sustainability

MDPI

Article

Sustainability Model for the Internet of Health Things (IoHT) Using Reinforcement Learning with Mobile Edge Secured Services

Amjad Rehman [1,2], Tanzila Saba [1,2], Khalid Haseeb [2,3], Teg Alam [4] and Jaime Lloret [5,*]

1 College of Computer & Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
2 Artificial Intelligence and Data Analytics (AIDA) Lab, CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia
3 Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Pakistan
4 Department of Industrial Engineering, College of Engineering, Prince Sattam bin Abdul Aziz University, Al-Kharj 11942, Saudi Arabia
5 Insituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politecnica de Valencia, C/Paranimf, 1, 46370 Valencia, Grao de Gandia, Spain
* Correspondence: jlloret@dcom.upv.es

Abstract: In wireless multimedia networks, the Internet of Things (IoT) and visual sensors are used to interpret and exchange vast data in the form of images. The digital images are subsequently delivered to cloud systems via a sink node, where they are interacted with by smart communication systems using physical devices. Visual sensors are becoming a more significant part of digital systems and can help us live in a more intelligent world. However, for IoT-based data analytics, optimizing communications overhead by balancing the usage of energy and bandwidth resources is a new research challenge. Furthermore, protecting the IoT network's data from anonymous attackers is critical. As a result, utilizing machine learning, this study proposes a mobile edge computing model with a secured cloud (MEC-Seccloud) for a sustainable Internet of Health Things (IoHT), providing real-time quality of service (QoS) for big data analytics while maintaining the integrity of green technologies. We investigate a reinforcement learning optimization technique to enable sensor interaction by examining metaheuristic methods and optimally transferring health-related information with the interaction of mobile edges. Furthermore, two-phase encryptions are used to guarantee data concealment and to provide secured wireless connectivity with cloud networks. The proposed model has shown considerable performance for various network metrics compared with earlier studies.

Keywords: data analytics; machine learning; internet of health things; sustainable network; security; data hiding; healthcare

Citation: Rehman, A.; Saba, T.; Haseeb, K.; Alam, T.; Lloret, J. Sustainability Model for the Internet of Health Things (IoHT) Using Reinforcement Learning with Mobile Edge Secured Services. *Sustainability* **2022**, *14*, 12185. https://doi.org/10.3390/su141912185

Academic Editor: Zubair Baig

Received: 6 July 2022
Accepted: 21 September 2022
Published: 26 September 2022

1. Introduction

With the integration of IoT technologies and mobile networks, significant improvements have been made in developing smart applications [1–3]. These applications enhance communication networks' performances in various industries, including healthcare, transportation, security monitoring, etc., in terms of coverage, costs, scalability, and data gathering. Mobile computing supports IoT applications in healthcare, contributes to current and future research projects brings data security among healthcare devices, and influences IoT-based systems [4–6]. However, the majority of solutions are now having difficulties with dependability and long-term connectivity for healthcare systems. Disease prevention is a crucial component of healthcare due to the aging population and the increase in chronic patients. The medical sensors sense the patients' health and transmit the gathered data to data servers on the cloud for processing and analysis [7–9]. Sensor-produced data can assist patients and medical experts in better understanding symptoms, and promptly

identifying needed treatments. However, the resource constraints of sensor networks significantly increase the need for efficient solutions to route critical data and make reliable decisions [10–12]. Moreover, securing IoT-based healthcare systems against internal or external network threats is also a demanding research challenge. Many researchers have offered cloud-based security algorithms for smart applications, increasing data scalability with efficient information retrieval [13–15]. Big data in the context of e-health are transported from one site to another by utilizing a wireless communication and cloud network in an IoT-based teleradiology system [16–18], as shown in Figure 1. This allows hospitals to obtain quick input from radiologists, who perform the same responsibilities as if they were on-site. Various optimization solutions for various data processing processes are constantly being described in state-of-the-art techniques [19–21] for IoT networks. Because these small sensor nodes constitute the backbone of today's IoT-based applications [22–24], the primary purpose of constraint networks is to save energy. On the other hand, these nodes perform various services, such as data sensing, transmission, and aggregation, and operate in dangerous settings solely on battery power. As a result, to extend the network's operational period, we must investigate and develop appropriate routing solutions. Medical data security across unstable networks is also a prominent research topic. Because data are sent across insecure pathways, hostile nodes can interfere and cause the communication system to be compromised [25–27]. According to a recent study, solutions for IoT devices are efficient and environmentally friendly, however, most of them need further improvement in terms of energy and computing overheads. Additionally, reducing route breakages in the presence of movable edges is seen as a critical challenge for prompt data response. Furthermore, IoT sensors are inextricably linked to resource usage and play an essential role in governing green technological systems. An efficient and secure mobile edge computing solution must be proposed to reduce power consumption in communication networks while preserving cloud computing for digital systems.

