human body or a sink node, can both function as the cluster head (CH) in this method. Medical data packets are sent back and forth via the CH. For this method to work, a quick and efficient CH

*Corresponding Author: Puneeta Singh
Email: puneeta12cs37@gmail.com

Cite as: *J. Integr. Sci. Technol., 2024, 12(4), 794.*
URN:NBN:sciencein.jist.2024.v12.794

election is needed to aggregate and transfer the packets. Security is the main difficulty in WBAN, much as energy efficiency, because nodes interact via a public channel, which makes it vulnerable. Blockchain has promise as a way to give WBAN suitable security. To prevent a single point of failure, it functions as a decentralized entity. However, in a resource-constrained context, the typical blockchain design is unable to guarantee data secrecy.

In the networking arena, blockchain technology is a distributed ledger in which any participant can own a ledger. Another name for this technique is a peer-to-peer system, in which all users work together to administer the network. The following benefits of blockchain technology include chroming, scalable, unity, and traceability.[10,11] Four different forms of blockchain exist:

Public blockchain: Every user able to write and read, there is no centralized authority, and it has high trust, but it also uses a lot of energy.

Private blockchain: Only the specific company that owns the blockchain may be able to access or make changes. It is a less trustworthy centralized blockchain. The energy usage is lower when the throughput is high.

Blockchain consortium: It can be held by a collection of organizations, and all of the group's members could have read and write access to it. It is also known as a partially centralized blockchain and has a high throughput while using less energy.

Hybrid blockchain: Like a public blockchain, a hybrid blockchain might grant all members read and write access. It offers a small degree of centrality and medium credibility.

Medical records are secured from unauthorized access and cannot be changed to the assistance of blockchain-based security technologies. Because security risks could limit energy efficiency, the proposed study also uses blockchain technology for secure data management and storage.

Review of Related Literature

Villarreal E.R.D et.al.[1] contended that by dividing the quantity of blocks produced by blockchain technology, they may reduce the amount of human labour while simultaneously safeguarding IOT smart sensors from hackers and providing transparency. Many security issues exist, including fabrication attacks and delays in authentication.

Singh, P., et al.[2] suggested using blockchain technology in conjunction with the CIA (Confidentiality, Integrity, and Availability) formulae to address the security issue. It might take the place of the existing IOT system. They may have to deal with matters of confidentiality and honesty.

Araujo-Inastrilla, et.al.[3] reported the suggestions that 5G technology can be deployed through NFV, control and administrative features, and integration with Internet of Things devices. They examined several blockchain-related issues, including standardization and regulation. Blockchain technology and artificial intelligence (AI) can help tackle these issues.

According to Lakhan, A., et.al.[12], it is possible to use IOT devices and blockchain technology with the concept of a consensus mechanism. A shared key can be used by the blockchain and its IOT sensors to create hash-based authentication codes and create block nodes using a random function. The block node is the election's victor, also referred to as the offline quick election node. AI approaches are also added to remove sensor outliers before block nodes are upgraded for the blockchain process.

Ahmad, S., et.al.[13] proposed that Internet of Things sensors establish connections with each other and exchange data with every node. The author acknowledges that there is a major issue with centralized infrastructure that may be fixed by utilizing decentralized methods.

Sun, M., et.al.[5] The three primary issues with the Internet of Things (IoT) are security, reliability, and transparency. with the help of decentralization, the key component of blockchain technology. The consensus process is the most important feature of all nodes, which are networked and make use of smart contracts, data encryption, decryption, proof of work, and proof of ownership properties of stake.

Tareen, F. N., et.al.[6] proposed that all patient data be recorded via the Internet of Things (IoT). This study gave more consideration to security and patient privacy when collecting data using patient data. Maintaining data integrity is difficult.

The distributed nature of blockchain technology and its different applications, such as consortium, public, and private blockchains, are covered by Singh, P.[14] The authors also provided a comprehensive explanation of blockchain, including authentication, privacy, and secret data.

Pathak, R., et.al.[15] suggested the efficient and speedy transportation of commodities is made possible by intelligent logistics. Lead times have been greatly reduced and logistics management has become simpler thanks to new technology and the Internet of Things. It uses less personnel, cars, paperwork, and other resources while relying more on digital technology. But it might also lead to privacy invasion and data theft problems. Nonetheless, the digital logistics system's security will be enhanced by the combination of blockchain technology with IoT.

Despite the IOT security threats, Elgamal, E., et.al.[16] suggested that the problem can be solved by using the secure communication platform that blockchain technology offers. Smart contracts will be used in blockchain technology for security reasons.

The functioning of the healthcare industry and its impact on information technology were explained by David S.[17] impacts personal data security and privacy. Their efficacy, robustness, and transparency are increased by this technology.

Table 1: Research Gap

Regional Focus	Study Deficit
QoS Accomplishment	• Some of the published studies have achieved direct data transfers to the sink nodes without taking clustering into account, which has an impact on the quality of service in terms of excessive latency. • Although clustering is performed in many of the published articles, the gateway's inefficient handling of the clustered data in terms of intermission and postponement also negatively impacts the quality of service. • The extant research's routing protocols are constrained, have lower communication

	dependability, and experience transmission mistakes that also have an impact on QoS.
Security Deployment	• Certain current efforts do not take authentication into account; instead, they focus on data security, which has an impact on patient privacy. • For data encryption and authentication, many cutting-edge works use complex cryptographic methods, which increases energy consumption in WBAN-IoT networks. • The WBAN-IoT environment is vulnerable to significant assaults like impersonation and fake injection attacks because of some of the current work's limitations in taking into account the bare minimum of security metrics for ensuring security.
Blockchain	• High energy consumption, latency, and scalability problems about block production and validation time characterize conventional blockchain models. These issues with traditional blockchains are inappropriate for WBAN-IoT, which has limited resources.

