Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4735272, 10 pages
https://doi.org/10.1155/2022/4735272

Research Article

Optimized Embedded Healthcare Industry Model with Lightweight Computing Using Wireless Body Area Network

Tanzila Saba,[1] **Amjad Rehman**,[1] **Khalid Haseeb**,[2] **Saeed Ali Bahaj**,[3] **and Jaime Lloret**[4,5]

[1]*Artificial Intelligence and Data Analytics (AIDA) Lab, CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia*
[2]*Department of Computer Science, Islamia College Peshawar, Peshawar, Pakistan*
[3]*MIS Department, College of Business Administration, Prince Sattam bin Abdulaziz University, Al Kharj 16273, Saudi Arabia*
[4]*Universitat Politenica de Valencia, Spain*
[5]*Staffordshire University, Stoke, UK*

Correspondence should be addressed to Jaime Lloret; jlloret@dcom.upv.es

Received 15 December 2021; Revised 14 March 2022; Accepted 29 March 2022; Published 25 April 2022

Academic Editor: Marica Amadeo

Wireless technology is offering numerous growth to develop communication systems. The Internet of Things (IoT) is combined with the sensing ecosystem to transfer and process the physical environment. Recently, IoT devices have collaborated with wireless devices to improve embedded medical applications. Many solutions are proposed to decrease the power consumption of the sensing ecosystem and support the health industry. However, optimizing the transformation of collected data with lightweight power consumption is still a burning research issue. Moreover, uncontrolled network devices and healthcare professionals are remotely accessed by such embedded systems. Thus, securing sensitive information is also a significant factor for mobile communications. Therefore, this research presents an optimized embedded healthcare industry model with lightweight computing using a wireless body area network (WBAN), aiming to lessen the control overheads and improve the power consumption in mobile e-health services. To begin, it employs an optimal learning algorithm to lower the management costs of embedded systems in order to transform and administer the electronic health record (EHR) more efficiently. Second, with the help of trustworthy gateways, it delivers a safe EHR algorithm as well as lightweight computing resources for embedded systems. The proposed model is tested with a variety of experiments and demonstrates its significant improvement over state-of-the-art techniques.

1. Introduction

Internet of Things (IoT) has grown in popularity; it has begun to reform and modify our lifestyles through wireless networks. RFID, sensors/devices, communication lines, and an end-user interface are all part of the IoT system's architecture. Wireless technologies and medical devices offer many real-time services while keeping the availability and maintainability of patient-related data [1–3]. Smart processing is a revolutionary innovation that attempts to link various physical objects with embedded technology that communicates and perceives or interacts with their internal states or external surroundings. In embedded healthcare applications [4, 5], sensor-enabled digital devices are connected to the Internet, and such paradigms enable new services for smart cities. Using the Internet of Medical Things (IoMT), the biosensors are utilized for information sensing, analyzing, and sharing the sensitive data of WBAN with a medical expert over the open-space wireless systems [6–8], as depicted in Figure 1. Accordingly, it is now possible for the IoT systems to act upon the distribution of smart services to end-users by including tiny microcontroller chips, smart sensors, and actuators. Many advanced wireless technologies have been caused by an enormous amount of linked devices, resulting in the IoT-based medical revolution. These embedded devices continuously gather and analyze the

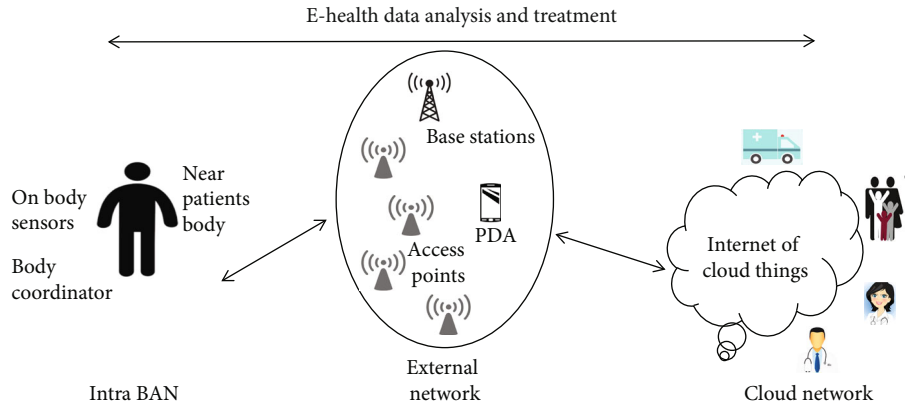


Figure 1: E-health model using IoMT.

biometric data and then send large volumes of data via the network towards the cloud system [9–11]. E-health data is transmitted to the body coordinator, and the body coordinator further forwards it to medical experts for real-time treatments with the support of a digital mobile network [12–14]. Embedded IoT-based healthcare systems are probable to decrease the management cost and improve the real-time analysis of patients' conditions. Although many suggested solutions have been offered as valuable solutions to the medical field [15–17]; however, despite this, IoT inherits the significant problems of advanced technologies in terms of resource management and trustworthiness data relaying systems.

Moreover, smart devices such as mobiles, sensors, and actuators communicate with each other over the unpredictable communication medium and are subject to network threats, thus needing more security functionalities [18–20]. This research introduces an optimization model for embedded medical applications using a wireless ecosystem that lowers the processing overheads for smart devices. It uses the artificial intelligence technique to make the embedded system more robust and offers timely decisions for analyzing the health data. The proposed model extracts the most reliable and near-optimal network edges from the undirected graph by exploring the multivariable objective function. Moreover, gateways perform dual responsibilities to reduce excessive latency and offer an energy-efficient healthcare system. The proposed model provides compatibility among heterogeneous communication devices and sink nodes by utilizing the gateways in embedded applications. The sink nodes are interconnected with centralized storage systems, and authorized users can access the needed data with the support of security policies. Based on recent studies, IoMTs for embedded applications have limited constraints and can be easily compromised in terms of privacy, integrity, and availability of health data. Therefore, the proposed model also copes with protection issues and provides a collaborative algorithm for mobile communication against malicious attacks.