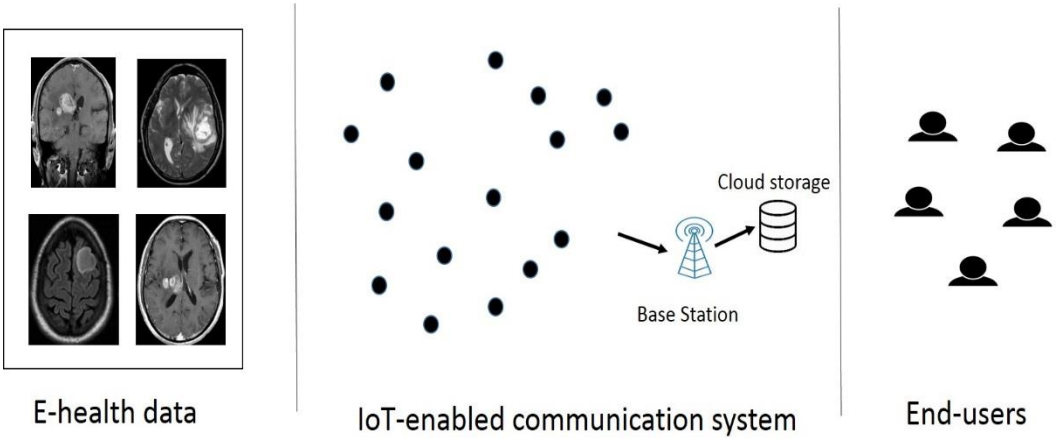

Figure 1. IoT-based communication system with e-health cloud.

In summary, the MEC-Seccloud model delivers the following contributions:

i. It employs a reinforcement learning technique to explore QoS and assist green computing technologies;
ii. It achieves an intelligent methodology based on global optimal solutions for IoHT-based systems and offers effective resource usage with edge computing;
iii. In addition, it secures the cloud environment by providing encryption and integrity verifications to enhance the consistency of massive amounts of data. The proposed model is compared to existing work in terms of energy- and security-related indicators.

The research paper is organized as follows: Section 2 discusses the literature; Section 3 provides an explanation of the proposed model and its related components; Section 4 describes the network model and performance analysis; finally, the conclusion is presented in Section 5.

2. Related Work

IoT is a wireless network made up of various sensors, devices, and smart objects that communicate with each other through telecommunication services [28–30]. In recent years, machine learning and deep learning algorithms have broadly explored different areas with the support of IoT networks to monitor and track remote environments; however, providing network coverage with better connectivity and reliability are some important research objectives for IoT technologies [31–33]. The authors of Ref. [34] provide dynamic spectrum sensing methods for two-way information exchange to increase energy efficiency for data transmission in licensed channels. They also offer an energy-efficient optimal transmit power allocation technique to improve dynamic spectrum sensing and data throughput. This addresses the question of energy consumption in dynamic spectrum sensing and switching. According to the simulations, the proposed dynamic spectrum sensing technique can significantly reduce energy usage in cognitive radio-based IoT networks. In recent decades, the development of optimization schemes is playing a significant part in delivering medical data over wireless communication systems. However, due to the unpredictable factors of constraint devices and transmission routes, most of the solutions still lack the time-delivery and management efficiency of the transmission model. Additionally, medical data are very sensitive and should be safely forwarded to cloud services for processing. The authors in Ref. [35] provide a technique for robust data transmission for the Internet of Things (RDDI) using Harris hawks optimization (HHO), a safe data diffusion mechanism that accompanies a fuzzy hierarchical network model for IoT based on a wireless sensors network (WSN). RDDI notifies users of assaults and monitors information exchange operations on nodes. The method seeks to combine routing skills, energy-aware and geographic data circulation, and fuzzy clustering to create a dependable, nature-inspired, optimized routing algorithm for IoT termed Harris hawks optimization (HHO). The performance of RDDI in multi-cluster settings is evaluated using five metrics: dependability, end-to-end latency, energy consumption, computational overhead, and packet forwarding distance. The authors in Ref. [36] proposed a transmission data dissemination system with a multiple-load-balancing approach. This research leverages an ant-colony-optimization-inspired approach to create transmission lines for nodes located in diverse locations. Their approach is distinguished by three load-balancing systems that aid in constructing transmission lines arranged in a path tree. The first is the load decentralization strategy, which establishes many route subtrees early on and distributes the whole load among them to prevent excessive load concentration. The second is the load maintenance strategy, which utilizes an appropriate pheromone update mechanism to preserve previously successful pathways, resulting in great next-generation solutions. The last one is the load diversion scheme, which uses the heuristic factor to redirect traffic to routes with low traffic volumes to remove inefficient solutions. Finally, detailed simulations are applied to ensure the novel transmission strategy's efficacy and benefits. A unique cluster-based data aggregation approach based on the male lion optimization algorithm (DA-MOMLOA) is presented in Ref. [37]. It analyzes the network's energy, latency, density, and distance. The data aggregation approach is implemented using a cluster head, which forwards consolidation data from comparable clusters to the sink node, where intelligent methods are applied. Consequently, the suggested technique exhibits promising results, as it dramatically improves network efficiency and decreases packet loss rates due to the reduction in the number of consolidation procedures. The software-defined wireless sensor networks (SDWSNs) controller is trained using reinforcement learning in Ref. [38] to improve the routing paths. The authors merged reinforcement and SDN to construct routing tables on the SDN controller. To enhance network performance, the proposed solution offered four different reward functions. Compared with reinforcement-based routing algorithms, the proposed solution significantly increases network performance in terms of lifetime.

Moreover, compared to existing work, it offers a faster network convergence rate. For WSNs, the authors in Ref. [39] proposed a reinforcement-based routing system and

achieved global optimization without any additional cost. The proposed solution considers these aspects, such as hop count, link distance, and remaining energy, to compute the reward function. Using the proposed reward function decreases energy consumption and improves data delivery for WSN. It also handles communication problems inside the clusters and among cluster heads. Table 1 summarizes the research contributions of the related work along with their shortcomings.