Problem Statement

- Since the CF computation can be time-consuming when many sensors are utilized, and it does not guarantee that the optimum solution is always produced, the clustering process is ineffective. While the amount of duplicated data is reduced in this work, anomalous (faulty) data is still there. For CHs, this means high bandwidth and energy usage.
- Interference occurs when two sensors engage in simultaneous communication over the same channel. Delivery rate decreases and energy consumption rises when multi-hop transmission occurs via suboptimal nodes.

Methodology/ system model

For QoS provisioning in the IoT-WBAN environment, we address the security and energy efficiency concerns in this study. Thus, we created a medical data transfer framework in an Internet of Things-based WBAN that is cognizant of energy and delays.

4.1. System Model

Figure 1 shows the overall architecture of the system. This study designs three layers: layer 1 is for intra-WBAN communications, layer 2 is for inter-WBAN communications, and layer 3 is for beyond-WBAN communications. Our suggested work includes things like

Body sensors: The body sensors (Bs = Bs1, Bs2, Bsn) are implanted in patients' bodies to track several health parameters, including heart rate, blood pressure, and other parameters.[18]

Environmental sensors: Depending on the patient's health, the environmental sensors (Es = Es1, Es2, Esn) are positioned throughout the environment to track changes in the surrounding conditions. These sensors keep an eye on the surrounding conditions for patients, including humidity and air quality.

Patient block agent (PBA): The PBA oversees data transmission and gives users a sense of legitimacy. It works with three modules: the classifier and queue manager, the security manager, and the channel selector, which categorize and secure the data.

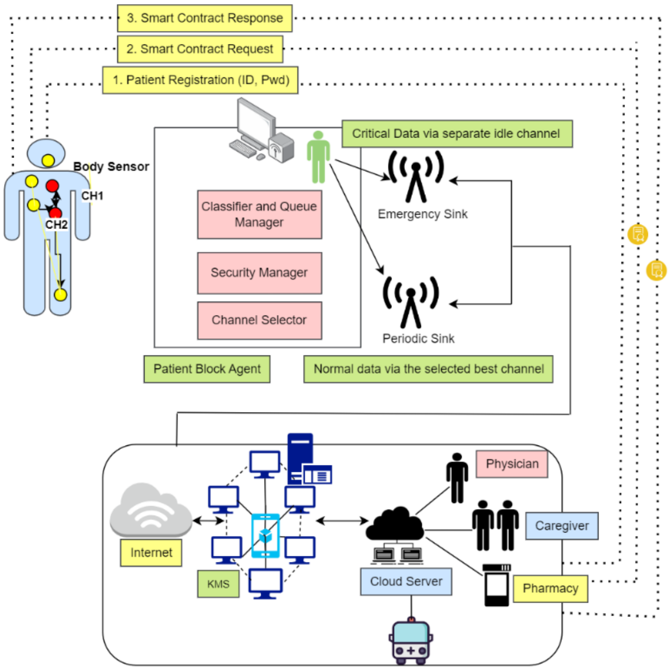

3. Smart Contract Response
2. Smart Contract Request
1. Patient Registration (ID, Pwd)
Critical Data via separate idle channel
Body Sensor
CH1
CH2
Classifier and Queue Manager
Security Manager
Channel Selector
Emergency Sink
Periodic Sink
Patient Block Agent
Normal data via the selected best channel
Physician
Internet
KMS
Cloud Server
Caregiver
Pharmacy

Figure 1: System Architecture

Periodic sink and emergency sink: These sinks oversee keeping the data on the cloud server and internet. To transfer health information with minimal delay and congestion, the emergency sink (SE) is used to share vital data from the PBA and the periodic sink (SP) is used to communicate regular data from the PBA.

Blockchain (key management server, or KMS): the WBAN IoT networks' security and privacy are ensured by blockchain. In the blockchain, the KMS.

4.2. Distribution of Keys

It is assumed that patients migrate dynamically between locations. We create a safe, energy-efficient, and delay-aware healthcare monitoring system for WBANs in this instance. By using their ID, PWD, location, and biometric data, we were able to register every patient with the KMS. Patient Pi must provide the KMS with {ID, PW}. The related patient's ID and PWD are first confirmed by the KMS. The KMS then confirms the patient's current location and biometric records if ID and Pwd are accurate. Lastly, for patients who have registered, SK is generated. The formula for this step is as follows:

$$\begin{array}{c} U_i \rightarrow \{ID \oplus PW\} \rightarrow KMS \\ KMS \rightarrow \{SK(P), \text{ if } (ID\&\&PW\&\&BR\&\&L == \text{True})\} \end{array} \qquad (1)$$

The secret key (SK) is created, sent to the patient, and kept in the PBA if the patient's registration is successful. We validate these entities for authentication. Data transmission is used for authorized patients, and data access is permitted for patients who possess the hidden key. The figure depicts the flow of security provisioning.

