energies

MDPI

Article

Energy-Efficient IoT e-Health Using Artificial Intelligence Model with Homomorphic Secret Sharing

Amjad Rehman [1], Tanzila Saba [1], Khalid Haseeb [2], Souad Larabi Marie-Sainte [1] and Jaime Lloret [3,4,*]

[1] Artificial Intelligence and Data Analytics (AIDA) Lab, CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia; rkamjad@gmail.com (A.R.); drstanzila@gmail.com (T.S.); slarabi@psu.edu.sa (S.L.M.-S.)
[2] Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Pakistan; khalid.haseeb@icp.edu.pk
[3] Integrated Management Coastal Research Institute, Universitat Politecnica de Valencia, 46730 Valencia, Spain
[4] School of Computing and Digital Technologies, Staffordshire University, Stoke ST4 2DE, UK
* Correspondence: jlloret@dcom.upv.es

Abstract: Internet of Things (IoT) is a developing technology for supporting heterogeneous physical objects into smart things and improving the individuals living using wireless communication systems. Recently, many smart healthcare systems are based on the Internet of Medical Things (IoMT) to collect and analyze the data for infectious diseases, i.e., body fever, flu, COVID-19, shortness of breath, etc. with the least operation cost. However, the most important research challenges in such applications are storing the medical data on a secured cloud and make the disease diagnosis system more energy efficient. Additionally, the rapid explosion of IoMT technology has involved many cyber-criminals and continuous attempts to compromise medical devices with information loss and generating bogus certificates. Thus, the increase in modern technologies for healthcare applications based on IoMT, securing health data, and offering trusted communication against intruders is gaining much research attention. Therefore, this study aims to propose an energy-efficient IoT e-health model using artificial intelligence with homomorphic secret sharing, which aims to increase the maintainability of disease diagnosis systems and support trustworthy communication with the integration of the medical cloud. The proposed model is analyzed and proved its significance against relevant systems.

Keywords: health system; artificial intelligence; inflectional diseases; energy efficiency; homomorphic secrets

Citation: Rehman, A.; Saba, T.; Haseeb, K.; Larabi Marie-Sainte, S.; Lloret, J. Energy-Efficient IoT e-Health Using Artificial Intelligence Model with Homomorphic Secret Sharing. *Energies* **2021**, *14*, 6414. https://doi.org/10.3390/en14196414

Academic Editors: Jaume Segura-Garcia and Santiago Felici-Castell

Received: 21 August 2021
Accepted: 4 October 2021
Published: 7 October 2021

1. Introduction

Internet of Things plays a vital role in information gathering with the help of battery-powered sensors and transmits the patients' data to end-users [1–3]. Currently, they are collaborating with computing devices to diagnosis different inflectional diseases and issues of public health such as typhoid, malaria, blood pressure, etc. [4–6]. These are biosensors that can collect health-related data from any implanted surgical device, wearable bands, mobile device, etc. However, these biosensors are very limited in terms of battery power, transmission power, storage, and processing units, so their efficient utilization is one of the common factors for improving any medical system. Many solutions have been presented to initially analyze the medical symptoms using constraint-oriented IoMT biosensors and support different services on emergency cases [7–9]. These medical sensors are directly communicated with a local coordinator and further collaborate with sink nodes to send health data to the public cloud [10–12]. However, the management of healthcare resources efficiently with the slower response time from medical experts is one of the critical research challenges. Additionally, medical systems are more sensitive to data compromise and illegal attempts on medical data and gain significant interest from the research community [13,14]. Since medical data is based on tier structure [15,16] and

flooded on free access medium, IoMT technology often deals with malicious machines, and ongoing health records are easily accessible to intruders. Therefore, this research work presented a lightweight, trustworthy, and efficient health model for the maintainability of disease diagnosis systems using artificial intelligence. It not only utilizes the heuristics and gradually reaches the goal state with nominal overhead on IoMT infrastructure but also leads to secured routing using homomorphic secret sharing. The proposed artificial intelligence heuristic decision balances the energy load and decreases communication overheads while communicating smart healthcare technologies. It significantly offers intellectual performance over the public network and increases the transmissions reputation of medical detection systems. Moreover, it establishes trust among peer medical sensors and avoids unauthorized access to medical data. In the security component, the proposed model utilizes strong cryptosystems to protect the health care system from malicious nodes and increases the reliable transmission among edge network and sink nodes.

The fundamental objectives of our proposed model are:

i. To develop a best first search (BFS) based artificial intelligence heuristic algorithm using IoMT. It supports data fitness and stability for IoT communication.
ii. To develop a trusted algorithm for finding harsh actions on real-time IoMT data and enhance the sureness level in an unreliable and unpredictable situation.
iii. To develop a security algorithm using cryptosystems and ensure to support online protection for health data against interferences.

The rest of the research article is organized as follows. Section 2 discusses the related work and problem findings. Section 3 presents the main components of the proposed model. Section 4 shows the analysis of the performance of the proposed model in the comparison to other solutions. In the end, Section 5 concludes the paper.

2. Related Work

The wireless networks [17–19] are integrated with various physical objects and small sensors to gather data either on an event-by-event or continuous basis. The systems are self-configuring and scalable in terms of multiple tools. The collected data is redirected via different switching nodes to the sink node, where all linked end-users can reach it. In contrast to other ad hoc network architecture, sensor nodes are installed at random and their locations are not pre-planned. They are helpful for various industrial, healthcare, military, agricultural, and smart applications, but the sensor nodes are limited in terms of energy, control, and transmission. One of the most critical activities in an intelligent city is retrieving the various parameters involved in multiple control systems. Transportation, energy storage, air conditioning, and other applications are examples of these types of processes. Controlling the air quality in smart cities, on the other hand, stands out as a crucial problem because it has profound health implications, rendering environmental sensing a critical challenge and an effective service [20,21]. Wireless body area network (WBAN) [22,23] is a new technology that can be used in many areas, including healthcare, emergency management, remote medical care, and sports, entertainment, and consumer electronics. WBAN connects many medical sensors and machines through wireless links to help the healthcare industry handle patient data. These tiny sensors, which are ultra-low power, emit harmless radiations, are intelligent and lightweight, and track and collect medical data to send to a coordinator using low-power RF technology. The data is then sent to a central location to be analyzed and implemented. The call centers and doctors used IoMT instruments to access the sensed data and handle the patients accordingly. The sensed data in WBAN applications are biological signals, such as blood pressure, ECG, pulse, sugar level, and so on, which require immediate medical attention. As a result, such systems usually demand low latency and high data reliability.