Table 1. Summary of related work.

Comparative Approaches	Contributions and Limitations
Existing solutions	• The majority of the technologies improved communication systems by increasing energy efficiency and ensuring consistent delivery; • However, the majority of systems lack cognitive data re-transmission detection and resource allocation across IoT-enabled sensors; • Due to the presence of network threats, most current solutions dealt with the issue of a network compromise, which harmed the integrity of green computing; • It was also discovered that the majority of the solutions ignored the concept of edge cloud computing to reduce latency without taking any security insurance when retrieving critical data.
Proposed model	To support the secured cloud, a machine learning-based solution is provided that uses edge computing and provides an intelligent decision-making approach for massive data management. It also ensures cloud data security by guaranteeing authentication, data concealing with integrity, and protection against malicious access.

3. Exploring Machine Learning-Enabled Mobile Edge Computing Model with Secured Sustainable IoHT

In this section, we present the development flow of the proposed model with a network model and discussion. It is comprised of the following sub-sections.

3.1. Network Model and Assumptions

The proposed efficient and secured cloud model is based on visual sensors that interact with each other using edges. The visual sensors are randomly placed in the region to capture the IoT data and, after processing, forward them toward the sink node. Let us consider that N denotes the set of visual sensors s_1, s_2, ..., and s_n, and E denotes the set of edges e_1, e_2, ..., and e_n. Accordingly, the consecutive nodes are connected using an undirected graph by G. The following is a summary of our network assumptions:

i. The visual sensors have limited resources and are immobile;
ii. The sink node has no limited resources and is rotated around the edge boundary;
iii. IoT data can only be received to sink nodes using the edge boundary;
iv. Malicious nodes can generate false information and compromise the communication system;
v. Each node has enough memory to store its neighbor's information.

3.2. Proposal

Currently, medical applications are obtaining significant growth in the development of their smart services. IoT technologies offer fast functionalities in the healthcare industry for better remote monitoring, treatment, and telemedicine. However, the number of devices connected to collaborate and transfer the patients' data requires a high level of connectivity with a robust forwarding mechanism. Moreover, most healthcare solutions do not ensure data security standards and end-to-end trusted communication. Thus, providing security is another important research challenge for implementing IoT in the medical field. Therefore, in this work, we proposed a model that is comprised of forwarding schemes in

e-health applications. It formulates a fitness function based on a machine learning-based optimization technique and explores a multi-heuristic function. The function integrates energy r_e, hops to edge boundary h_e, and link consumption l_c factors. The proposed model utilizes the reinforcement learning optimization algorithm [40] to learn the behavior of the nodes for data forwarding and optimizes the green computing system accordingly. Firstly, the sensor nodes create a local scheme by storing their neighbors' information. The local scheme contains identity, transmission power, and residual energy information. Such a scheme is created at the beginning of the transmission; however, its information is updated at the end of the round timer. Moreover, the proposed model also provides the securing algorithm for cloud networks to attain information hiding and integrity using the collaboration of edge boundaries. Figure 2 depicts the designed components of the proposed MEC-Seccloud model. It consists of three main sub-blocks. The first block is comprised of e-health data and fitness parameters—this phase is utilized for system initialization. The second block combines weighted analysis, computing rewards, and states identification. Its main aim is to apply reinforcement learning by exploring fitness parameters and assigning rewards. In the end, security against threats with verification and data hiding is performed.

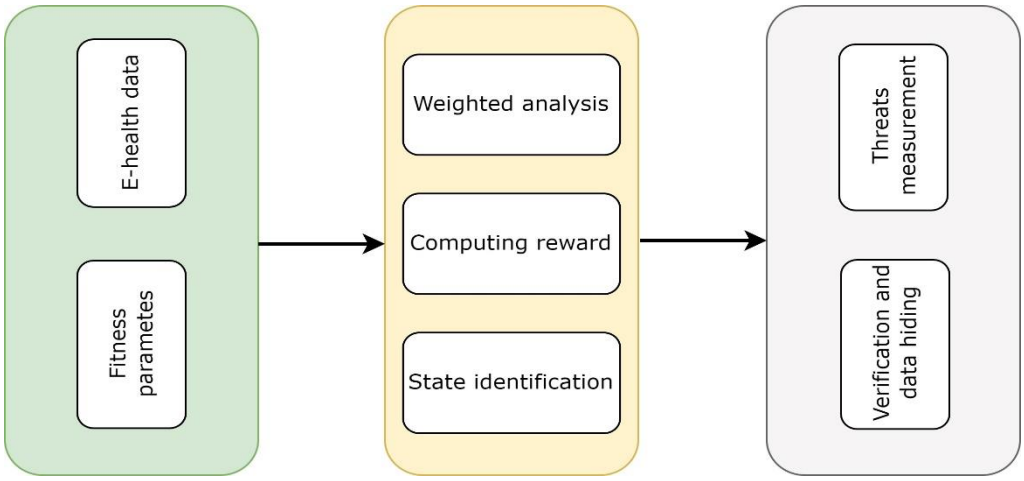

Figure 2. Block diagram of the efficient and secure IoT-based cloud model using machine learning.