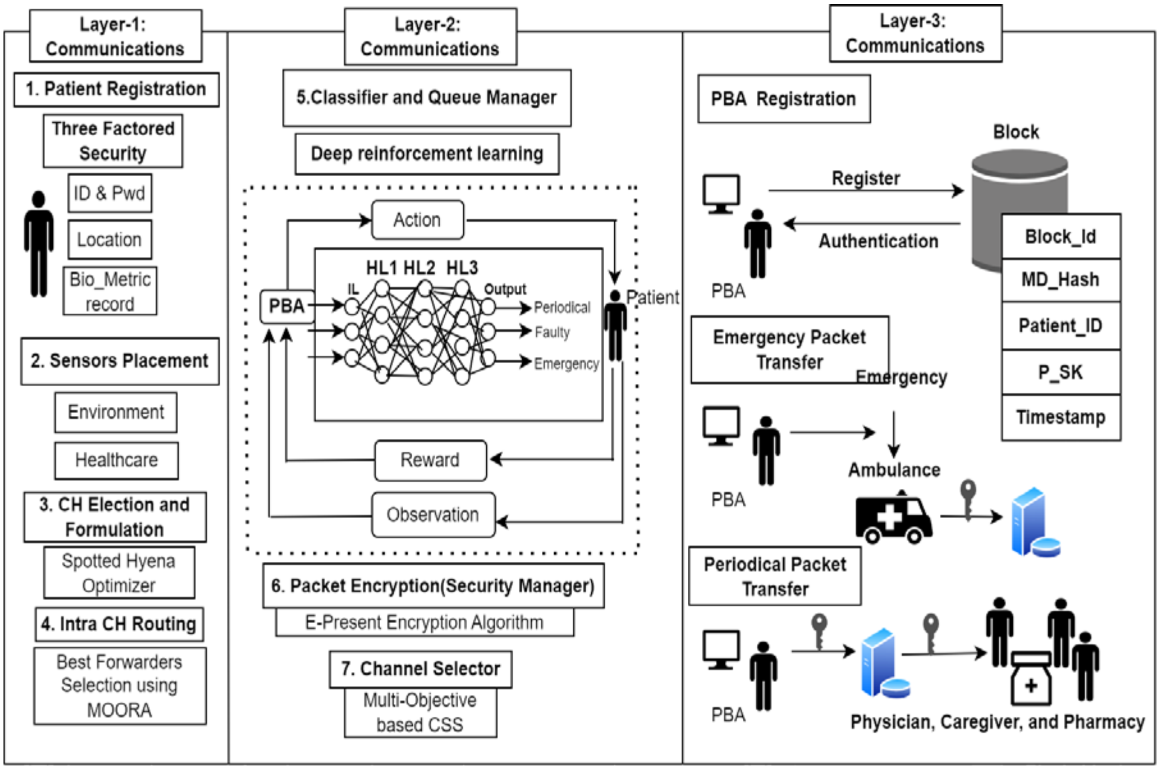


Figure 2: System Architecture

4.3. Routing Based on Clusters

From the sensors positioned within the patient, we create clusters. The quantity of IoT devices deployed for patient monitoring is shown in Table 2.

Table 2: Patient medical records.

Factors in Data Collection	ICT Equipment	Specifications	Type of Sensing Event
Body sensor-related information	Accelerometers, gyroscopes, pressure sensors, light sensors, proximity, motion, flow, gas, sound, image, magnetic, and cameras.	Blood Pressure, Temperature, ECG, Respiration rate	Anxiety, high blood glucose level, high heart rate
Data pertaining to the environment	Humidity, moisture, temperature, and chemical detectors	Noise Level, Air quality, Temperature	High noise level, high light intensity

The best objective function (BOF), which is determined by node residual energy, transmission power, bandwidth, and SNR using the spotted hyena optimizer (SHO), is computed to implement the cluster head [50]. The data traffic type field, which displays the five distinct packets, is introduced to the MAC protocol. An emergency packet detected by the sensor will be forwarded straight to the CH. The best path is chosen for the remaining four packets. We suggest multi-hop data routing with optimum forwarder selection, taking into account the distance to the CH, RSS, node residual energy, and path duration. The four stages of the SHO algorithm—searching, encircling, hunting, and attacking prey—are used to identify the best CHs. The ideal CHs are established by appropriately balancing exploration and exploitation. The fitness values among sensors are higher when the spotted hyena cooperates better.

The following parameters are used to calculate the fitness:

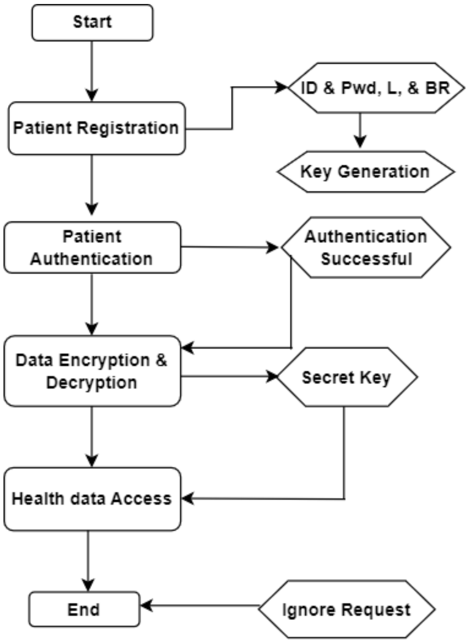


Figure 3: Security evaluation for WBAN

Residual Energy Level: This value indicates how much energy the node has left. The difference between the starting energy level and the total energy used after one cycle is used to calculate it. Higher residual energy nodes become CHs, and as a result, the CH is in charge of gathering and aggregating data.