Due to the huge collection of health data, disease diagnosis systems need a high degree of data processing and analysis to facilitate medical science. Recently, many edge-based solutions [24–26] are proposed that are integrated with medical technologies and

improving energy efficiency. The IoMT nodes may be installed separately at the base, such as at home, clinic, or hospital, where medical data must be monitored [27,28]. These edge health nodes now have a complete OS supporting the edge CPU and graphics processing unit (GPU). This system enables edge nodes to conduct high-cost deep learning-based computations, particularly in the medical system. Many studies have recently concentrated on working with inflectional diseases and safely transferring them to medical centers to gain personal protection and authentication. Since the gathered data is more vulnerable and can be used by intruders to make false medical statements, authentication is also a significant factor in preventing unauthentic access [29,30]. In [31], authors suggested a dual sink solution for body area networks (DSCB) using clustering, to achieve effective and secure connectivity while still being energy efficient. Based on clustering approaches with dual sink nodes, it extends the network lifespan. The data forwarder node is chosen using a cost function that considers residual capacity, distance from the sink node, and transmission power parameters. It contrasted itself with previous work and showed improved network throughput, data delay, and network reliability. Authors in [32] suggested attribute-based encryption (ABE) authentication scheme for medical applications at the network layer in HetNets to authenticate the data requester. This security protocol assists in the defense of sensitive information from intruders. Capturing the intruders also cuts down on communication costs. Their results, which were confirmed in AVISPA, demonstrated improved data protection and privacy in the face of intrusion attacks. In [33], the authors suggested an algorithm for protecting personal identity by combining cluster principles with access control policies. This algorithm has been successfully applied to data exchange and knowledge collection in clusters while protecting individual identity. Compared to current machine learning algorithms, the highest number of clusters creation took the least amount of time. Compared to OKA and K member algorithms, the second proposed algorithm has lost the least detail. The protection of the patient's data is greatly improved as a result of these performances. Security risk analysis and effective coordination efficiency are also recent issues in medical and healthcare systems. Because of the problem of unbalanced energy consumption, IoMT sensors can slow down data transmission to remote data centers. The authors of [34], proposed a smart edge-based health system, which aims to minimize the system latency and increases energy efficiency. It also optimizes the service in the delivery of medical data. It formulates a multi-objective optimization framework, which provides an edge node for the adjustment of compression parameters and chooses the optimal radio access. The experimental results have proven that the proposed system saving energy resources and improving the delivery time than other solutions. In [35], the authors created a medical diagnosis humanoid (MDH). This low-cost, high-reliability mobile robotic device conducts a full diagnostic test to decide whether or not a person is contaminated with COVID-19. Their methodology focuses on creating an artificial intelligence-based system for medical research, in which humanoids can navigate to desired destinations, diagnose an individual for COVID-19 using various parameters, and conduct a locality survey for the same. The humanoid uses several sensors in the field to provide real-time data sensing and analysis through machine learning. Lin et al. [36] proposed a revised privacy-enhanced data fusion approach (PDFS) to overcome these medical and healthcare-related issues. The four main components of the proposed PDFS are sensitive task description, work fulfillment estimation, reward mechanism-based task contract architecture, and homomorphic encryption-based data fusion. Extensive simulation studies show that PDFS can boost the privacy security for data fusion in COVID-19 application environments based on IoMT while achieving high task classification precision, task completion rate, task data reliability, and task participation rate as well as a low average error rate. Using the trusted platform module, the authors suggested a group cloud architecture in an IoMT environment that guarantees end-to-end security and avoids many of the current negative aspects [37]. Authors in [38] proposed a configurable, reliable, and confidential distributed data storage scheme, which aims to encrypt the data and controlling the computing processes. It utilizes the redundant residue

number system (RRNS) with the new functions for secret sharing and error control. It offers the concept of an approximate value of a rank of a number (AR) that explicitly decreases the computational complexity and size of the coefficients. The theoretical analysis has proven that the proposed scheme supports not only enhancing reliability, and reducing the data storage overheads, but also offering data encryption. In [39], the authors proposed a secure K-NN, which aims to offer privacy-preserving K-NN training for IoT networks. It uses the concept of a Blockchain technology integrated with a partial homomorphic cryptosystem (PHC) known as Paillier to save all applicants with data security. It securing the IoT data that is receiving from various providers and maintains the data integrity. The proposed solution significantly increases the efficiency and security as compared to other solutions. The authors in [40], proposed an energy-efficient approach for the collection and analysis of IoT data. It applied a fast error-bounded lossy compressor on the collected IoT data before its transmission and decreases the ratio for high energy consumption. Moreover, it offers the transmission of data on an edge node and executes the supervised machine learning techniques. The experimentation results have proven that the ratio of transmitted data is improved without compromising the quality of medical data. Table 1 illustrates the summary of the related work.

Table 1. Summary of related work.

Comparative Approaches	Contributions and Research Challenges
Existing work	• Unlike traditional communication systems, IoMT-based communication is more adaptive and prone to failure due to the involvement of the public and uncontrolled communities over the Internet. • Due to limited resources for medical sensors, energy-saving and maintaining the communication nominal response time are significant parameters. • Moreover, as medical sensors are participating on an open medium such as the Internet, they are subject to increased cybercrimes and medical malpractice rights. • In recent years, improving the energy efficiency and security of disease diagnosis systems using lightweight processing power and easy access to medical data are some other demanding tasks.

3. Proposed Model

This section presents the detail of the proposed model with along all the developed components. Our proposed model is comprised of two main components. Figure 1 depicts a block diagram of the proposed model. In the first component, we utilize the heuristic technique to flow the medical information to its goal state with lower communication breakage and time. Initially, the medical nodes are structure in undirected graph G with edge E. Each edge is assigned to a particular score and its value is updated whenever any changes arise in-network or nodes status. This component also ensures to lower the traffic in the specific route to flow the medical data and offers delivery of medical data using network edges. In the second component, the proposed model first establishing trust among the chain of IoMT nodes and increases the trustworthiness in transmitting the medical records. Such a component eliminates the involvement of malicious devices to be part of transmitting the medical data. Secondly, it also provides the services of securing the sensitive information of inflectional diseases from leakage and unauthentic permission over insecure routes. The following are few network assumptions that consider in the development of the proposed model in a realistic environment.

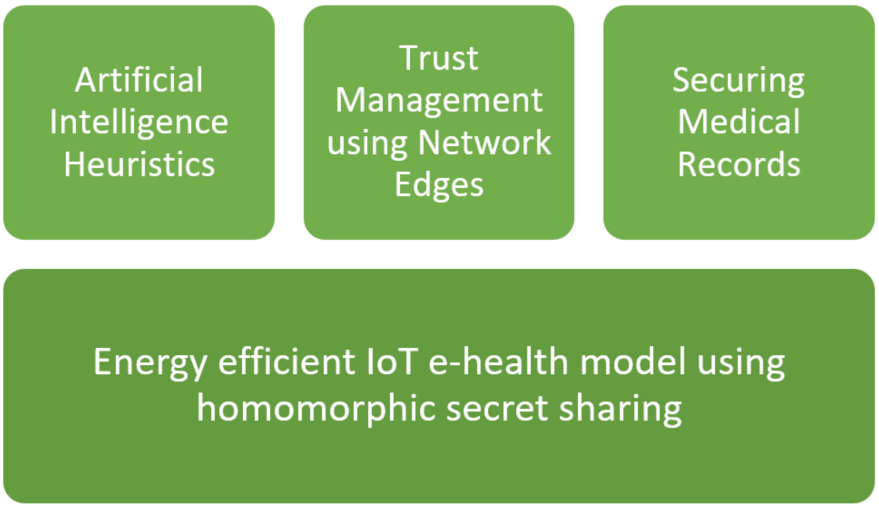


Figure 1. Block diagram of the proposed model.

i. The medical sensors are constraint-oriented devices with embedded global positioning system (GPS).
ii. Network edges are mobile, can interact with both medical sensors and the sink node.
iii. Network edges and sink nodes are robust with high computing resources.
iv. Nodes can set the neighbor table using position coordinates.
v. Malicious machines are deployed for redirecting the health data or flood false data packets on request.