This work is comprised of the following contributions.

(i) An optimization algorithm is introduced for embedded health applications that efficiently manage the routing cost in transforming digital records

(ii) It also incorporates the security features for medical devices and copes with communication anomalies using data protection and integrity

(iii) The IoT-based wireless ecosystem secures the health data and offers a lightweight algorithm to detect unauthentic devices in the proximity of remote cloud systems

(iv) The embedded system is simulated with a wide range of experiments to compare existing work and analyze its performance

The article's remaining sections are divided into the following subsections. Section 2 examines related work and points out the shortcomings of the present solutions. The plan and development of the proposed model are explained in Section 3. The simulation parameters and details of the experiments are discussed in Section 4. Section 5 concludes this research work with future work.

2. Related Work

In the embedded system, IoT technologies are broadly used to integrate wireless objects for information collection, processing, and facilitating the physical world [21–23]. The data gathering and transmission depend on various parameters including computing power, storage space, and energy utilization. Due to tight constraints for embedded systems, optimizing the performance of the wireless system is the main research challenge. Health monitoring systems based on the Internet of Things operate on a tiered architecture, including a perception layer, a network layer, and an application layer [24–26]. Each layer has certain security and privacy implications that must be handled appropriately. Numerous studies have been conducted to address these security concerns across various IoT sectors. Additionally, many security frameworks for IoT-based e-health systems have been established. In [27], the authors build and construct a specific framework for an IoT-based smart health system and focused on interoperability challenges. The IoT system's particular requirements were investigated and utilized as the basis for developing a framework based on multiple technological standards and communication protocols.

Within the scope of protocols and standards, contemporary web technologies, communication protocols, and hardware design are used. This technique guarantees that the proposed model's unique expectations may be met with certainty. The studies demonstrated that a dedicated gateway device may be utilized to provide interoperability between various IoT devices, standards, and protocols in a smart health system and the concurrent usage of many web technologies in limited and Internet contexts.

Authors in [28] present an approach for anonymizing sensitive health datasets transmitted in an IoT setting utilizing a wireless communication system. The algorithm specifies records that cannot be released during the data session from users engaging online to maintain security and privacy, hence protecting user privacy. In addition, the proposed technique incorporates a safe encryption procedure that ensures the confidentiality of health data. The authors also conducted a mathematical function analysis to verify the algorithm's anonymity function. The findings reveal that the anonymization method ensures security for the IoT system in question when used in the context of healthcare communication networks. A deep reinforcement learning-(DRL-) based intelligent routing method for IoT-enabled WSNs is presented [29], which dramatically reduces latency and increases network lifespan. The suggested technique separates the whole network into various unequal clusters based on the current data load in the sensor node, preventing the network from dying prematurely. The experimental findings are compared to state-of-the-art algorithms to show that the suggested method is efficient in terms of the number of live nodes, packet delivery, energy efficiency, and network communication latency.

Clustering is a valuable data collecting technique for the IoT that reduces energy usage selectively by grouping IoT nodes into clusters [30]. The cluster head has complete control over all cluster nodes and is responsible for all intracluster and intercluster communication. Due to the NP-hard nature of the clustering issue, this paper proposes a moth-flame optimization algorithm for selecting the smallest number of required clusters for routing. This technique, derived from the moth's life cycle, promotes efficient communication by establishing the ideal number of clusters. The suggested fitness function is composed of three components: the total of the distances, the remaining energy, and the degree of the nodes. The experimental findings are compared to those obtained using a variety of clustering techniques, including the whale optimization algorithm, innovative chemical reaction optimization, and cuckoo search optimization. In [31], the authors offer a security architecture for real-time health monitoring systems that ensure data confidentiality, integrity, and authenticity via the use of two widely used IoT protocols: the constrained application protocol (CoAP) and message inquiry telemetry transports (MQTT). This security architecture is designed to protect sensor data from security flaws while it is being sent continually between layers, and it accomplishes this goal by using hypertext transfer protocols (HTTPs). As a result, it protects against breaches with a very low risk-to-benefit ratio. This article's approach focuses on how the security architecture of IoT-based real-time health systems is safeguarded through the CoAP and HTTPs layers. This study suggests ERBAC and the Twofish algorithm to safeguard IoT health data from a public cloud storage standpoint. In IoT applications, the proposed system is expected to drastically reduce storage costs and offer secure cloud storage of medical data based on role-based access regulations.

The authors [32] also introduce a clustering approach to speed up the retrieval of important medical data. The rationale for finding hidden instances in clinical data is clustering. Using these examples, clinicians made professional decisions about illness likelihood. Compared to other collections, the dataset for clustering categories is greater. Also proposed is a clustering approach based on the computation of the progress of a swarm of molecules, dubbed clustering calculation. For the grouping technique, it leverages global improvements in PSO computation. The authors present a FOG-assisted CnCI model for dependable healthcare facilities [33]. Creating a safe and reliable CnCI for IoTH networks is difficult to solve. We developed a unique mathematical approach to design FOG-assisted CnCI for IoTH networks (i.e., integer programming). Wireless link interfacing gateways are regarded as virtual machines (VM). An IoTH network is made up of three wirelessly connecting nodes: virtual machines (VMs), reduced computing power gateways (RCPG), and full computing power gateways (FCPG). The goal is to reduce the weighted total of infrastructure and operating expenses associated with IoTH network design. An evolutionary technique based on swarm intelligence is applied to tackle IoTH network planning for higher quality solutions in a reasonable period. The summary of the related work is given in Table 1.

3. Embedded Healthcare Paradigm with a Lightweight IoT-Protected System

The proposed work comprises medical devices that are collaborated and interconnected with each other with a wireless system for sensing health information. The medical sensors may collect the health data such as heartbeat, blood pressure, ECG, and temperature. The set of medical devices is further attached with the body coordinator to accomplish intercommunication with remote systems. Medical data is very crucial for accurate decisions and supporting a reliable health system. Therefore, the proposed model also provides security services with a mobile sink and protects the communication with nominal wireless breaches. The proposed e-health model is comprised of two main components. At the beginning of the network setup, nodes are interconnected in the form of an undirected graph $G(n, e)$. Each node is known as a vertex, and each edge has some numeric value to represent the initial cost among consecutive nodes. The first component presents the optimization criteria to decrease the consumption in the decision support system and train the model with the updated values. Secondly, the mobile sink is protected from nonvalid requests and offers secured services to constraint devices, thus avoiding frequent damages to health systems. The proposed model exploits the combinatorial optimization [34] to connect the sensor nodes and

Table 1: Summary of the existing work with the proposed model.