Distance: This metric is widely recognized as the separation between a single body sensor and a neighbouring sensor. When it comes to the CH election, a node closer to the center is eligible. This is how it is computed:

$$D_s = \sqrt{(x_i - x_j)^2 + (y_i y_j)^2} \qquad (2)$$

Path Duration: This option indicates how long it takes to transmit a packet. Many relay nodes connected to a single node are used to measure it.

The section that follows provides an explanation of RSS calculations. As the CH, a node with greater residual energy, shorter path length, less distance travelled, and higher RSS is chosen. The values of the remaining nodes determine how they are connected. We used multiobjective optimisation based on ratio analysis (MOORA) to choose the route. It is an algorithm for making decisions that chooses one or more options from a group of nodes that are accessible. Creating the decision matrix (DM) for the given problem is the first step in the MOORA method. The M × N matrix contains the objectives and alternatives, and the input parameters and alternatives affect the performance of DM. It is said as follows:

$$X = DM(i,j)_{M\times N} = \begin{bmatrix} x_{11} & x_{12} & x_{1n} \\ x_{21} & x_{22} & x_{2n} \\ x_{m1} & x_{m2} & x_{mn} \end{bmatrix}` \qquad (3)$$

The alternative rows and columns are denoted by M and N, respectively, and the performance value of the ith alternative on the jth criterion is represented by xij. Next, the alternative performance value is derived using the following formulas to compare it to the other criteria:

$$x^*_{ij} = \frac{P_{ij}}{\sqrt{\sum_{k=1}^{m} P_{kj}^2}} \qquad (4)$$

where xij generates the normalized performance for each input criterion and is a range between 0 and 1.

Nonbeneficial criteria are used to calculate the normalized values for the criteria. The favourable criteria are deducted from the total of the nonbeneficial criteria. The alternative's overall score value is the outcome. The MOORA algorithm terminates when it reaches the optimal set of options. The special feature of the MOORA algorithm is to determine the best alternative by multiple objectives. Alternative values are arranged in ascending order, and the best node is selected based on the alternative value. In previous works, the sensor node sends sensed information through single-hop communication. However, this type of communication is not available at all times, whereas some existing works have used multihop communication in which next forwarder selection was not optimal. Hence, packet losses are very high. Furthermore, this can be applied when a large number of sensors are placed over the body. Our proposed routing protocol computes the weight value for the best forwarder selection.

4.4. Contention Window Size Adjustment

To further minimize the end-to-end delay and energy consumption for transmitting emergency packets, we also modify the contention window size (CWS) based on three QoS factors: residual energy, RSSI, and distance. Table 3 displays the data traffic specification.

4.5. Blocker for Patients

PBA is essential to this research. It serves as a coordinator and has four-Q-curve algorithm authentication to the blockchain. The performance of this asymmetric cryptography algorithm is better than that of the ECC. After compiling data from the CHs, it is transmitted to the following organizations:

4.5.1. Queue manager and classifier

In this entity, a two-stream deep neural network (TS-DNN) in deep reinforcement learning is used to classify aggregated data into three classes: emergency, periodic, and erroneous data. From the many available Sensors 2022, 22, 5763 12 of 29 inputs, including packet size Ps, data traffic type DTt, time to live TTL, health parameter, and QoS constraint (delay, data rate, and bandwidth) QoSCS, TS-DNN identifies the classes. Environmental sensor data is forwarded in the second stream of DNN, whereas body sensor data is forwarded in the first. Environmental data and BAN-sensed data are considered for classification in this architecture. Three different types of layers make up each DNN: input, hidden, and output layers. Figure 3 shows the flow and operation of the queue manager and classifier. The following is an illustration of how each layer in DNN (1) and DNN (2) operates. Algorithm 1 explains the TS-DNN.

The **input layer** is where the input neurons are first processed. Environment events and BAN packets are sent to the input layers of DNN (1) and DNN (2), respectively. As a result, the following is a representation of the observed packets from the body and environment sensors:

$$bo(s(i)) =\{bo(s)_1, bo(s)_2,\ldots,bo(s)_n\} \qquad (5)$$

$$ev(s(i)) =\{ev(s)_1, ev(s)_2,\ldots,ev(s)_n\} \qquad (6)$$

Hidden Layers: Various computation weight values are applied to each sensed packet input parameter. The number of hidden layers is defined based on the intended outcome and the input requirements. The hidden layers of the previously listed parameters are used to compute the fitness value. Lastly, the following is the expression for the fitness function F(f):

$$F(f) = \left(\sum_{S=1}^{n} \frac{\tau_x + \mu_x + \alpha_x}{\Gamma_x(C_1, C_2, C_3)} \right) \qquad (7)$$

where S stands for the sensor nodes of n numbers (i.e., {S = 1, 2,..., n}), τx stands for the packet size weight value, μx for the weight value of distinct traffic types, αx for the TTL weight value, Γx for the weight value for QoS restrictions, and C1, C2, and C3 for the bandwidth, latency, and data rate.