The proposed model exploits the undirected graph G and executes the greedy BFS algorithm to accomplish the route optimization for medical applications. The undirected graph G acts as a search zone to route the medical data from the source state to the sink node with an optimal forwarding system. Additionally, the proposed model distributes network edges to minimize the nodes' load and latency in sending the data from the lower layer of medical application to the user layer. Firstly, it initiates the process of greedy BFS from the source node towards network edges and later network edges communication with the sink node. If the distance from network edges and sink nodes is greater than a certain threshold, then the proposed model utilizes a neighbor discovery scheme. Thus, unlike most of the current work, the proposed model improves the forwarding system of medical applications and reaches the goal state with the management of minimum communication overhead and cost.

Furthermore, it utilizes the score of network edges $f(n)$ and introduces artificial intelligent heuristics. The proposed model is comprised of two states, i.e., Verified and Unverified. All the computed neighbors are included in Verified state S and those neighbors that have not been evaluated yet are included in Unverified state S'.

Let us consider that source node i need to send to data to the network edge n_{edges}. To initiate this process, the source executes the neighbor discovery scheme that aims to explore the optimal subset of neighbors n_i among nodes N. Additionally, the neighbor discovery scheme arranges the n_i in a particular queue using their priority ID. The queue is updated when any changes incur in the network or nodes' attributes. Equation (1) defines the formulation of nodes' queue $N(Q)$.

$$N(Q) = max \sum_{i=i}^{k} n_i \quad (1)$$

where $n_i \; \varepsilon \; N$

In neighbor discovery scheme, the computation of $f(n)$ performs a vital role in optimizing network performance and delivering the medical data on time to response centers. The $f(n)$ exploring the minimum number of neighbor nodes in such a manner to least the

number of hops and reducing the latency factor using heuristic $h(n)$. Each node computes its heuristic value using $h(n)$ and share the computed value in their proximity. In the proposed model, $h(n)$ value is comprised of distance d, and delivery time t_d. Equation (2) defines the computation of heuristics $h(n)$.

$$h(n) = d + t_d \tag{2}$$

The value of d is the integration of distance of source node i to a neighbor n_i as denoted by d', the distance of neighbor to network edges $edge_i$ as denoted by d_edge and mobility ratio of network edge $edge_m$, as defined in Equation (3).

$$d = {}^{1}/_{(\,d' + d_{edge} + edge_m)} \tag{3}$$

Additionally, the computation of t_d is based on the delaying time and fluctuation in data receptions d_{recp}. The proposed model set a threshold to identify the strong s and weak w transmission channel c, as defined in Equation (4).

$$\begin{cases} if\ d_{recp} > threshold \\ then\ c = s,\ else\ \ c = w \end{cases} \tag{4}$$

The network edges maintain a table T for all its neighbor *sensors* to identify the malicious traffic and further collaborate with sink node to attain privacy for medical data. In the proposed model, network edges utilize the homomorphic secret sharing (HSS) scheme and divide the secret key X into different pieces x_i [41]. Each piece is distributed to individual nodes such that each node $x_i\ \varepsilon\ T$. All the shares are mathematical hidden actual secret key X from malicious nodes. The secret must be split in such a manner when all or any k subset of shares are combined to recover the actual secret information X. Each node can use its homomorphic secret to encrypt the health data as defined in Equation (5).

$$E(m) = m_i \oplus x_i \tag{5}$$

Moreover, the encrypted data is mapped with digital hashes to network edges as defined in Equation (6).

$$C = E(m_i) + E(m_{i+1}) + \ldots + E(m_k) \tag{6}$$

Upon receipt, network edges combine all the pieces x_i to construct the actual secret information as define in Equation (7). When it recovers the actual secret, it ensures the authenticity of incoming medical data from the sensors layer. The network edges further collaborate with the sink node to transmit the medical record.

$$X = \sum_{i=0}^{k} x_i \tag{7}$$

RSA cryptosystem [42] is utilized among network edges and sink node to transmit medical records as defined in Equation (8).

$$E_k(D_i) = {D_i}^e\ mod\ n \tag{8}$$

Upon receiving the medical data, the sink node performs the decryption function defined in Equation (9) and obtains the medical data. Later, the data is stored in the response center and medical experts analyze the disease with appropriate treatment.

$$D \equiv {E_k}^d\ mod\ n \tag{9}$$

Figure 2 illustrates the flow chart of the proposed model. It consists of the development of initiate routes, determining heuristics, data mapping, secret shares, data encryption, and hash mapping components. In the beginning, it establishes the initial routes for

the forwarding of data to network edges and from the network, edges to sink nodes. It determines the score using heuristics and split the nodes either into two states. It initiates the process of neighbor discovery and at the time of data routing, it selects the most optimal ones. Moreover, the optimal nodes are readjusted using network dynamics and inform the neighbors about the current state. Afterward, the network data is routed on the selected nodes until it is successfully arrived at the sink node by utilizing network edges. The network edges make use of the homomorphic secret sharing scheme for the generation and distribution of secrets among nodes and securing the process of data encryption. Moreover, the chain of encrypted data is constructed using the technology of hash mapping which gives the hard and complex computation for attackers to recover the actual data. In the end, sink nodes offer a high-level security approach to protect the shared data with various application users.