Existing solutions	
(a) Medical applications have been developed to improve society's comfort by delivering real-time patient data to doctors and consultants using wireless systems. (b) IoMT-based biosensors periodically collected health data and forward it to the remote system using body coordinators. However, their several limitations offer the main critical challenges in IoT-based environments, such as delay management, energy consumption, and security attacks. (c) Many solutions have been proposed to overcome the problems of medical applications in forwarding health data over wireless technologies, but optimization methods are still desirable. (d) Moreover, most solutions fail to protect e-health data from malicious examinees and threats. As a result, end-users must be trusted on obtained data from unreliable IoT networks.	
Proposed optimized embedded healthcare industry model with lightweight computing using WBAN	(a) An algorithm is developed for healthcare services with the support of an optimization algorithm and mobility. (b) It balances the contribution of nodes uniformly in terms of various factors. (c) Efficiently explores the random communication channels with an adaptive mobility evaluation. (d) Formulates a protected and secured option for malicious traffic detection and supports trusted IoT-based medical applications.

extract the most feasible solutions for reaching its goal state. The feasible solutions are obtained by computing a multivariable objective function. It provides the intelligence method for a decision support system and reduces the excessive computing resources with timely delivery of critical data to medical centers. Let us consider that $X = x_1, x_2, \cdots, x_n$ is the set of medical nodes. If the system is a node $x_i \in X$, then $f(x)$ is the finite set of feasible solutions. Suppose that $t_1, t_2, t_3, \cdots, t_n$ are set of feasible solutions towards the goal state S, as given in the following equation.

$$x_i \longrightarrow : f(x) = t_1, t_2, t_3, \cdots, t_n. \tag{1}$$

The proposed model optimizes the decision criteria for the two cases. The first one is how many paths are available for sending medical data and the second one is which the most optimal solution to S. The proposed model computes the cost function using a multivariable process to determine this process. The multivariable process determines the weighted values in terms of distance d_i, nodes density nd, and loss length loss_len_i over the edge $e(i, j)$, as given in the following equation.

$$f(x) = \alpha * \frac{1}{d_i} + \beta * \text{nd} + \gamma * \left(\frac{1}{\text{loss\_len}_i}\right). \tag{2}$$

In Equation (2), d_i is the absolute value from the source device to sink node using Euclidean distance, nd is the number of neighbors in the proximity of node i that can be derived from its local table and loss_len_i shows the consecutive number of packets lost over the edge $e(i, j)$. The longer the loss length indicates the unreliable and unstable edge. Accordingly, the proposed model uses the packets' information and interval of instability time; accordingly, loss_len_i can be defined in the following equation.

$$\text{loss\_len}_i = pkts_{\text{info}} + \left(\frac{E}{T}\right), \tag{3}$$

where E denotes the time interval in packet receiving and T is the total time.

After the computing of $f(x)$ value of the selective edge by exploiting cost function, the proposed model restructures the route formation $R(i)$ process as given in the following equation.

$$R(i)\colon x_i t_i, f(x). \tag{4}$$

Figure 2 illustrates the working flow of the proposed optimization model for embedded medical applications. Firstly, exploring the combinatorial optimization algorithm proposed model offers the balanced utilization of the embedded resources in data transformation. Furthermore, the multivariable objective function effectively computes the cost value and intelligently reduces route reconfiguration. The system is supported by multivalued judgments that uniformly balance communication between devices.

A distributed privacy-aware health management system with authentic services is also provided by the proposed model. All communication devices in the healthcare system must validate themselves in a distributed manner and provide a reliable solution to e-health consumers. The proposed model also provides the securing of health data using the integration of gateways and mobile sink. In the first stage, by exploring the role of the sink node, the proposed model identified the authentic and trusted gateways. The mobile sink rotates around the gateways' perimeter, keeping track of information about registered gateways. The gateway node authenticates with the mobile sink first, and the mobile sink adds the entry to its map table once it receives the request. The map table is comprised of gateway identity ID and time stamp t. Also, the request packet is digitally signed with the private key of the gateway node. Let us consider that request message $r \in R$ and generates a digital signature S as $e_k(r)$. The digital signature S is transmitted towards the mobile sink with the integration of ID. Upon receiving the request packet, the mobile sink m_s first performs a verification function v_f as given in the following equation.

$$m_s \longrightarrow g_n : v_f(r, S). \tag{5}$$

Upon successful verification, the mobile sink generates a secret key for the corresponding trusted gateway and performs an encryption method to ensure privacy for health

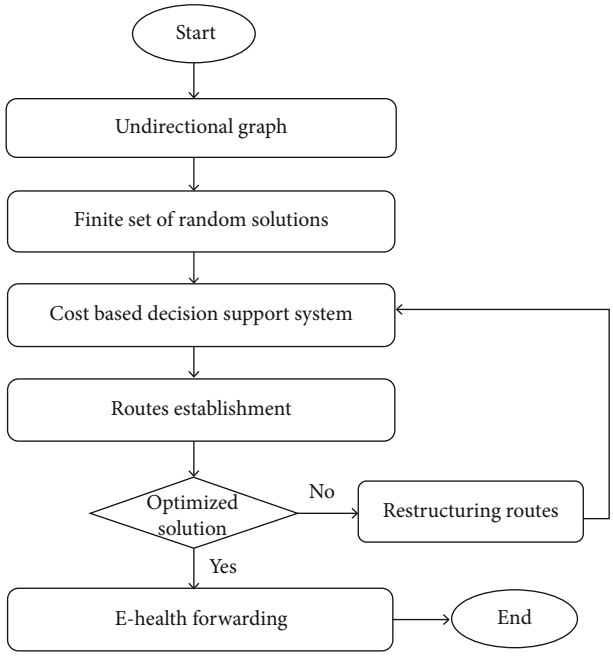


Figure 2: E-health forwarding system using IoMT.