The **output layer** makes predictions about the classes based on the previously given parameters. It computes fitness values for every packet and selects the best class among them.

In terms of math, it is expressed as follows:

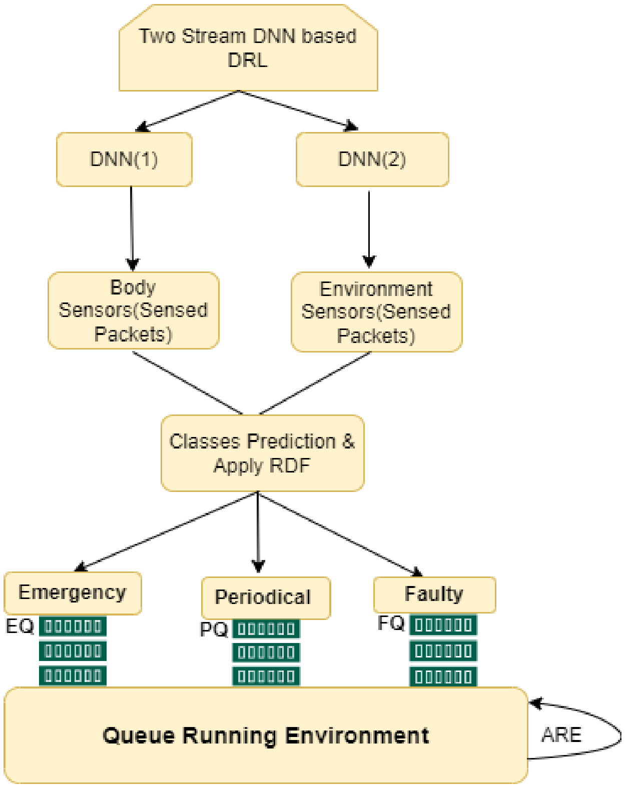

Two Stream DNN based DRL
DNN(1)
DNN(2)
Body Sensors(Sensed Packets)
Environment Sensors(Sensed Packets)
Classes Prediction & Apply RDF
Emergency
Periodical
Faulty
EQ
PQ
FQ
Queue Running Environment
ARE

Figure 4: TS-DNN Environment

Algorithm 1

```
Inp: $bo(s(i)) = \{bo(s)_1, bo(s)_2, …., bo(s)_n\}$
$ev(s(i)) = \{ev(s)_1, ev(s)_2, …., ev(s)_n\}$
Output: Three Classes
Beg
// DRL-based TS-DNN algorithm
For Q(S,a), initialise all bo((s(i)) and ev(s(i)).
Continue (For every episode)
Pick a from S using the policy that comes from Q
Input Layer
For all $BAN_i$ do
    Take action a and observe r and s
    Q(S, a) to Q(S, a) + $\tau$[r + $\gamma$Max a, Q(S}'}, a'}}) to Q(s, a)]
End for
in the case of Si ∈ S, do
    Discover ⟵ $\tau, \Gamma, \mu, \zeta$
    Determine F(fi)
    Set the weight function f to F(fi).
conclude for
Gather all of the neurons' F(fi)
Calculate O
Revert(classes)
Finish
```

Using training set values as a guide, we categorize the defect data. We calculate the relative difference factor (RDF) for the packet that is now being transmitted, which displays the inaccurate sensor data. To calculate the notation RDF,

$$S(sr(c),(p)) = \frac{Sr(c*p)}{|c|\times|p|} = \sum_{i=1}^{n} \frac{i(c*p)}{\sqrt{\sum_{i=1}^{n} C_i^2} * \sqrt{\sum_{i=1}^{n} P_i^2}} \quad (8)$$

where the sensor readings for the previous and current packets are indicated by Sr(c ∗ p). Following classification, each packet type is placed in a different queue, which is then arranged by the queue manager to almost completely fill three queues: the emergency queue (EQ), the periodical queue (PQ), and the faulty queue (FQ). The alarm message is sent to the specific sensor via PBA using the FQ packets to locate the RDF. We proposed Reyni entropy Re, which processes all packets and converts the processing of one queue into another queue by computing the input parameters, in order to process all medical packets without experiencing any packet dropouts. Re is the order of δ, and its definitions are δ >= 0 and δ 6= 1.

$$H_\alpha(x) = \frac{1}{1-\alpha}\log\left(\sum_{i=1}^{N} P_i^\alpha\right) \quad \textbf{(9)}$$

where x is a discrete random variable, and for every i,.. n, the corresponding probability are pi = 1 n. The potential results for x are 1, 2,.. n. At that point, the distribution's Renyi entropies are all equal: Hα(x) = logn, where P α i denotes the current values of the input parameters, and α is the weight value, which is a number between 0 and 1. Ultimately, the packets are sent to the ambulance, carer, pharmacist, and physician so they can take additional action.

The E-HARP was then used to calculate the optimal cost function (CF). The distance between nodes, transmission power needed, link SNR, total energy gathered, and residual were all used to calculate the ideal cost function. When the LOS and high RSSI value are met, two sink nodes—which also serve as CHs—are deployed. Still, there is usually more energy usae because a patient's important packets must wait longer.