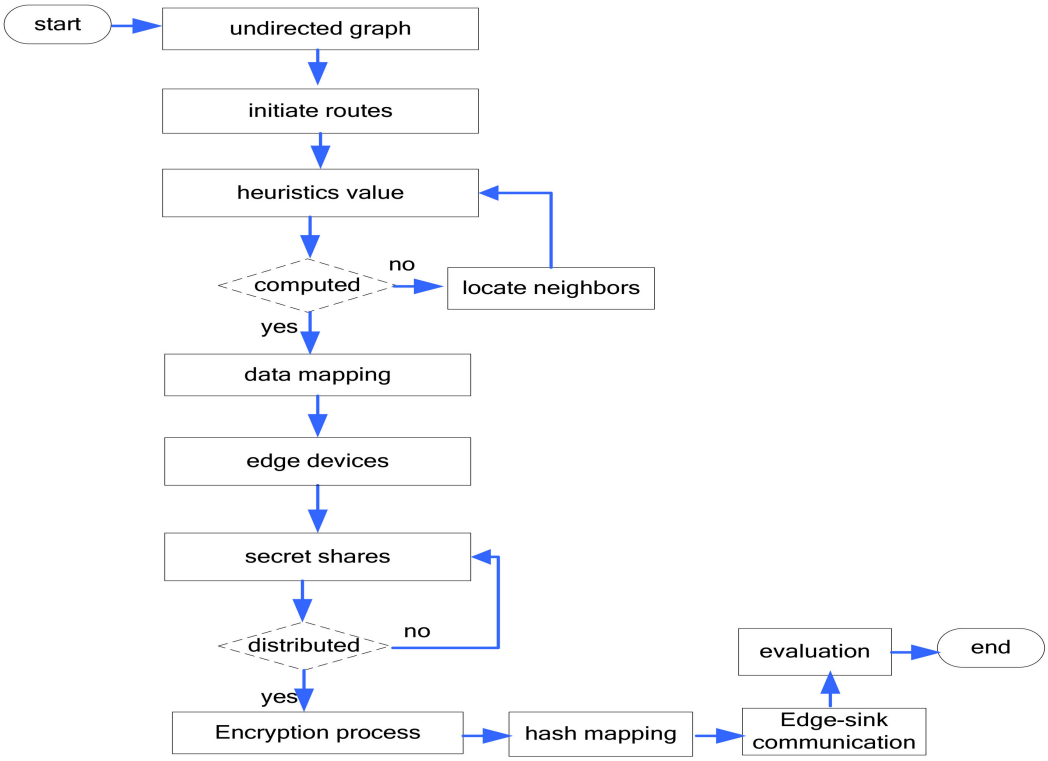


Figure 2. Flow chart of the proposed model.

4. Performance Analysis

In this section, we present the performance analysis of the proposed model using simulations. An object-oriented network simulation software NS-3 [43] is used to build the scenario in the Ubuntu platform. Our proposed model utilizes the WBAN topology that is comprised of wearable and implanted sensors inside the human body. These sensor nodes collecting the monitor physiological factors of the human body, i.e., blood pressure, glucose level, flu, fever, etc. The number of sensors nodes is varying from 25 to 125. Each node has fixed a transmission radius of 3m. The size of data packets is set to 64 bits. Initially, the energy level of all the sensor nodes is set to 2j. The simulation is executed for the duration of 1000s. We deployed the 10 malicious nodes randomly and at different locations. The number of sensor nodes is set from 25 to 125. The network edges are varying in the range of 3 to 15 and moving with a speed of 1 to 5 m/s in a fixed radius. Table 2 illustrates the parameters for simulating the proposed model.

Table 2. Simulation parameters.

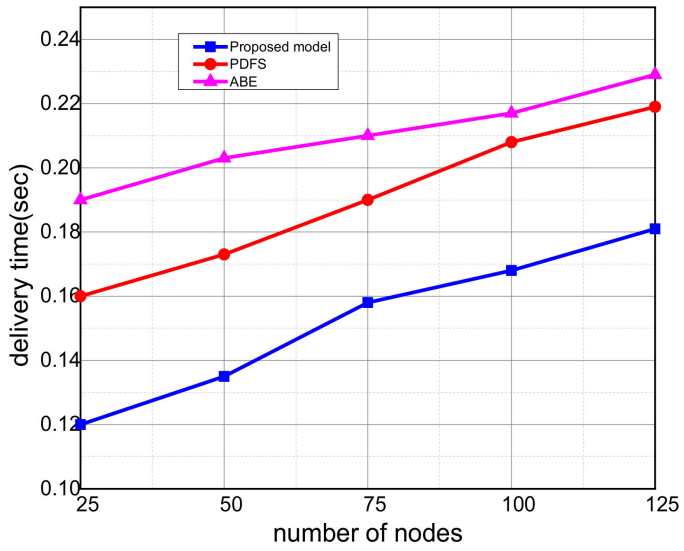
Parameters	Values
Initial energy	2j
Sensors	25 to 125
Deployment	Random
Malicious nodes	10
Data flow	CBR
Nodes transmission range	3 m
Medical sensors	100
Packet size	64 bits
Simulation time	1000 s
Initial energy	2j
Network edges	3 to 15
Speed of network edges	1 to 5 m/s

Experiments

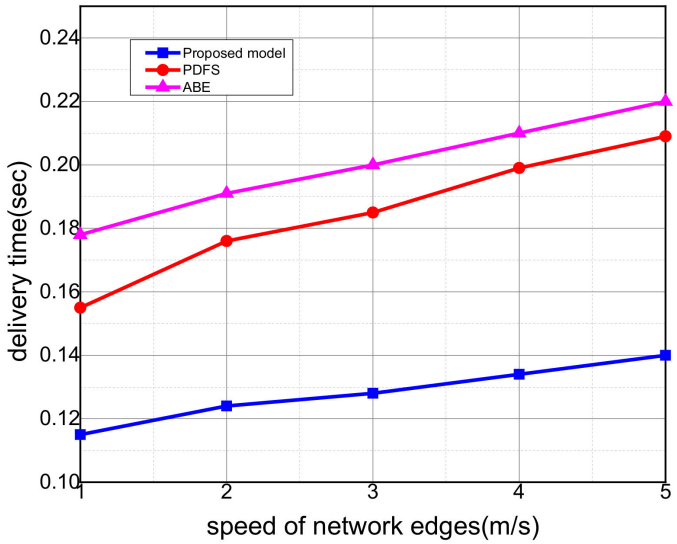
In this section, the performance of the proposed model is compared with other solutions. The experiments are done in terms of energy consumption, packet drop ratio, delivery time, and data leakage. The simulation data is recorded in the trace file and later it is utilized to evaluate the performance of network metrics. The performance results are tested in two different scenarios varying the number of network nodes and the varying speed of network edges. The comparison evaluation is based on the proposed model, ABE [32] and PDFS [36].

Figure 3a,b illustrate the performance of the proposed model in terms of delivery time. It is observed that the proposed model improved the efficacy of data latency by 13% and 15% in the comparison of the existing solutions. It is due to the involvement of the multi-hop model instead of direct communication. Additionally, the generated routes are based on the heuristic value which is comprised of quality-aware parameters. During computation of heuristics, the longer routes are eliminated from the choices and shortest with high delivery ratio channels are included. Thus, the utilization of mobile network edges performs a vital role in decreasing the delivery time in forwarding data of medical applications. In the proposed model, the network edges provide the bridging facility among medical sensors and sink nodes and maintain the structure of associated nodes in its local database, which keeps track of established routes for medical records.