data. In the proposed model, the mobile sink generates the secret keys for gateway nodes by using the Blum Blum Shub algorithm [35], as given in the following equation.

$$X_{n+1} = X_n^2 \bmod n. \tag{6}$$

In Equation (6), $n = pq$, which is the product of two large prime numbers. X_n is the secret random value for the gateway node g_i, and X_0 is the seed integer value that is coprime to n. After generating and distributing secret keys between the mobile sink and gateway nodes, the gateway node uses an encryption method E_x to retain privacy for health data m_i, as given in the following equation.

$$E_x(m_i) = (m_i \oplus X_n) \oplus \mathrm{ID}. \tag{7}$$

Furthermore, the encrypted data is further protected by using the X or operation with identity to give authentication. The flowchart of the developed security method for e-health systems is shown in Figure 3. The trusted gateways have dual collaboration with sensing devices and mobile sink. The sink node just enables the request for genuine gateways and then transfers the health data to the remote system based on the mapping table. Gateway nodes can transport data after receiving a valid response from the sink node. Furthermore, secret values are used by all devices for EHR encryption and decryption processes to preserve data privacy. As a result, end-users are able to obtain secure and trustworthy health information via an insecure communication system.

The list of abbreviations in the proposed model is given in Table 2.

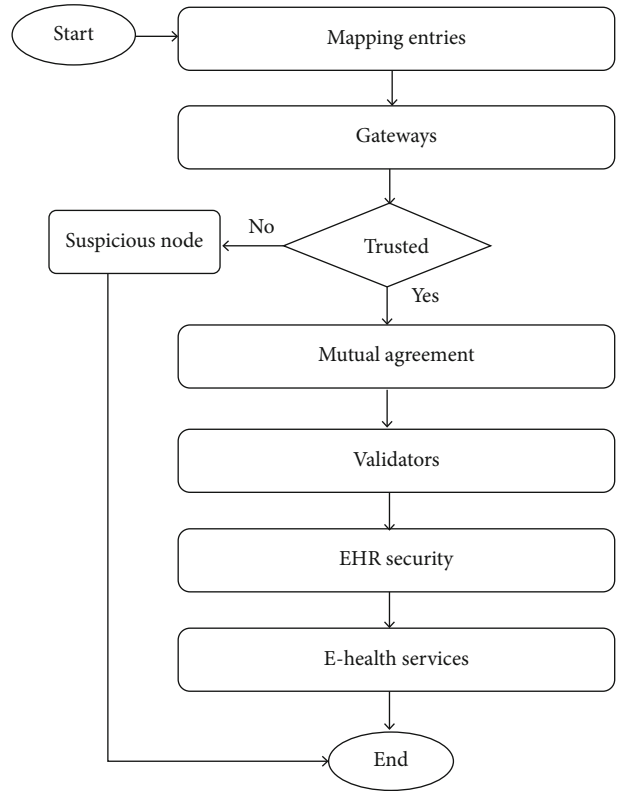


Figure 3: Flowchart of the verification and security for embedded medical application.

Table 2: List of abbreviations.

Notations	Definitions of the abbreviations
G	Complete graph
S	Goal state
ID	Identity
$f(x)$	Finite set of solutions
d_i	Distance
nd	Node density
$\mathrm{loss\_len}_i$	Loss length
$R(i)$	Route formation
m_s	Mobile sink
g_n	Gateway node
X_{n+1}	Set of keys
E_x	Encryption function
m_i	Health message

4. Simulation Environment

This section presents the simulation environment and experiment results of the proposed model with existing solutions. Using the NS-3, we conduct the simulation and analyze the results in terms of network throughput, packet drop rate, link downtime, and erroneous packets. The proposed model is tested against the FOG-assisted CnCI model

and DRL-based intelligent routing method. The experimental tests are performed using varying data sensing rates and speeds of the mobile sink. The data sensing rate varies from 50 to 400 bits/sec, and the sink's speed varies from 2 to 6 m/sec. The number of sensor nodes is set to 20, 40, and 60 with homogeneous constraints. Sink node has no limits for various constraints and processing power. Initially, the sensor nodes have an energy resource of 2 J. We considered the wireless standard IEEE 802.15.6 to support the routing process of the proposed model. The simulation is run for a period of 20 min. Packet size is set to 3 bytes, and data flow is exploiting periodic intervals. It is adopted for simulation experiments that need an expected response time and delivery performance between communication devices with limited channel bandwidth. The number of malicious nodes is set to 5. The simulation environment's configuration parameters are shown in Table 3.

Table 3: Simulation parameters.