3.3. Discussion

This section presents a detailed discussion of the proposed model and its stages. Energy efficiency is the key fitness parameter in sending the data using the sensors node s_i as it depletes based on transmission t_x, receiving r_x and aggregation a_x operations on data packets n, as given in Equation (1):

$$s_i = t_x + r_x + a_x \text{ , where } i \leq n \tag{1}$$

Let us consider that total available energy is denoted by N, and consumed energy in the formation of the route is denoted by r', then the consumed energy r_e at time t can be defined as given in Equation (2):

$$r_e(t) = \frac{s_i}{N} + r' \tag{2}$$

Moreover, the link consumption l_c also performs a significant role in the timely delivery of large-size IoT data and supports the selection of robust channels. To attain efficient utilization of the routing process, the proposed MEC-Seccloud model set a threshold T for the forwarding of maximum data rates by sensor node i, as given in Equation (3):

$$T = \lim_{0 \leq B \leq S} node(i) \tag{3}$$

where B is the size of transmitted data bits and S is the maximum size. Using Equation (4), the proposed MEC-Seccloud model evaluates the link consumption at time interval $t = [t_0, t_1, \ldots, t_k]$:

$$l_c = \sum_{i=0}^{t} B_i \tag{4}$$

After computing all the fitness parameters, weighted fitness $w(f)$ is determined using Equation (5):

$$w(f) = \alpha * r_e(t) + \beta * 1/l_c + \gamma * 1/h_e \tag{5}$$

The proposed MEC-Seccloud model executes the reinforcement learning optimization algorithm for the source node, and selects the optimal node as a forwarder for sensors' data, as given in Equation (6), and it shifts to the next state, S', whose reward R is higher.

$$R = max \sum_{i=1}^{n} (S, w(f)) \tag{6}$$

In Equation (6), the reward for all neighboring nodes n is computed and the highest priority is assigned to the maximum-rewarded node. Accordingly, the source node selects that node for forwarding sensor data that scored the highest reward and shifts it to the new state. Before forwarding the sensor data toward the cloud network, the edge devices announce the formulation of the mapping table, and accordingly, nodes S_i that fall in the predefined transmission range interact with each other and transmit their identities and secret keys S_k toward particular edge devices *es*. Additionally, the transmitted information is encrypted with the public key E_u of the edge devices, as given in Equation (7). Edge nodes generate public keys on their own and are stored inside the memory of edge devices. They flood them into the network so other devices can use them for performing cryptographic operations.

$$S_i \rightarrow es: \; E_u(ID, S_k) \tag{7}$$

Upon receiving the information, the edge device decrypts it using the private key, obtaining the nodes' identities and secret keys. In the proposed MEC-Seccloud model, the sensor data attained its privacy and integrity using the CBC-MAC algorithm [41]. Our proposed model is tested for e-health images and they are divided into various blocks of fixed sizes. The security process is divided into two main stages. Firstly, the CBC processing is executed to maintain the information hiding in the form blocks, as defined in Equation (8):

$$H_i \leftarrow E_{S_k}(xor(H_{i-1}, d_i) \tag{8}$$

where H_i is the cipher block and E is the encryption process based on a secret key S_k. Afterward, it uses the second secret key $S_k{}'$ and computes the MAC for a block, as given in Equation (9):

$$H_i{}' \leftarrow E_{S_k{}'}(H_i) \tag{9}$$

In the proposed MEC-Seccloud model, the sink node is mobile and collects the sensor data from the edge boundary. The sink node is periodically rotated with a fixed speed in the clockwise direction. It sends its latest location to edge devices and receives the network data after successful verification from the edge boundary. Moreover, the sink node maintains a local data management process and records all the information for authorized edge devices. When any data come from the edge boundary, the sink node first verifies the authenticity of the edge nodes, and after declaring it authentic, the sink node collects the sensor data.

Moreover, the sink node communicates with the cloud network to facilitate remote users. It also provides comfort to connected users to attain network information with high trust and security against anonymous attacks. Two steps in the proposed MEC-Seccloud model are provided before accessing the e-health records from the cloud network. Firstly, the requester sends the request packet to the cloud system and, upon passing the verification process, is allowed to access the database server *ds* for data access. Secondly, the MEC-Seccloud model begins lightweight encryption and decryption processes after

the successful verification process. In the security phase, the cloud system *cs* generates a digital certificate *cer* for each requestee, which needs to be provided to access e-health records, as defined in Equation (10):

$$Req(Cer)_{x \rightarrow cs} = id, N_a \tag{10}$$

where *id* is the identity of the requestee node. Upon successful verification of the requestee, the cloud system generates the session key K_s for the interaction with x, which is digitally signed with its private key P_r, as provided in Equation (11):

$$C_{x \leftrightarrow cs} = P_r\ (K_s\ ),\ N_b \tag{11}$$

In Equations (10) and (11), N_a and N_b are system-generated nonces. Based on the obtained K_s, e-health records D_n are encrypted E. Additionally, the result of encryption is xor with *ID* to retain authentication. On the other side, firstly, the encrypted data are decrypted D, and the outcome is xor with *ID* to verify the identity, as given in Equations (12) and (13).

$$E = ((k_s \oplus D_n) \oplus ID) \tag{12}$$

$$D = (e_p \oplus ID) \tag{13}$$

where e_p denotes the encrypted packet using $k_s \oplus D_n$ in Equation (12). Figure 3 illustrates the developed procedures for the MEC-Seccloud model. It has three main components. First, health data are collected using sensors, and using wireless transmission standards the devices collaborate. Secondly, the proposed model utilizes the fitness function with the values of the nodes and accordingly announces the neighboring states. Finally, security is applied to dual communication paradigms. The security stage provides the consistent and reliable delivery of health data to remote users for treating patients' conditions.