In Figure 4a,b, the proposed model is compared with an existing solution in terms of packet drop ratio. It is seen that the proposed model improves the efficacy of the packet drop ratio by 19% and 21% in the comparison of existing work. It is due to that unlike PDFS and ABE, the proposed model utilizes the most capable and reliable forwarders to carry the medical record towards emergency centers. The proposed model supports a more optimal way using a greedy BFS algorithm to extract the long-run routing path from the source state to the sink node. Thus, it decreases the ratio of data loss and interruption due to fluctuation of link damages as the data rate increases. It is also observed that, unlike PDFS and ABE schemes, the proposed artificial intelligence heuristics avoid selecting damage routes for health records and decreasing the frequency of data re-transmission. In the proposed model, the network edges act as a controller for the nodes that reside in its proximity and efficiently reduce the packet loss ratio. Furthermore, due to optimum heuristics, the proposed model denies the data for forwarding on highly congested routes. Ultimately, it increases the significance of IoMT technology in a fault-tolerant manner.



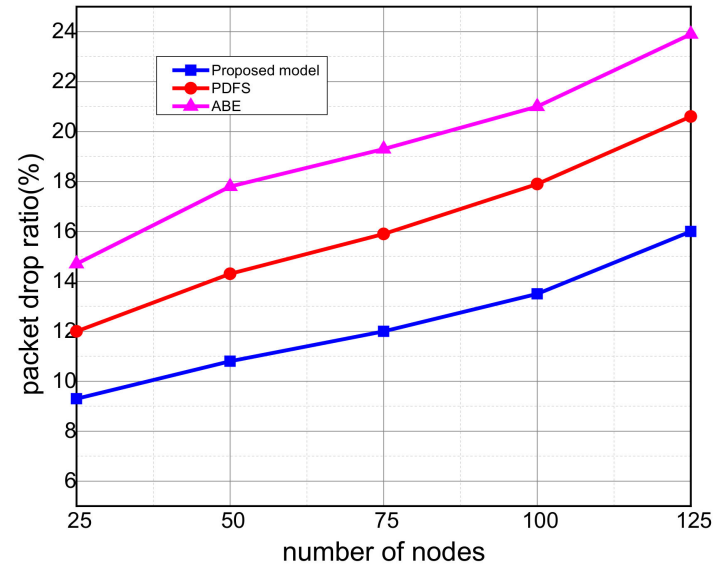
(**a**) Comparison under a varying number of nodes



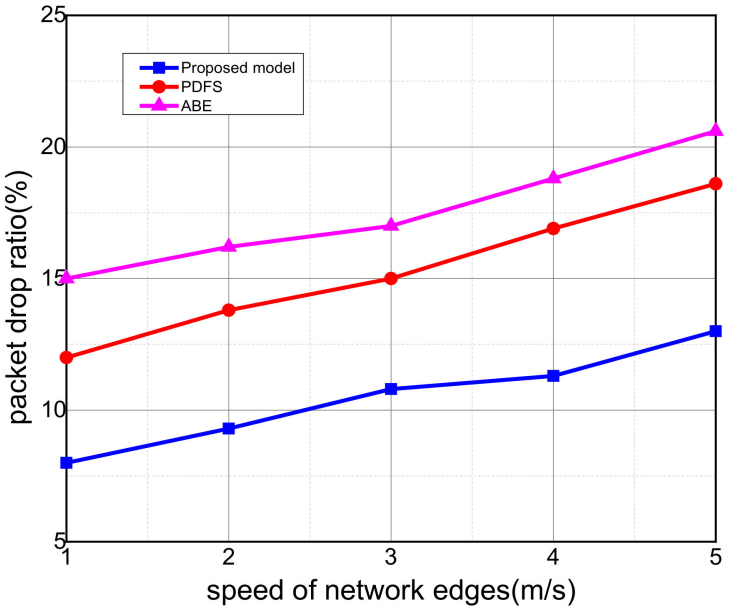
(**b**) Comparison under the varying speed of network edges

Figure 3. Evaluation of delivery time among proposed model, PDFS, and ABE.

In Figure 5a,b, the performance result of the proposed model against existing solutions is illustrated in terms of energy consumption per round. It is seen that the proposed model improves the energy consumption per round by 16% and 18% under a varying number of network edges and their variable speed. Previously, it was seen that with time, the number of packets drop ratio is also increasing by the proposed model. This was due to the exchange of high control messages and congestions in the presence of malicious sources. However, it is observed that the proposed model decreases the ratio of energy consumption among IoT nodes due to the use of artificial intelligence heuristics and extracting the optimal cost for the forwarding of medical records. Furthermore, various factors in the transmitting the data for medical application manages the network resources efficiently without overloaded the additional energy consumption. Moreover, it generates and maintains more reliable and long-run data transportation forwarders based on the update status of the network. Accordingly, it moves towards optimum decision gradually with the integration of network edges until the goal state is achieved. Such an approach explicitly decreases the load on sensors and increases the strength of healthcare systems.



(**a**) Comparison under varying network of nodes

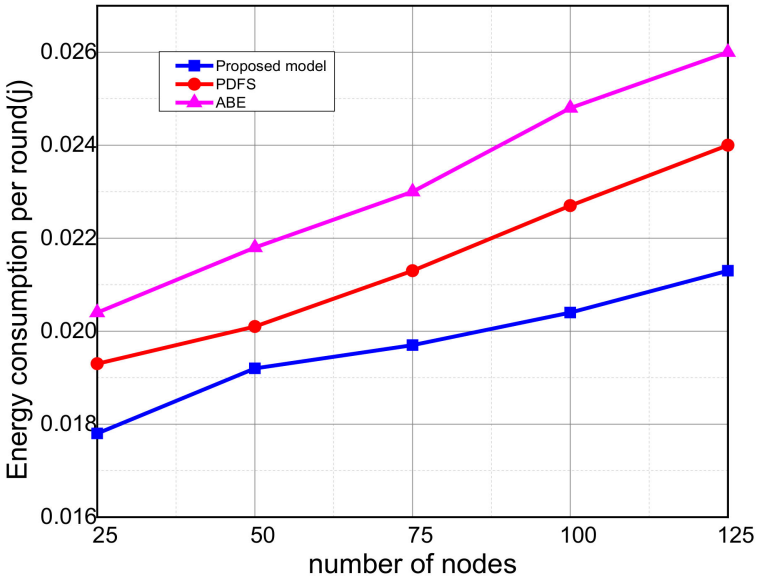


(**b**) Comparison under the varying speed of network edges

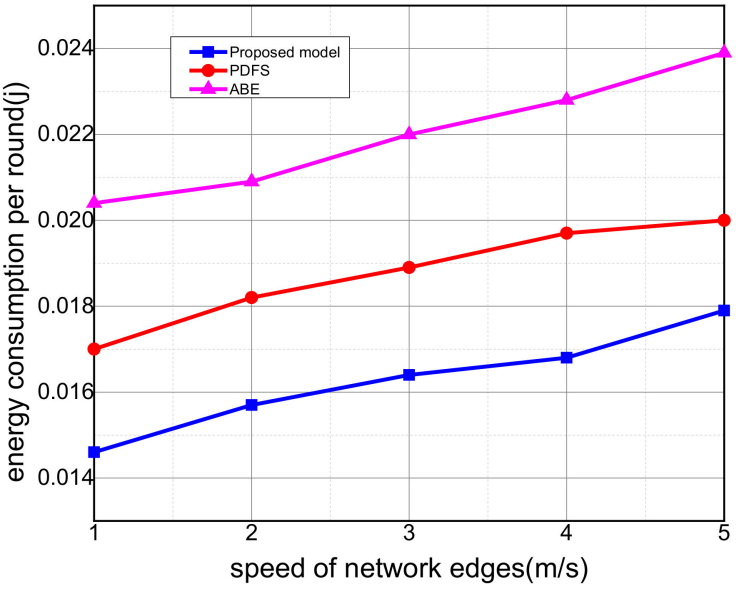
Figure 4. Evaluation of packet drop ratio among proposed model, PDFS, ABE.