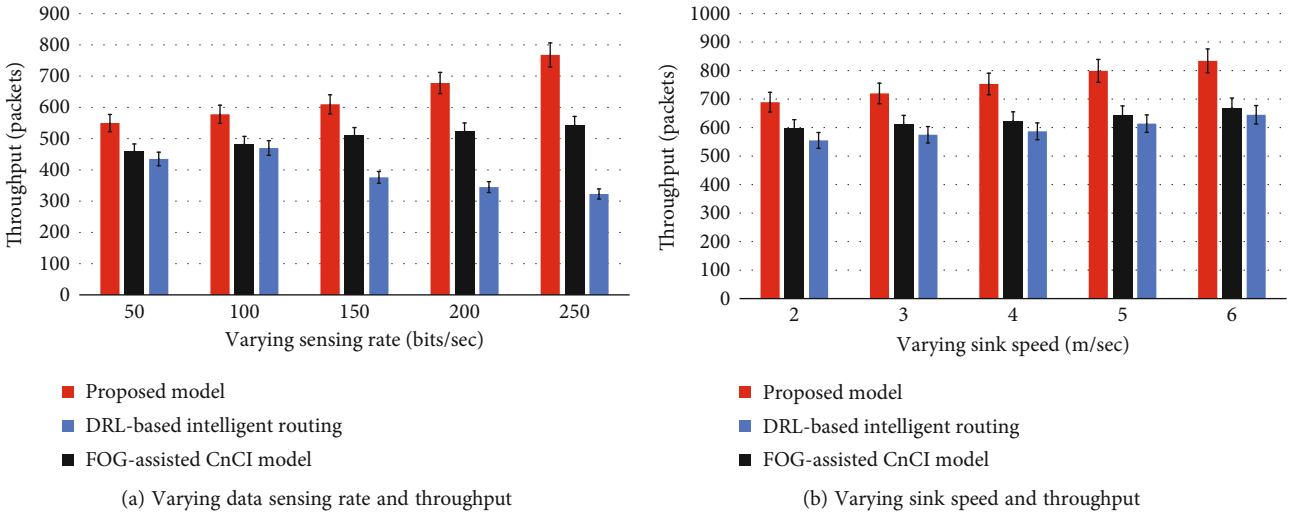
Parameter	Value
Simulation area	20 m × 20 m
Initial energy	2 J
Malicious nodes	1-5
Sensor nodes	20, 40, 60
Gateways	1-5
Packet size	32 bytes
Transmission range	3 m
Wireless standard	IEEE 802.15.6
Simulation time	20 min
Simulations	10
Data traffic	Periodic intervals

In Figures 4(a) and 4(b), the performance evaluation of the proposed model against the existing solution is presented. The performance is computed in terms of network throughput. It can be defined as how many data packets can be transferred between a source and sink node in particular time limits. It is seen that with a varying sensing rate and sink speed, the proposed model improves the network throughput by an average of 43% and 23%. It is that the proposed model uses the optimization technique to estimate the usage of resource consumption. Moreover, the multivariable objective function utilizes the realistic parameters to compute the cost value, and accordingly, edges are extracted from the unidirectional graph for data transportation. Also, the mobile sink explicitly increases the delivery ratio of embedded systems to end-users and facilitates the smart devices for getting the ERH timely. In this approach, the suggested model facilitates the identification of neighbors and the updating of optimization criteria. Furthermore, the suggested approach employs the mobile sink to lower the transmission power of medical equipment while balancing the communication load by transmitting the ERH to emergency centers. The suggested approach uses a multihop forwarding strategy and interacts with gateways to improve the delivery performance of the embedded system.

Figures 5(a) and 5(b) illustrate the proposed model's performance evaluation for packet drop ratio with existing solutions. It is defined as the fraction of the total sent data packets that have not been received at the destination side within a particular time interval. It was discovered that, in contrast to previous research, the suggested model reduces the packet drop ratio by an average of 61% and 59% throughout a range of sensing rates and sink mobility. As a result, the proposed model uses the metaheuristic technique to efficiently analyze the cost function of the available solutions and, as a result, select the most trustworthy nodes as a next hop. The suggested model also balances the transmission links with an efficient data flooding scheme by exploiting the network condition. Furthermore, the proposed model utilizes the lost and response time factors in determining the optimal neighbors from the set of nodes. Moreover, by efficient utilization of link channels, the proposed model increases the lifetime for routes and offers balanced communication services in terms of delivery performance. Furthermore, the multiobjective function provides optimized routing metrics and forwarders the health data through reliable neighbors. Finally, the security functions deal with the malicious nodes and reduce their capabilities in dropping the IoT data with robust verifications.

Figures 6(a) and 6(b) illustrate the proposed model's experimental results against the existing solution in terms of link downtime. It is defined as a computed time when a particular wireless link between consecutive nodes is unavailable due to any communication issue. It was observed that the proposed algorithm significantly decreases the link downtime by an average of 27% and 36% for varying sink speed and data sensing rates. It explores the mobility aspect of the sink node and dynamically floods the positioning coordinates for rapid data gathering and forwarding processes. Furthermore, a multiheuristic algorithm offers the balance contribution of medical sensors in terms of various parameters and generates an optimal decision supporting system. The integration of cost evaluation function based on network parameters and assigning the appropriate solutions for set for nodes, decreasing the response time and data delay for smart devices. Furthermore, the proposed model uses the metrics of lost time to find the optimal links; thus, only fewer overhead nodes are elected for IoT data transformation. Besides, the devices' mutual authentication and hop-by-hop verification secure the data on each iteration and develop a trusted chain. Accordingly, the proposed model increases the flow of the information without frequent data disruption and excessive latency to support the applications of the health industry.

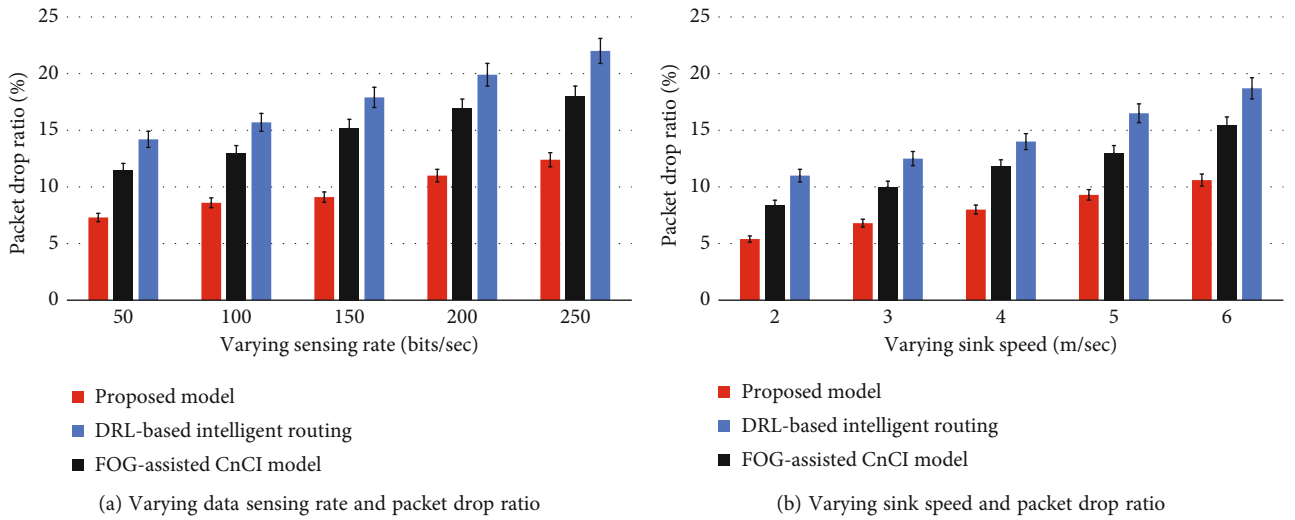
Figures 7(a) and 7(b) explain the proposed model's performance results with other works for overheads. With increasing data sensing rate and speed of sink, it was noticed that overhead also increases. However, the proposed model significantly reduces the overhead by 36% and 41% as compared to other works. It is due to that the proposed model efficiently computed the cost factor of the device by exploring the quality-aware parameters and intellectually updating the decision support system. Moreover, the routes are established using the integration of a mobile sink, which not only reduces the transmission distance among devices but also