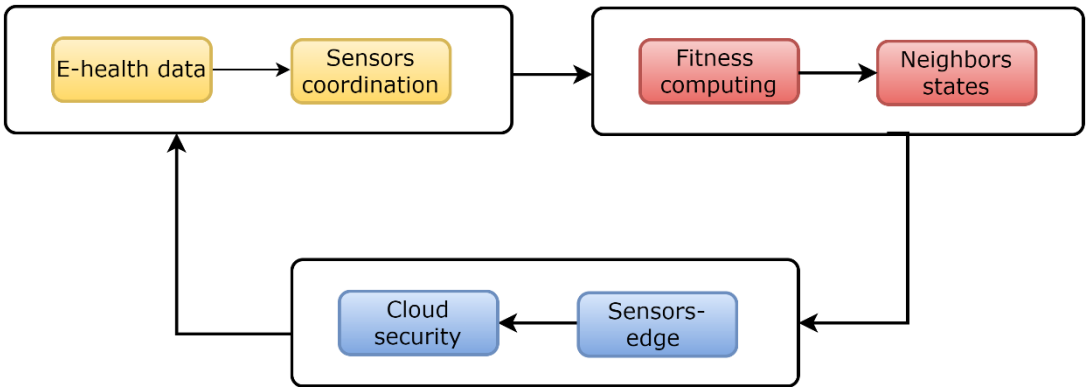

Figure 3. Developed flow of the proposed efficient and secure IoT-based big data analytics.

The flowchart of the proposed schemes in the proposed model is illustrated in Figure 4. It is comprised of many modules: the first is for computing weighted fitness using a reinforcement learning optimizing algorithm, the second is for selecting neighboring states for the transmission of the IoT sensors' data, and the third is for securing the e-health cloud. The fit is dependent on metaheuristics parameters, and their values are updated by evaluating the communication system. The process of evaluating neighboring states is continued intelligently until network data are obtained by the edge boundary. Using reinforcement learning, the proposed model learns how to optimize the network and provide rewards. The edge devices are further associated with the cloud structure for robust health data delivery and reliability. All error messages that occur because of the existence of network threats are stored in log files. Algorithm 1 shows the pseudocode for the proposed model.

Algorithm 1: Sustainable model using machine learning with secured data connections

1. *procedure* network registration (*R*) //nodes and devices declaration
2. devices initialization and sensing
3. fitness parameters
4. *foreach* (neighbors) do //weighted function with network metrics
5. determine the weighted fitness $w(f)$
6. $w(f) = \alpha * r_e(t) + \beta * 1/l_c + \gamma * 1/\ h_e$
7. *end for*
8. *if* $w(f)$ of node i is maximum then //assigned rewards
9. execute reward function R
10. *end if*
11. *foreach* (selected forwarder j) do //nodes-edges connection
12. collaborate with edges in multi-hop paradigm
13. *end for*
14. *end procedure*
15. *procedure* connections_secured //end-to-end secured connections
16. share the identities and secret keys
17. each forwarder validates its identity on the edges
18. *if* identity is acceptable then
19. call CBC for data chaining
20. *end if*
21. *foreach* (blocks) do
22. verified its integrity
23. *end for*
24. *end procedure*

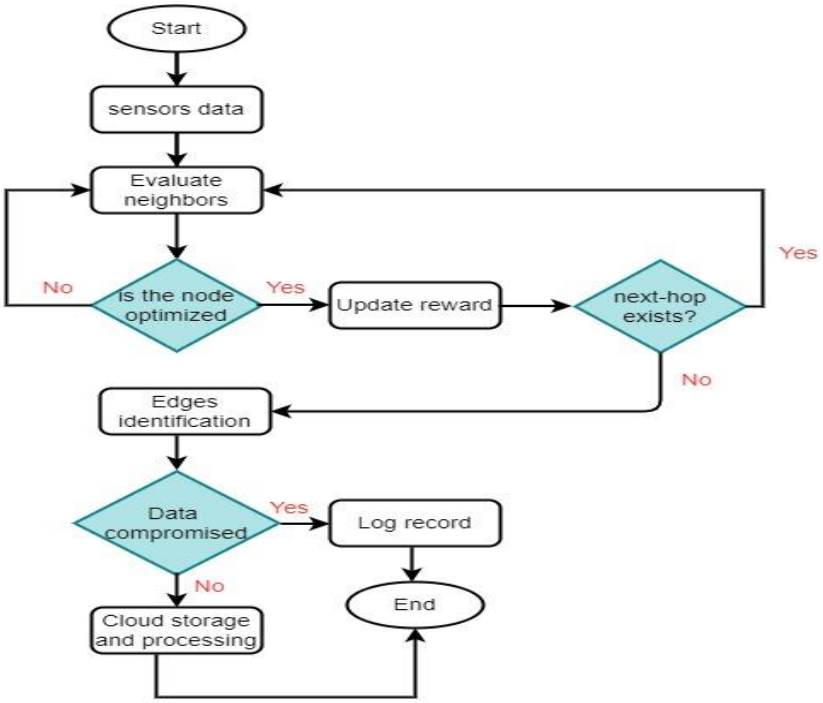

Figure 4. Flowchart of the presented schemes in the proposed model.