In Figure 6a,b, it is noticed that the proposed model utilizes the energy resources of individual nodes efficiently by 21% and 28%, unlike other solutions. It determines the optimal value for the selection of neighboring nodes and minimizes the communication distance. In forwarding the data, the source node only considers the distance status but it is considered the mobility factor and attain a reliable state. Additionally, is the proposed model, generates the secret parts using HSS and makes it hard for a malicious node to flood enter the proximity of the network. Accordingly, it decreasing the reception ratio of normal nodes to receive the bogus packet and facilitate it. Such a method decreases the additional energy consumption on the level of the nodes and improves the efficiency of the IoT network. Moreover, it achieves the data load on mobile edges rather than normal nodes and increases the energy efficiency by excluding the false data packet for re-transmitting the medical data based on the trustworthy system.

Figure 7a,b demonstrate the performance analysis of the proposed model against other solutions in terms of data breaches. It is seen that the proposed model significantly improves the detection of data breaches by 12% and 14% than existing solutions. It is due to that the proposed model makes use of homomorphic secret sharing among medical sensors and gives severe time to malicious nodes for the recovering of actual secret. Additionally, the medical sensors perform data encryption functions using homomorphic secret share and forward the map of the data in hashing until it receives at network edges. It increases the trust value among neighbors and does not compromise the health records. Moreover, network edges and sink node utilizes the RSA cryptosystem to offer high-cost security mapping against unauthorized access.

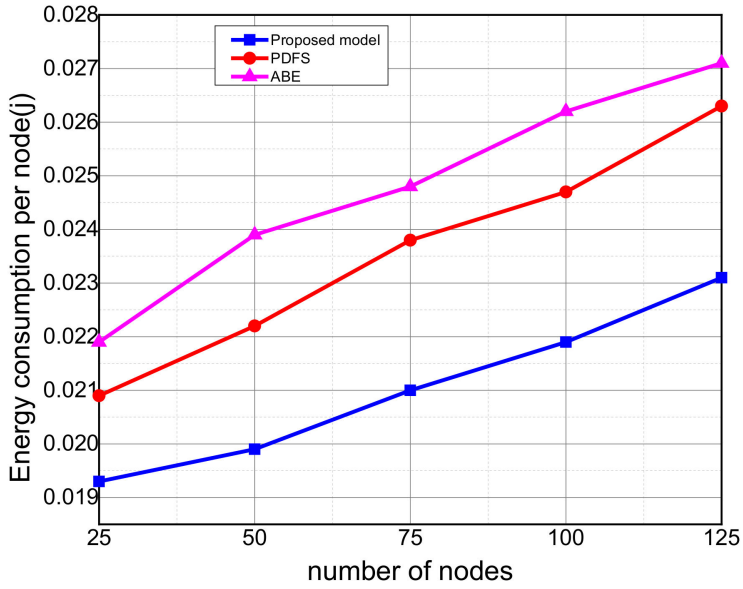


(**a**) Comparison under a varying number of nodes

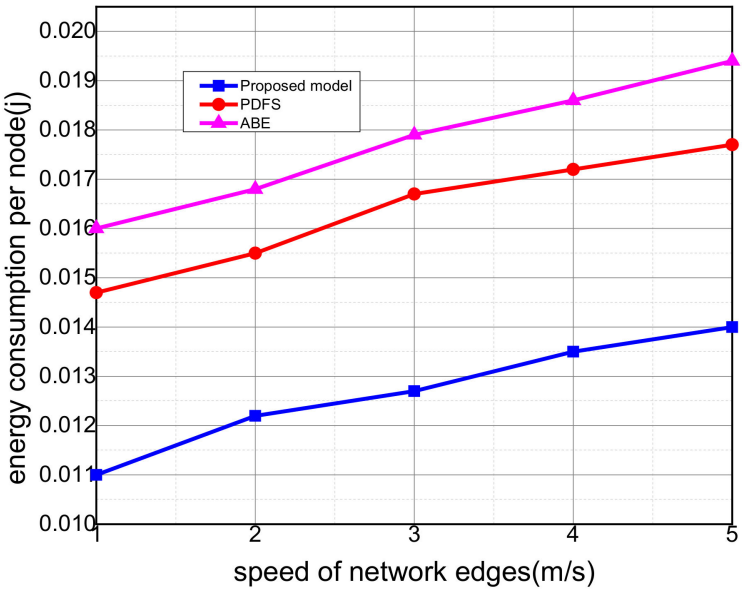


(**b**) Comparison under the varying speed of network edges

Figure 5. Evaluation of energy consumption among proposed model, PDFS, ABE.