(a) Varying data sensing rate and throughput

(b) Varying sink speed and throughput

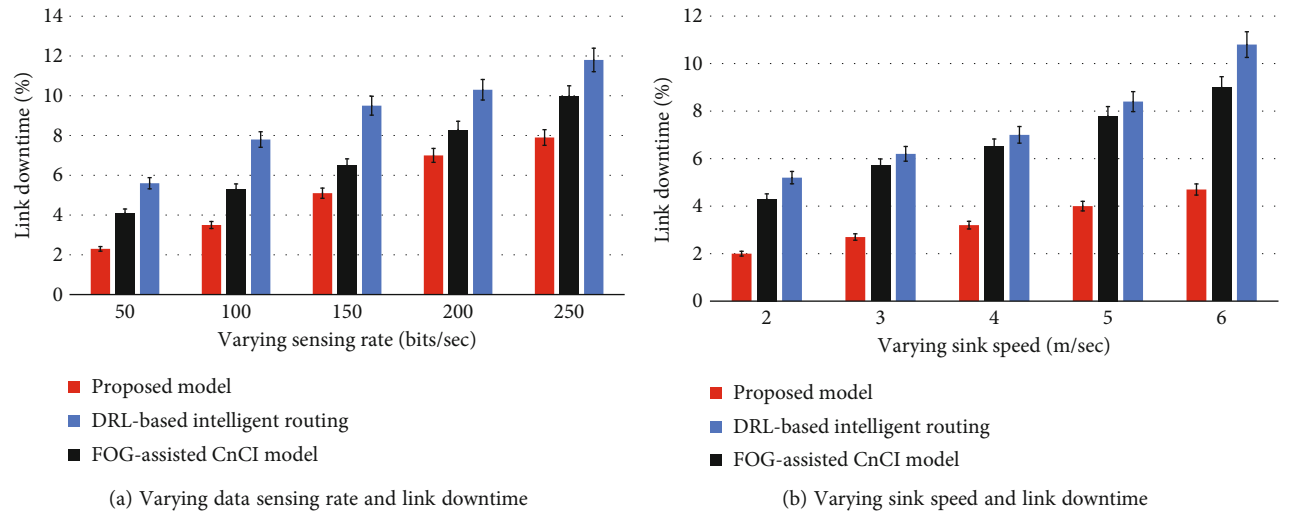
FIGURE 4: Performance evaluation of the proposed model for throughput.



(a) Varying data sensing rate and packet drop ratio

(b) Varying sink speed and packet drop ratio

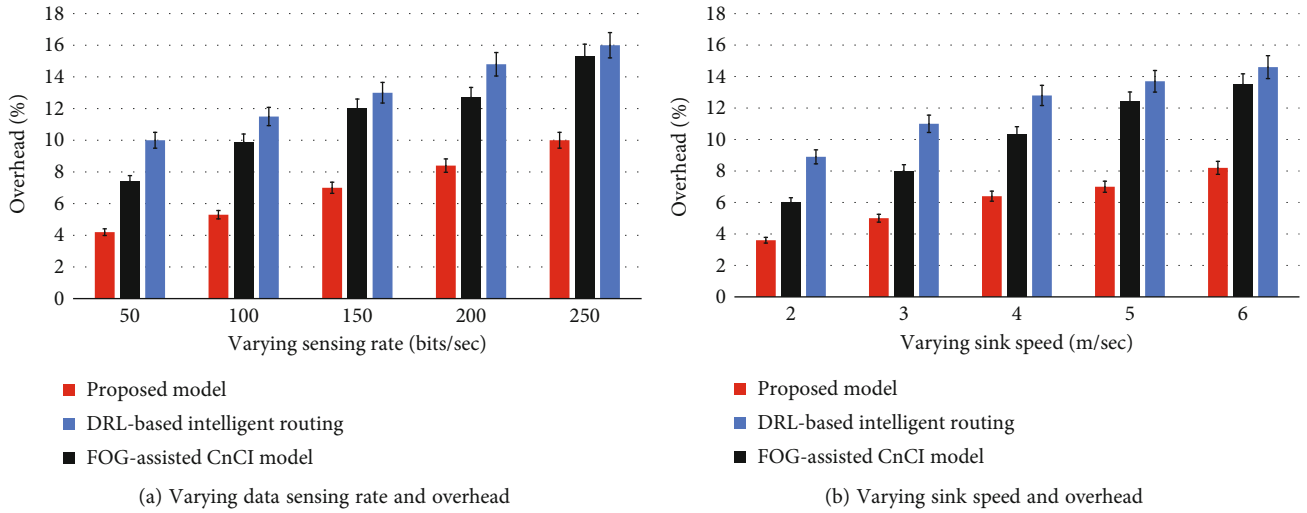
FIGURE 5: Performance evaluation of the proposed model for packet drop ratio.