4. Simulations

This section presents the network setup configuration and evaluates the proposed model's performance against the existing solution. The experiments are performed using an NS-3 simulator with different network metrics, such as network throughput, data delivery performance, packet drop ratio, energy consumption, and data integrity. The proposed model is trained and tested on the Kaggle data sets by extracting medical images. The

20 simulations were executed. Medical sensors are deployed on a preset location to conduct the experiments and are set as 100 in number. The transmission radius of each sensor is fixed to 5 m. Additionally, to evaluate the performance of the proposed model against security attacks, 20 malicious nodes are randomly deployed. The sink node is mobile and is rotated around the edge boundary. The edge devices comprise 10 nodes. Initially, the energy resource of all the nodes is set as 5 J. Table 2 illustrates the simulation parameters for the experiments.

Table 2. Simulation parameters.

Parameters	Values
Simulation area	two-dimensional
Sensor nodes	50–250
Malicious nodes	20
Transmission power	5 m
Initial energy	5 J
Simulation time	5000 s
Data flow	CBR
Sink node	1
Edge nodes	10
Cloud devices	4
Size of public key	512 bits

Comparison with Existing Schemes

Table 3 shows the simulation tests of various performance metrics for the proposed MEC-Seccloud model and existing solutions. The results are recorded after the series of simulations for network throughput, energy consumption, packet drop ratio, and data integrity. The evaluation criteria are based on the varying numbers of nodes and data generation rates.

Table 3. Tests result in performance metrics under two scenarios.

Proposed Model and Existing Work	Network Throughput (%)	Energy Consumption (j)	Data Drop Ratio (%)	Data Integrity (%)
	Number of Nodes: 50 to 250			
MEC-Seccloud	87.5	1.21	7.9	85.2
RDDI	72.4	1.63	15	73.1
DA-MOMLOA	70	2.07	17.8	63.8
	Data Generation Rates: 100 to 500 bits/sec			
MEC-Seccloud	88	1.3	9.4	85.8
RDDI	77.4	1.65	15.6	74.4
DA-MOMLOA	73	1.83	18.6	71.9

In Figure 5a, b, the performance of the proposed MEC-Seccloud model is compared with other solutions for network throughput. The network throughput defines the successful delivery of data packets from sensors to the sink node. Based on the experiments, it is seen that the proposed model significantly improved the performance of network throughput against RDDI and DA-MOMLOA because of the nature-inspired optimization model, which utilized machine learning techniques for the optimal selection of neighboring states. The metaheuristic parameters judge the conditions of the nodes and environment,

and the weighted fitness function provides a uniform contribution for each parameter. Moreover, the boundary of the edges collaborates with the sink node and reduces the communication distance from the medical sensors to the sink node. Our proposed MEC-Seccloud model balances the sensors' energy depletion and explicitly provides the most stable communications link for green computing technologies.

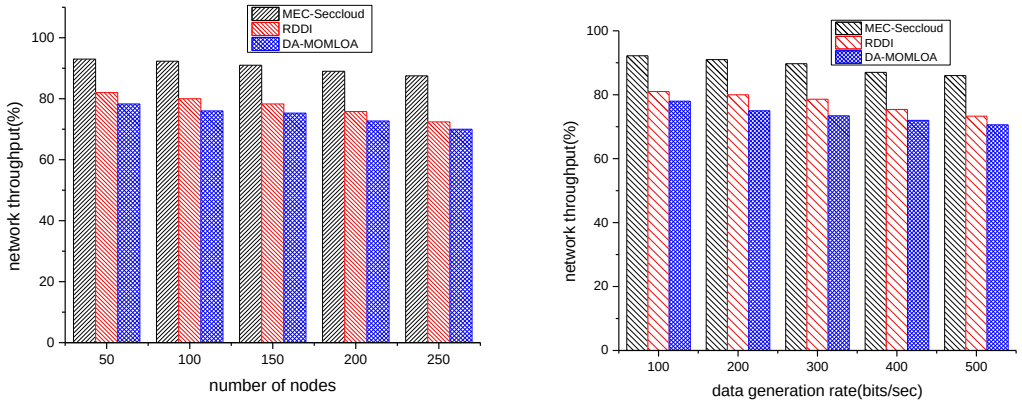

Figure 5. Network throughput under a varying number of nodes from 50 to 250, and varying data generation rates from 100 to 500 bits/s. (**a**) Network throughput with varying nodes. (**b**) Network throughput with varying data generation rates.

Figure 6a,b illustrate the performance of the proposed MEC-Seccloud model with other solutions for energy consumption. It is observed that with the increasing number of nodes and data generation rates, the value for energy consumption is also increased. However, based on the experimental results, the proposed MEC-Seccloud model has efficiently improved the utilization of energy resources compared with RDDI and DA-MOMLOA. This is because of its efficient computation of the weighted fitness function by exploring the metaheuristic parameters. Additionally, the selection of neighboring states using a machine learning algorithm imposes the least communication overheads and trains the model using updated conditions. Moreover, to avoid overloaded links based on a fitness function, the proposed MEC-Seccloud model reduces the high amount of data re-transmissions and ultimately efficiently manages energy consumption. The proposed MEC-Seccloud model divides the e-health data into chunks and ensures prompt delivery without imposing additional energy costs on the IoT-enabled network system by utilizing the CBC-MAC algorithm.