Large-scale surroundings are not suited for it. Body sensors produce large-sized erroneous packets that take more energy to sense, thus it is necessary to sense the environment.

Results

The performance of the suggested B-DEAH architecture is demonstrated in this section. The three components that make up this section are the simulation environment, the comparison analysis, and the security and efficiency analysis of the suggested B-DEAH architecture from the works that are now in existence.

5.1. Context of Simulation

The OMNeT++ simulator is used to build the suggested B-DEAH model, and it is appropriate for body area networks. This tool supports the programming language C++.

Moreover, WBAN makes use of the unique network module MiXiM and is modelled using the network description language (NED). Battery, channels, packets, messages, mobility, mac, PHY, network models, application layers, and several WBAN examples are among the helpful built-in modules it offers.[19] The establishment of data transmission from the source to the destination is the function of the physical WBAN environment. Five WBANs are examined in this article, and each has unique qualities that are as follows:

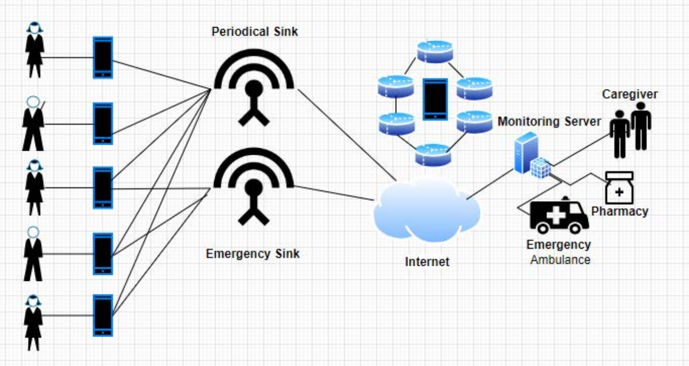


Figure 5: Network Topology

In Figure 5, the simulation environment is depicted. The suggested B-DEAH model's simulation configuration is shown in the following table. Additionally, Table 4 thoroughly explains body sensors for a single BAN configuration.

5.2. Evaluation via Comparison

The specifics of the simulation results are covered in detail in this section. The three earlier studies, CF-EHARP, PCA, and E-HARP, are contrasted with the suggested B-DEAH.

Network throughput, end-to-end latency, packet loss rate, authentication time, residual energy, and success rate are the primary sets of metrics that are compared. Additionally, the work's efficiency is contrasted with earlier efforts regarding dependability (%) and defect data removal check (%).

5.2.1Throughput of Networks

Its definition is the total amount of data that is successfully transferred to the target node. On the other hand, increased throughput indicates improved performance. It is a crucial QoS metric that illustrates the network's quality of data transmission. As a result, in WBAN, optimising QoS performance is crucial. In terms of math, the calculation is as follows:

Network Throughput= P(s)/T(t) (10)

T(t) is the transmission time for a single packet, and e P(s) is the size of the delivered packet. The throughput analysis for emergency and non-emergency packets is shown in Figures 8 and 9, respectively.

5.3. Residual Energy

It is a key WBAN parameter that assesses the system's energy efficiency. For every sensor, the initial energy distribution is the same. To perceive WBAN communication, controlling the remaining energy of body sensors is the primary challenge. The amount of residual energy can be adjusted based on the processing time, packet size, and number of rounds. Moreover, residual energy values vary depending on coverage and connectivity to nearby sensors. The model's energy efficiency is demonstrated by the lower residual energy usage for each processing step, including sensing, transmission, and reception. Below is a mathematical expression for residual energy.

$$R_E(i) = \frac{(E_{\text{node}} \times E_{\text{init}})}{100} \qquad (11)$$

where Einit is the starting energy level and Enode is the node's residual energy consumption rate. Nonetheless, the relationship between the transmission energy and the distance between the source and the destination is straight. The energy that a sensor has left over after sending one packet is known as its residual energy. Remaining energy progressively drops as the number of rounds increases. For both emergency and non-emergency packets, residual energy is compared with the two parameters, simulation rounds and simulation time. At fifty rounds, previous works are decreased to the lowest level of leftover energy. Creating a lightweight framework improves quality of service (QoS). This is accomplished through three different mechanisms: blockchain technology security, RDF fault data elimination, and the proposed B-DEAH method's two sink deployment for emergency and non-emergency packet transmission. By increasing residual energy, these mechanisms also improve energy efficiency. The remaining energy is shown in terms of simulation rounds for emergency and periodic packets in Figures 6 and 7.

The remaining energy is shown in Figures 8 and 9 for both emergency and periodic packet simulation timeframes.