(a) Varying data sensing rate and link downtime

(b) Varying sink speed and link downtime

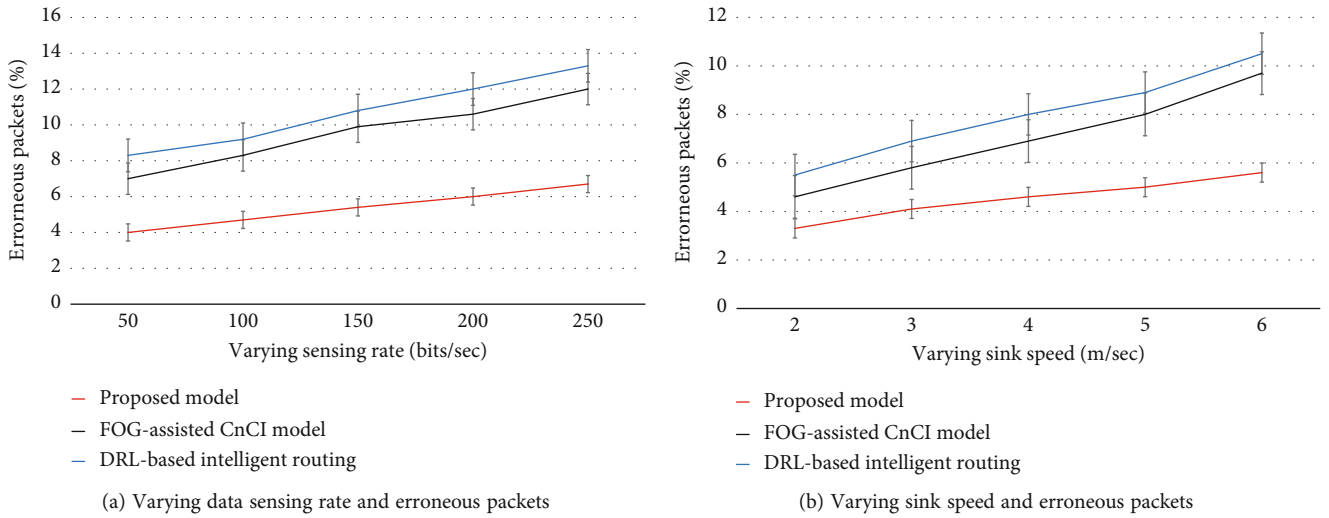
FIGURE 6: Performance evaluation of the proposed model for the link downtime.



(a) Varying data sensing rate and overhead

(b) Varying sink speed and overhead

Figure 7: Performance evaluation of the proposed model for the overhead.



(a) Varying data sensing rate and erroneous packets

(b) Varying sink speed and erroneous packets

Figure 8: Performance evaluation of the proposed model for erroneous packets.

minimizes the computing power for the processing of EHR. Unlike most of the existing work, the proposed model for health systems also protects health data with the support of security features. The adaptation of security functions increases the confidence among devices with data privacy and avoids network interruption and additional overheads.

In Figures 8(a) and 8(b), the performance analysis of the proposed model is done against other solutions in terms of erroneous packets. It is defined as a packet error that means something is wrong during data transmission. In the proposed model, this metric is used to determine the system's reliability in the presence of malicious nodes. It is noticed that the proposed algorithm minimizes the ratio of erroneous packets by an average of 47% and 44% under a varying data sensing rate and speed of the sink node. It is because of the uniform load distribution among IoT devices using combinatorial optimization. Moreover, it also decreases the extra energy consumption in sending the data from the observing field using the mobile sink, which balances the load on nodes near uniformly and provides lesson packet errors in the presence of malicious nodes. Also, only those nodes exchange their information to proceed with the data routing that falls into the coverage range.

5. Conclusion

Embedded applications are widely utilized using IoT and wireless technologies for crucial processing and monitoring. However, the limited resources of embedded applications reflect the unpredictable performance and compromise the data transformation for the wireless environment. This study uses WBAN to offer a methodology for optimizing embedded systems that are expressly utilized for health information. It gives innovative solutions for lowering administration and processing expenses on constrained medical equipment by exploring the combinatorial optimization technique. Moreover, the embedded system is also provided privacy and authentication using lightweight

computing functions among wireless devices. The proposed model is beneficial for real-time observing. On the other hand, the multivariable objective function is utilized to eliminate erroneous communication among IoT-based ecosystems. Furthermore, the compromising ratio for embedded systems in forwarding the electronic health record over wireless channels also decreases with the integration of security algorithms. However, by using the movable sink, it is acknowledged that the suggested model suffers from frequent route damages and is not always optimal in real-world scenarios. Therefore, we aim to develop some machine learning model to support the proposed model against communication anomalies and increase its trustworthiness. It also needs to embrace the autonomous cloud concept to reduce computing overheads on embedded systems.

Data Availability

The research does not have a dataset.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

This work was technically supported by the Artificial Intelligence & Data Analytics Research Lab, CCIS Prince Sultan University. The authors are thankful for their support.

References

[1] J. Maktoubian and K. Ansari, "An IoT architecture for preventive maintenance of medical devices in healthcare organizations," *Health and Technology*, vol. 9, no. 3, pp. 233–243, 2019.

[2] L. Wei, S. Hou, and Q. Liu, "Clinical care of hyperthyroidism using wearable medical devices in a medical IoT scenario," *Engineering*, vol. 2022, pp. 1–10, 2022.

[3] C. Kotronis, I. Routis, E. Politi et al., "Evaluating Internet of Medical Things (IoMT)-based systems from a human-centric perspective," *Internet of Things*, vol. 8, article 100125, 2019.

[4] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial Internet of Things (IIoT) healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2736–2744, 2018.

[5] M. M. Dhanvijay and S. C. Patil, "Internet of Things: a survey of enabling technologies in healthcare and its applications," *Computer Networks*, vol. 153, pp. 113–131, 2019.

[6] M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, and P. K. R. Maddikunta, "A review on security and privacy of Internet of Medical Things," in *Intelligent Internet of Things for Healthcare and Industry*, pp. 171–187, Springer, 2022.