Figure 7a,b illustrate the performance of the proposed MEC-Seccloud model in terms of packet drop ratio against the existing solution. Based on the experiments, it is observed that the number of nodes and random deployment of malicious nodes increase the ratio of the lost packets. This is because of fake data forwarding requests by malicious nodes. Additionally, with high congestion traffic over the transmission channels, the communication link is overloaded and there is no free space for the routing of medical data. However, the proposed MEC-Seccloud model remarkably improves the packet drop ratio compared with RDDI and DA-MOMLOA. Furthermore, unlike the existing solution, the proposed model periodically utilizes the consumption data flow and selects the optimal channel based on a machine learning algorithm. Furthermore, only those extracted sensors whose reward values are higher than their neighbors are gaining high priority. Additionally, securing the algorithm of the proposed model improves the consistency of medical data against inauthentic processes.

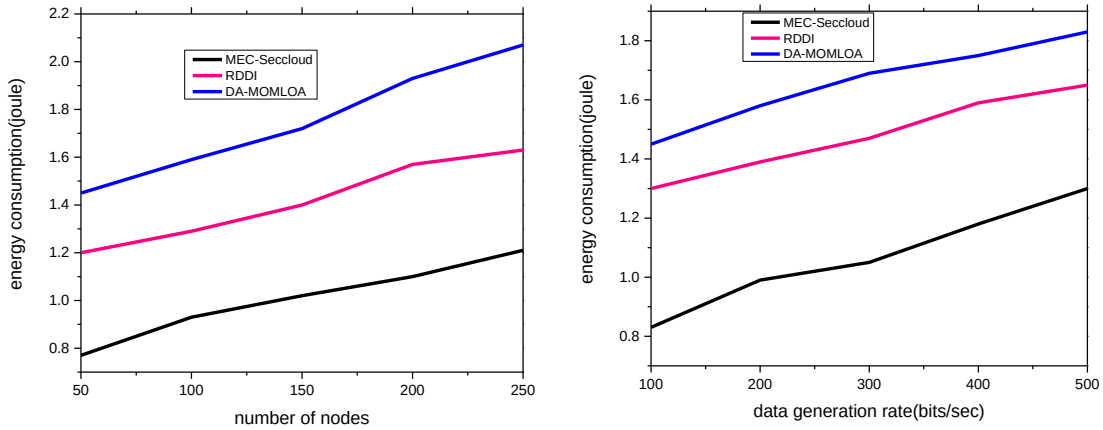

Figure 6. Energy consumption under a varying number of nodes from 50 to 250, and varying data generation rates from 100 to 500 bits/s. (**a**) Energy consumption with varying nodes. (**b**) Energy consumption with varying data generation rates.

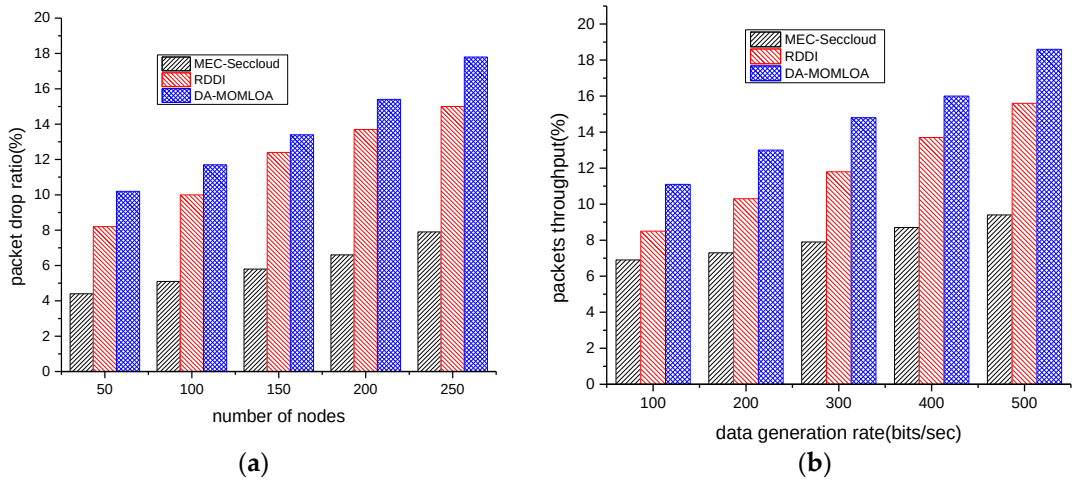

Figure 7. Packet drop ratio under a varying number of nodes from 50 to 250, and varying data generation rates from 100 to 500 bits/s. (**a**) Packet drop ratio with varying nodes. (**b**) Packet drop ratio with varying data generation rates.

In Figure 8a,b, the performance analysis of the proposed MEC-Seccloud model is presented in terms of data integrity compared with other solutions. It is observed that with increasing the number of malicious nodes, the data integrity reduces. However, the proposed MEC-Seccloud model improves the data consistency with integrity compared with the existing solutions. This is because it efficiently manages false route requests and avoids malicious nodes from being a part of the communication system by utilizing the machine learning algorithm. Moreover, using two-phase CBC-MAC security from edge-boundary sensors eliminates the non-normal processes for e-health data and attains lightweight encryption. Two separate keys are utilized by the proposed model for maintaining data encryption and integrity. Furthermore, the verified process is also maintained from the edge boundary to the cloud network in a controlled manner.