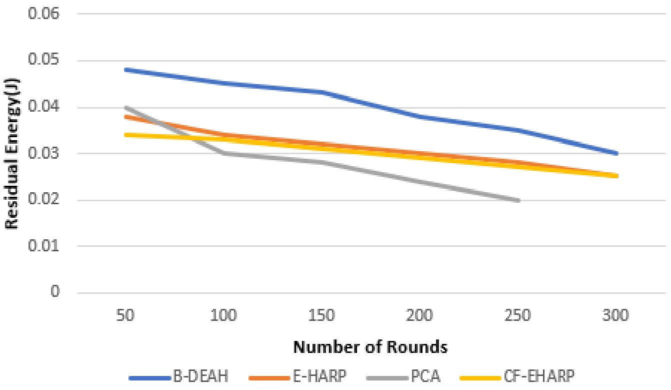


Figure 6: Residual energy vs. simulation rounds (emergency packets)

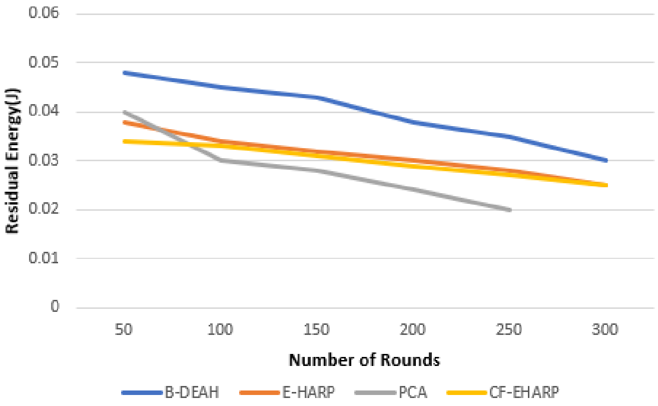


Figure 7: Residual energy vs. simulation rounds (periodic packets)

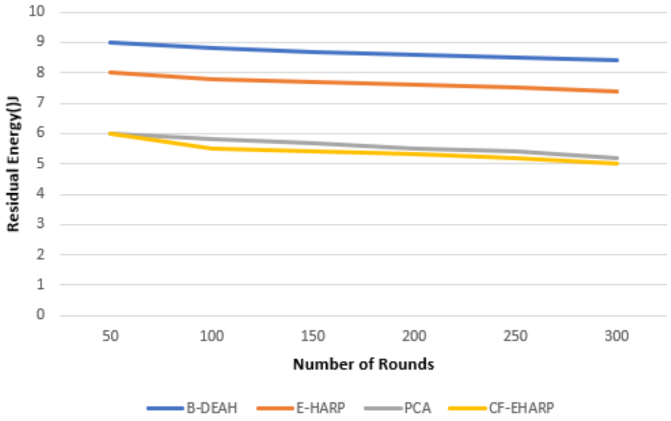


Figure 8: Residual energy vs. simulation time(s) (emergency packets)

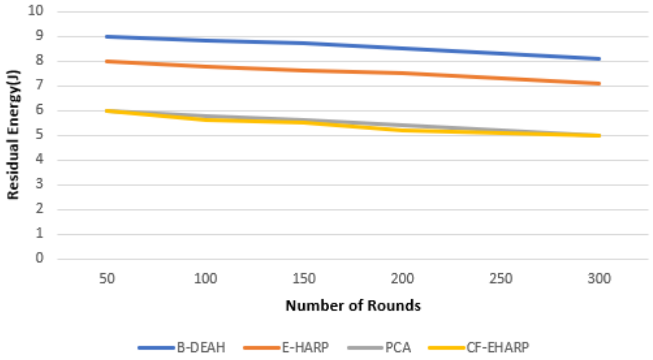


Figure 9: Residual energy vs. simulation time(s) (periodic packets)

5.4. Success Rate

The success rate of data transmission over time is represented by this metric. Fewer packets successfully reach their destination and packet transmission is altered because of collision and rogue node activity. In this work, we calculate the success rate performance for both the existing works and the suggested B-DEAH. The success rate fluctuates frequently because of BAN movement. descend to a lower tier. Any type of network must have adequate network architecture to overcome this problem.[20] A successful broadcast exhibits no channel interference, no collisions, and no attackers. The success rate can be calculated mathematically in the following way.

$$\text{SucessRate} = \frac{\#\text{ of sent packets}}{\#\text{ of received packets}} \quad (12)$$

Therefore, the packet transmission success rate is computed using the total number of packets sent and the total number of packets received successfully. Figures 8 and 9 represent the success rate of the proposed B-DEAH model concerning the simulation time for the previous works. Comparing the suggested B-DEAH to CF-EHARP, PCA, and E-HARP, it is 40% superior. The residual energy of each sensor and relay sensor is considered for multi-hop-based routing for each communication. The average behavior of the proposed work demonstrates that it does not require larger residual energy and gives the stochastic nature of increased residual energy availability. larger residual energy yields a longer network lifetime.

Conclusion

To overcome the current problems, this study effort suggests a new patient remote healthcare monitoring system. For three different kinds of communications—intra-, inter-, and beyond-WBAN—the proposed B-DEAH model is made. In an IoT-based WBAN system, blockchain is implemented for decentralised communication and security. For patient registration, a three-factored security technique is suggested, and security credentials are sent to KMS. Clustering is started to reduce energy use and facilitate data transmission. For clustering, the Spotted Hyena Optimizer is employed, which determines the optimal CH based on the prey's fitness and modifies position as necessary. The MOORA algorithm is then used to implement intracluster routing. It prevents packet losses and delays and enhances packet success rate performance. Three operations are employed in PBA: four-Q-curve for PBA authentication and packet encryption using the PRESENT algorithm; multi-objective-based channel selection algorithm; and classification and queue management, security provisioning and channel selection using TS-DNN in DRL. After that, packets are sent, based on priority, to the periodic and emergency sinks. Several performance measures, including QoS, energy efficiency, and security, are simulated. The results indicate that the suggested B-DEAH performs better than earlier efforts. We plan to concentrate on the following areas in the future. Mobility research is necessary because it's a key BAN parameter. Every aspect of the human body is continually moving. Here, we intended to manage mobility through handover techniques. The study of duty cycling MAC scheduling is done to control the energy state of every sensor. Moreover, user physiological parameter analysis is the focus of other newly developed medical diagnosis applications, such include COVID-19, diabetes, asthma, and Parkinson's disease.