[7] S. Tahir, S. T. Bakhsh, M. Abulkhair, and M. O. Alassafi, "An energy-efficient fog-to-cloud Internet of Medical Things architecture," *International Journal of Distributed Sensor Networks*, vol. 15, no. 5, 2019.

[8] D. D. Olatinwo, A. Abu-Mahfouz, and G. Hancke, "A survey on LPWAN technologies in WBAN for remote health-care monitoring," *Sensors*, vol. 19, no. 23, p. 5268, 2019.

[9] J. Lloret, L. Parra, M. Taha, and J. Tomás, "An architecture and protocol for smart continuous eHealth monitoring using 5G," *Computer Networks*, vol. 129, pp. 340–351, 2017.

[10] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: a survey," *Future Generation Computer Systems*, vol. 97, pp. 219–235, 2019.

[11] X. Liu, Z. Qin, Y. Gao, and J. A. McCann, "Resource allocation in wireless powered IoT networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4935–4945, 2019.

[12] C. Dhasarathan, R. Dayalan, V. Thirumal, and D. Ponnurangam, "A coordinator-specific privacy-preserving model for e-health monitoring using artificial bee colony approach," *Security and Privacy*, vol. 1, no. 4, article e32, 2018.

[13] K. Haseeb, T. Saba, A. Rehman, I. Ahmed, and J. Lloret, "Efficient data uncertainty management for health industrial Internet of Things using machine learning," *International Journal of Communication Systems*, vol. 34, no. 16, article e4948, 2021.

[14] K. Suriyakrishnaan and D. Sridharan, "Reliable packet delivery in wireless body area networks using TCDMA algorithm for e-health monitoring system," *Wireless Personal Communications*, vol. 103, no. 4, pp. 3127–3144, 2018.

[15] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–11, 2018.

[16] N. Kalid, A. Zaidan, B. Zaidan, O. H. Salman, M. Hashim, and H. Muzammil, "Based real time remote health monitoring systems: a review on patients prioritization and related "big data" using body sensors information and communication technology," *Journal of Medical Systems*, vol. 42, no. 2, pp. 1–30, 2018.

[17] S. Bhattacharya, P. K. R. Maddikunta, Q.-V. Pham et al., "Deep learning and medical image processing for coronavirus (COVID-19) pandemic: a survey," *Sustainable Cities and Society*, vol. 65, article 102589, 2021.

[18] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, article 293, 2019.

[19] T. Saba, K. Haseeb, I. Ahmed, and A. Rehman, "Secure and energy-efficient framework using Internet of Medical Things for e-healthcare," *Journal of Infection and Public Health*, vol. 13, no. 10, pp. 1567–1575, 2020.

[20] K. Haseeb, A. Rehman, T. Saba, S. A. Bahaj, and J. Lloret, "Device-to-device (D2D) multi-criteria learning algorithm using secured sensors," *Sensors*, vol. 22, no. 6, article 2115, 2022.

[21] M. Mohamed, "A comparative study on Internet of Things (IoT): frameworks, tools, applications and future directions," *Journal of Intelligent Systems and Internet of Things*, vol. 1, no. 1, pp. 13–39, 2020.

[22] A. Rehman, K. Haseeb, T. Saba, and H. Kolivand, "M-SMDM: a model of security measures using Green Internet of Things with cloud integrated data management for smart cities," *Environmental Technology & Innovation*, vol. 24, article 101802, 2021.

[23] S. Sendra, L. Parra, J. Lloret, and J. Tomás, "Smart system for children's chronic illness monitoring," *Information Fusion*, vol. 40, pp. 76–86, 2018.

[24] A. Rehman, K. Haseeb, T. Saba, J. Lloret, and U. Tariq, "Secured big data analytics for decision-oriented medical system using Internet of Things," *Electronics*, vol. 10, no. 11, p. 1273, 2021.

[25] M. Elhoseny, K. Haseeb, A. A. Shah, I. Ahmad, Z. Jan, and M. Alghamdi, "IoT solution for AI-enabled privacy-preserving with big data transferring: an application for healthcare using blockchain," *Energies*, vol. 14, no. 17, article 5364, 2021.

[26] S. Zeadally, F. Siddiqui, Z. Baig, and A. Ibrahim, "Smart healthcare: challenges and potential solutions using Internet of Things (IoT) and big data analytics," *PSU Research Review*, vol. 4, 2020.

[27] M. Pasha and S. M. W. Shah, "Framework for e-health systems in IoT-based environments," *Wireless Communications and Mobile Computing*, vol. 2018, 11 pages, 2018.

[28] X. C. Yin, Z. G. Liu, B. Ndibanje, L. Nkenyereye, and S. Riazul Islam, "An IoT-based anonymous function for security and privacy in healthcare sensor networks," *Sensors*, vol. 19, no. 14, article 3146, 2019.

[29] G. Kaur, P. Chanak, and M. Bhattacharya, "Energy efficient intelligent routing scheme for IoT-enabled WSNs," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11440–11449, 2021.

[30] M. Sadrishojaei, N. Jafari Navimipour, M. Reshadi, and M. Hosseinzadeh, "Clustered routing method in the Internet of Things using a moth-flame optimization algorithm," *International Journal of Communication Systems*, vol. 34, no. 16, article e4964, 2021.

[31] A. Hussain, T. Ali, F. Althobiani et al., "Security framework for IoT based real-time health applications," *Electronics*, vol. 10, no. 6, p. 719, 2021.

[32] S. Ramesh, T. Jayasankar, R. Bhavadharini, N. Nagarajan, and G. Mani, "Securing medical data using extended role based access control model and Twofish algorithms on cloud platform," *European Journal of Molecular & Clinical Medicine*, vol. 8, no. 1, pp. 1075–1089, 2021.

[33] H. M. Ali, J. Liu, S. A. C. Bukhari, and H. T. Rauf, "Planning a secure and reliable IoT-enabled FOG-assisted computing infrastructure for healthcare," *Cluster Computing*, pp. 1–19, 2021.

[34] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*, vol. 24, Springer, Berlin, 2003.

[35] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM Journal on Computing*, vol. 15, no. 2, pp. 364–383, 1986.