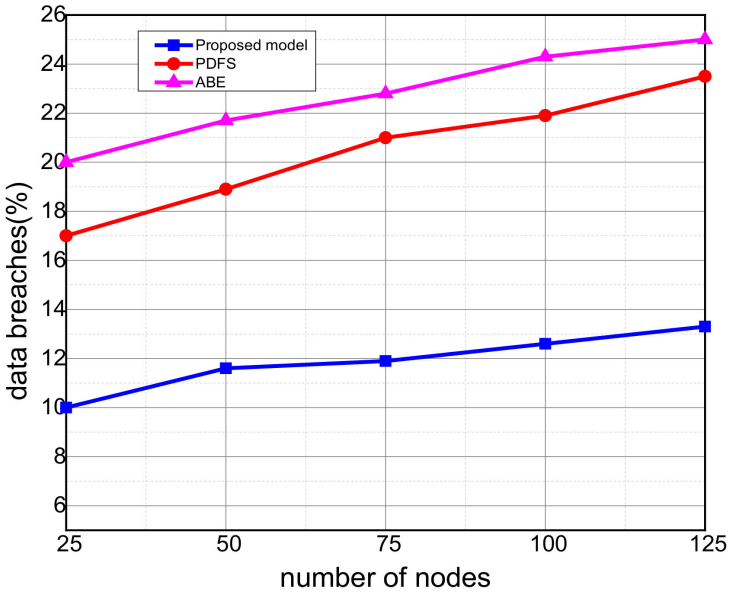


(**a**) Comparison under a varying number of nodes

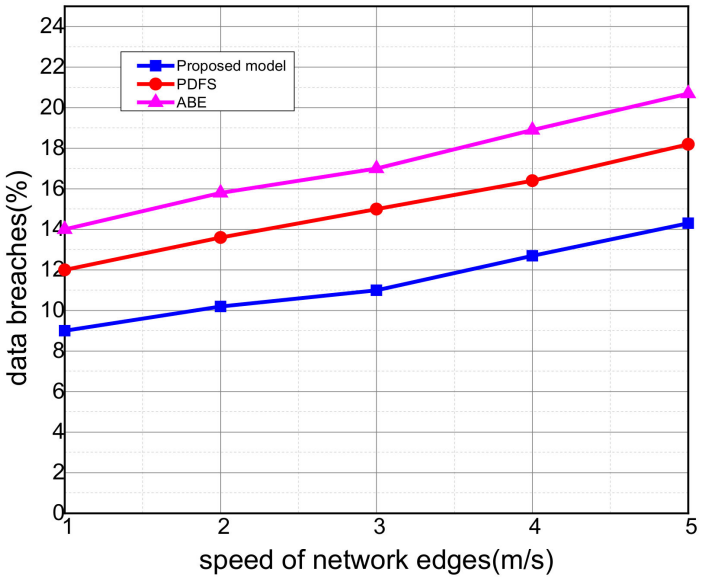


(**b**) Comparison under the varying speed of network edges

Figure 6. Evaluation of energy consumption per node among proposed model, PDFS, ABE.



(**a**) Comparison under a varying number of nodes



(**b**) Comparison under the varying speed of network edges

Figure 7. Evaluation of data breaches among proposed model, PDFS, ABE.

5. Conclusions

We present an energy-efficient IoT e-health model using artificial intelligence with homomorphic secret sharing, which aims to improve the data transferring in medical applications with energy-saving and reliability. The proposed model utilized the artificial intelligence heuristics to determine the lower cost forwarded to map the medical data using smart devices. The technology of IoMT gained a lot of research interest to identify illegal interactions of malicious machines and avoid compromising the data of medical applications. It ensures trust among medical nodes by distributing secret pairs using a homomorphic scheme and attains data privacy with authorized access. Furthermore, the multi-hop hashing mapping makes it very hard for intruders to affect the integrity of data blocks. Additionally, the RSA cryptosystem securing the medical records from network edges to sink node without the involvement of high computations on medical sensors.

However, it is seen from the experimental results that the proposed model still facing an increased packet drop ratio in the presence of high network load and uneven energy consumption among IoT nodes. Furthermore, it lacks the intelligence to avoid packets collision rate when the speed of edge nodes is increased. Therefore, in the future, we aim to introduce transfer learning, a machine learning approach to train the developed model for particular processes and reduces the usage of network resources for medical systems with consistent behavior.

Author Contributions: Conceptualization, A.R., K.H.; methodology, A.R., T.S.; software, A.R., K.H.; validation, J.L., S.L.M.-S., T.S.; formal analysis, A.R., S.L.M.-S.; investigation, J.L., K.H., T.S.; resources, A.R., T.S.; data curation, J.L.; writing—original draft preparation, A.R., K.H.; writing—review and editing, K.H., J.L.; visualization, T.S., S.L.M.-S.; supervision, A.R., J.L.; project administration, A.R., J.L.; funding acquisition, A.R. All authors have read and agreed to the published version of the manuscript.

Funding: Prince Sultan University, Riyadh Saudi Arabia, (SEED-CCIS-2021{85}) under Artificial Intelligence & Data Analytics Research Lab. CCIS.

Data Availability Statement: All needed data is inside the manuscript.

Acknowledgments: This work was supported by the research project "A secure and efficient healthcare model using internet of medical things for COVID-19 pandemic" Prince Sultan University, Riyadh Saudi Arabia, (SEED-CCIS-2021{85}) under Artificial Intelligence & Data Analytics Research Lab. CCIS". Authors are thankful for the support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wu, J.; Xie, X.; Yang, L.; Xu, X.; Cai, Y.; Wang, T.; Xie, X. Mobile health technology combats COVID-19 in China. *J. Infect.* **2021**, *82*, 159–198.
2. Rghioui, A.; Sendra, S.; Lloret, J.; Oumnad, A. Internet of things for measuring human activities in ambient assisted living and e-health. *Netw. Protoc. Algorithms* **2016**, *8*, 15–28. [CrossRef]
3. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Ahmed, Z. Mobility Support 5G Architecture with Real-Time Routing for Sustainable Smart Cities. *Sustainability* **2021**, *13*, 9092. [CrossRef]
4. Aman, A.H.M.; Hassan, W.H.; Sameen, S.; Attarbashi, Z.S.; Alizadeh, M.; Latiff, L.A. IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. *J. Netw. Comput. Appl.* **2021**, *174*, 102886. [CrossRef] [PubMed]
5. Ali, S. Combatting against COVID-19 & misinformation: A systematic review. *Hum. Arenas* **2020**, 1–16. [CrossRef]
6. Haseeb, K.; Saba, T.; Rehman, A.; Ahmed, I.; Lloret, J. Efficient data uncertainty management for health industrial internet of things using machine learning. *Int. J. Commun. Syst.* **2021**, *34*. [CrossRef]
7. Pustokhina, I.V.; Pustokhin, D.A.; Gupta, D.; Khanna, A.; Shankar, K.; Nguyen, G.N. An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. *IEEE Access* **2020**, *8*, 107112–107123. [CrossRef]
8. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of medical things security assessment framework. *Internet Things* **2019**, *8*, 100123. [CrossRef]
9. Parra, L.; Rocher, J.; Sendra, S.; Lloret, J. An Energy-Efficient IoT Group-Based Architecture for Smart Cities. In *Energy Conservation for IoT Devices*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 111–127.
10. Xu, X.; Huang, Q.; Zhang, Y.; Li, S.; Qi, L.; Dou, W. An LSH-based offloading method for IoMT services in integrated cloud-edge environment. *ACM Trans. Multimed. Comput. Commun. Appl.* **2021**, *16*, 1–19. [CrossRef]
11. Mohiyuddin, A.; Javed, A.R.; Chakraborty, C.; Rizwan, M.; Shabbir, M.; Nebhen, J. Secure Cloud Storage for Medical IoT Data using Adaptive Neuro-Fuzzy Inference System. *Int. J. Fuzzy Syst.* **2021**, 1–13. [CrossRef]
12. Rehman, A.; Haseeb, K.; Saba, T.; Kolivand, H. M-SMDM: A model of security measures using Green Internet of Things with Cloud Integrated Data Management for Smart Cities. *Environ. Technol. Innov.* **2021**, *24*, 101802. [CrossRef]
13. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of security and privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019.
14. Saba, T.; Haseeb, K.; Shah, A.A.; Rehman, A.; Tariq, U.; Mehmood, Z. A Machine-Learning-Based Approach for Autonomous IoT Security. *IT Prof.* **2021**, *23*, 69–75. [CrossRef]
15. Bakhsh, S.T. Multi-tier mobile healthcare system using heterogeneous wireless sensor networks. *J. Med Imaging Health Inform.* **2017**, *7*, 1372–1379. [CrossRef]
16. Yin, H.; Jha, N.K. A health decision support system for disease diagnosis based on wearable medical sensors and machine learning ensembles. *IEEE Trans. Multi-Scale Comput. Syst.* **2017**, *3*, 228–241. [CrossRef]