Conflict of Interest

Authors do not have any conflict of interest, academic or financial, for publication of this work. Authors takes the responsibility of text and contents presented in this article.

References

1. E.R.D. Villarreal, J. Garcia-Alonso, E. Moguel, J.A.H. Alegria. Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security. *IEEE Access* **2023**, 11, 5629–5652.
2. P. Singh, S. Verma, Kavita. Analysis on different strategies used in blockchain technology. *J. Comput. Theor. Nanosci.* **2019**, 16 (10), 4350–4355.
3. C.R. Araujo-Inastrilla, A.A. Vitón-Castillo. Blockchain in health sciences: Research trends in Scopus. *Iberoam. J. Sci. Meas. Commun.* **2023**, 3 (2).
4. K. Kaushik, A. Kumar. Demystifying quantum blockchain for healthcare. *Secur. Priv.* **2023**, 6 (3), 284.
5. M. Sun, Q. Chai, C.T. Ng. Managing the quality-speed tradeoff in blockchain-supported healthcare diagnostic services. *Omega (United Kingdom)* **2023**, 120.
6. F.N. Tareen, A.N. Alvi, A.A. Malik, et al. Efficient Load Balancing for Blockchain-Based Healthcare System in Smart Cities. *Appl. Sci.* **2023**, 13 (4), 2411.
7. S.A. Bennacer, K. Sabiri, A. Aaroud, K. Akodadi, B. Cherradi. A comprehensive survey on blockchain-based healthcare industry: applications and challenges. *Indones. J. Electr. Eng. Comput. Sci.* **2023**, 30 (3), 1558–1571.
8. P. Singh, A.P. Singh, A. Gupta. Design Strategies for Mobile Ad-hoc Network to Prevent from Attack. In *Proceedings of the 3rd International*

Conference on Advanced Computing and Software Engineering. SCITEPRESS; Science and Technology Publications, **2022**; pp 194–201.

9. D. Aloini, E. Benevento, A. Stefanini, P. Zerbino. Transforming healthcare ecosystems through blockchain: Opportunities and capabilities for business process innovation. *Technovation* **2023**, 119, 102557.
10. K. Kiania, S.M. Jameii, A.M. Rahmani. Blockchain-based privacy and security preserving in electronic health: a systematic review. *Multimed. Tools Appl.* **2023**, 82 (18), 28493–28519.
11. D. Doreen Hephzibah Miriam, D. Dahiya, Nitin, C.R. Rene Robin. Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. *Intell. Autom. Soft Comput.* **2023**, 35 (2), 1889–1906.
12. A. Lakhan, M.A. Mohammed, J. Nedoma, et al. DRLBTS: deep reinforcement learning-aware blockchain-based healthcare system. *Sci. Rep.* **2023**, 13 (1), 4124.
13. S. Ahmad, S.K. Arya, S. Gupta, P. Singh, S.K. Dwivedi. Study of Cryptographic Techniques Adopted in Blockchain. In *4th International Conference on Intelligent Engineering and Management, ICIEM 2023*; IEEE, **2023**; pp 1–6.
14. P. Singh, P. Sinha, A. Raghav. A blockchain IoT hybrid framework for security and privacy in a healthcare database network. In *Dynamics of Swarm Intelligence Health Analysis for the Next Generation*; IGI Global, **2023**; pp 210–225.
15. R. Pathak, B. Soni, N.B. Muppalaneni. Role of Blockchain in Health Care: A Comprehensive Study. In *Lecture Notes in Networks and Systems*; Springer Nature Singapore, Singapore, **2023**; Vol. 540, pp 137–154.
16. E. Elgamal, W. Medhat, M.A. Elfatah, N. Abdelbaki. Blockchain in Healthcare for Achieving Patients' Privacy. In *20th International Learning and Technology Conference, L and T 2023*; IEEE, **2023**; pp 59–64.
17. S. David, K. Duraipandian, D. Chandrasekaran, et al. Impact of blockchain in healthcare system. In *Unleashing the Potentials of Blockchain Technology for Healthcare Industries*; Academic Press, **2023**; pp 37–57.
18. H. Patel, M. Patel. Sensors for Falls and Fall Detection Techniques: From the past to the future. *J. Integr. Sci. Technol.* **2023**, 11 (4 SE-Biomedical and Pharmaceutical Sciences), 575.
19. K.P. Rama Krishna, R. Thirumuru. Optimized energy-efficient multi-hop routing algorithm for better coverage in mobile wireless sensor networks. *J. Integr. Sci. Technol.* **2022**, 10 (2), 100–109.
20. C. Awasthi, M. Nawal, P.K. Mishra. Security Concerns of Fog Computing in Field of Healthcare using Blockchain: A Review. In *Proceedings - International Conference on Communication, Information and Computing Technology, ICCICT 2021*; IEEE, **2021**; pp 1–5.