17. Haseeb, K.; Islam, N.; Saba, T.; Rehman, A.; Mehmood, Z. LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. *Sustain. Cities Soc.* **2020**, *54*, 101995. [CrossRef]
18. Rahman, G.M.; Wahid, K.A. LDAP: Lightweight Dynamic Auto-Reconfigurable Protocol in an IoT-Enabled WSN for Wide-Area Remote Monitoring. *Remote Sens.* **2020**, *12*, 3131. [CrossRef]
19. Mehmood, A.; Lv, Z.; Lloret, J.; Umar, M.M. ELDC: An artificial neural network based energy-efficient and robust routing scheme for pollution monitoring in WSNs. *IEEE Trans. Emerg. Top. Comput.* **2017**, *8*, 106–114. [CrossRef]
20. Alvear, O.; Calafate, C.T.; Cano, J.-C.; Manzoni, P. Crowdsensing in smart cities: Overview, platforms, and environment sensing issues. *Sensors* **2018**, *18*, 460. [CrossRef]
21. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Tariq, U. Secured Big Data Analytics for Decision-Oriented Medical System Using Internet of Things. *Electronics* **2021**, *10*, 1273. [CrossRef]
22. Cavallari, R.; Martelli, F.; Rosini, R.; Buratti, C.; Verdone, R. A survey on wireless body area networks: Technologies and design challenges. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1635–1657. [CrossRef]
23. El Atrash, M.; Abdalla, M.A.; Elhennawy, H.M. A wearable dual-band low profile high gain low SAR antenna AMC-backed for WBAN applications. *IEEE Trans. Antennas Propag.* **2019**, *67*, 6378–6388. [CrossRef]
24. Oueida, S.; Kotb, Y.; Aloqaily, M.; Jararweh, Y.; Baker, T. An edge computing based smart healthcare framework for resource management. *Sensors* **2018**, *18*, 4307. [CrossRef]
25. Kumar, S.M.; Majumder, D. Healthcare solution based on machine learning applications in IOT and edge computing. *Int. J. Pure Appl. Math.* **2018**, *119*, 1473–1484.
26. Wu, F.; Qiu, C.; Wu, T.; Yuce, M.R. Edge-based hybrid system implementation for long-range safety and healthcare IoT applications. *IEEE Internet Things J.* **2021**, *8*, 9970–9980. [CrossRef]
27. Saba, T.; Haseeb, K.; Ahmed, I.; Rehman, A. Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *J. Infect. Public Health* **2020**, *13*, 1567–1575. [CrossRef] [PubMed]
28. Rahman, M.A.; Hossain, M.S. An Internet of medical things-enabled edge computing framework for tackling COVID-19. *IEEE Internet Things J.* **2021**, 1. [CrossRef]
29. Gupta, D.; Bhatt, S.; Gupta, M.; Tosun, A.S. Future smart connected communities to fight covid-19 outbreak. *Internet Things* **2021**, *13*, 100342. [CrossRef]
30. Arifeen, M.M.; Al Mamun, A.; Kaiser, M.S.; Mahmud, M. Blockchain-Enable Contact Tracing for Preserving User Privacy during COVID-19 Outbreak. 2020. Available online: https://www.preprints.org/manuscript/202007.0502/v1 (accessed on 30 July 2021).
31. Ullah, Z.; Ahmed, I.; Razzaq, K.; Naseer, M.K.; Ahmed, N. DSCB: Dual sink approach using clustering in body area network. *Peer Peer Netw. Appl.* **2019**, *12*, 357–370. [CrossRef]
32. Lone, T.A.; Rashid, A.; Gupta, S.; Gupta, S.K.; Rao, D.S.; Najim, M.; Srivastava, A.; Kumar, A.; Umrao, L.S.; Singhal, A. Securing communication by attribute-based authentication in HetNet used for medical applications. *Eurasip J. Wirel. Commun. Netw.* **2020**, *2020*, 1–21. [CrossRef]
33. Ullah, F.; Ullah, I.; Khan, A.; Uddin, M.I.; Alyami, H.; Alosaimi, W. Enabling Clustering for Privacy-Aware Data Dissemination Based on Medical Healthcare-IoTs (MH-IoTs) for Wireless Body Area Network. *J. Healthc. Eng.* **2020**, *2020*. [CrossRef]
34. Emam, A.; Abdellatif, A.A.; Mohamed, A.; Harras, K.A. Edgehealth: An energy-efficient edge-based remote mhealth monitoring system. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019.
35. Karmore, S.; Bodhe, R.; Al-Turjman, F.; Kumar, R.L.; Pillai, S. IoT based humanoid software for identification and diagnosis of Covid-19 suspects. *IEEE Sens. J.* **2020**, 1. [CrossRef]
36. Lin, H.; Garg, S.; Hu, J.; Wang, X.; Piran, M.J.; Hossain, M.S. Privacy-enhanced data fusion for COVID-19 applications in intelligent Internet of medical Things. *IEEE Internet Things J.* **2020**. [CrossRef]
37. Ahamad, S.S.; Pathan, A.-S.K. A formally verified authentication protocol in secure framework for mobile healthcare during COVID-19-like pandemic. *Connect. Sci.* **2020**, 1–23. [CrossRef]
38. Chervyakov, N.; Babenko, M.; Tchernykh, A.; Kucherov, N.; Miranda-López, V.; Cortés-Mendoza, J.M. AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security. *Future Gener. Comput. Syst.* **2019**, *92*, 1080–1092. [CrossRef]
39. Haque, R.U.; Hasan, A.; Jiang, Q.; Qu, Q. Privacy-preserving K-nearest neighbors training over blockchain-based encrypted health data. *Electronics* **2020**, *9*, 2096. [CrossRef]
40. Azar, J.; Makhoul, A.; Barhamgi, M.; Couturier, R. An energy efficient IoT data compression approach for edge machine learning. *Future Gener. Comput. Syst.* **2019**, *96*, 168–175. [CrossRef]
41. Boyle, E.; Gilboa, N.; Ishai, Y. Breaking the circuit size barrier for secure computation under DDH. In Proceedings of the 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016. [CrossRef]
42. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
43. Riley, G.F.; Henderson, T.R. The ns-3 network simulator. In *Modeling and Tools for Network Simulation*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 15–34.