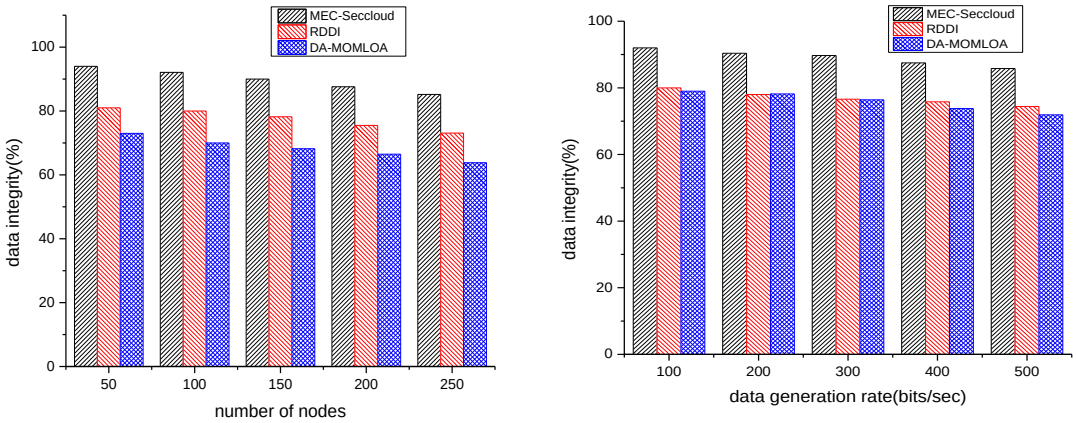

Figure 8. Data integrity under a varying number of nodes from 50 to 250, and under varying data generation rates from 100 to 500 bits/s. (**a**) Data integrity with varying nodes. (**b**) Data integrity with varying data generation rates.

5. Conclusions

With the integration of IoT communication and cloud networks, optimization approaches are increasingly being used for the growth and development of sustainable systems. Sensor nodes, unlike other communication systems, are resource-constrained and have an impact on energy usage in data management techniques. Therefore, machine learning algorithms significantly improved big data analytics delivery performance and lowered costs. On the other hand, the strategies of intelligent edge computing should be used in conjunction with metaheuristic variables to control QoS parameters. Furthermore, in the context of e-health, an edge cloud network requires hiding and integrity for massive data. This paper provides an efficient, sustainable, and secure machine learning-based cloud network optimization model. It uses reinforcement learning to optimize neighboring states for managing data analytics and energy efficiency. The weighted fitness is uniform to the routing system and provides a manageable cost by utilizing the network edges. Furthermore, two steps of the CBC-MAC algorithm strengthened the proposed machine learning model's resistance to harmful traffic while also ensuring data security in the edge cloud network. In the future, we intend to examine distributed denial of service (DoS) threats and train the proposed model using a real-time data set.

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

Funding: This work has been partially funded by the "La Fundación para el Fomento de la Investigación Sanitaria y Biomédica de la Comunitat Valenciana (Fisabio)" through the project PULSI-DATA (A43).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data are available in the manuscript.

Acknowledgments: This research is supported by the Artificial Intelligence & Data Analytics Lab (AIDA), CCIS Prince Sultan University, Riyadh, Saudi Arabia. The authors are thankful for technical support.

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

References

1. Sara, G.S.; Sridharan, D. Routing in mobile wireless sensor network: A survey. *Telecommun. Syst.* **2014**, *57*, 51–79. [CrossRef]
2. Keswani, B.; Mohapatra, A.G.; Mohanty, A.; Khanna, A.; Rodrigues, J.J.; Gupta, D.; de Albuquerque, V.H.C. Adapting weather conditions based IoT enabled smart irrigation technique in precision agriculture mechanisms. *Neural Comput. Appl.* **2019**, *31*, 277–292. [CrossRef]
3. Lloret, J.; Parra, L.; Taha, M.; Tomás, J. An architecture and protocol for smart continuous eHealth monitoring using 5G. *Comput. Netw.* **2017**, *129*, 340–351. [CrossRef]
4. Yuan, J.; Zhang, J.; Ding, S.; Dong, X. Cooperative localization for disconnected sensor networks and a mobile robot in friendly environments. *Inf. Fusion* **2017**, *37*, 22–36. [CrossRef]
5. Nazir, S.; Ali, Y.; Ullah, N.; García-Magariño, I. Internet of things for healthcare using effects of mobile computing: A systematic literature review. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 5931315. [CrossRef]
6. Acar, M.; Kaya, O. A healthcare network design model with mobile hospitals for disaster preparedness: A case study for Istanbul earthquake. *Transp. Res. Part E Logist. Transp. Rev.* **2019**, *130*, 273–292. [CrossRef]
7. Mishra, S.; Mishra, B.K.; Tripathy, H.K.; Dutta, A. Analysis of the role and scope of big data analytics with IoT in health care domain. In *Handbook of Data Science Approaches for Biomedical Engineering*; Academic Press: Cambridge, MA, USA, 2020; pp. 1–23.
8. Alshehri, F.; Muhammad, G. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. *IEEE Access* **2020**, *9*, 3660–3678. [CrossRef]
9. Rehman, A.; Haseeb, K.; Fati, S.M.; Lloret, J.; Peñalver, L. Reliable Bidirectional Data Transfer Approach for the Internet of Secured Medical Things Using ZigBee Wireless Network. *Appl. Sci.* **2021**, *11*, 9947. [CrossRef]
10. Bhushan, B.; Sahoo, G. Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective. In *Handbook of Computer Networks and Cyber Security*; Springer: Cham, Switzerland, 2020; pp. 683–713. [CrossRef]
11. El-Fouly, F.H.; Ramadan, R.A. E3AF: Energy efficient environment-aware fusion based reliable routing in wireless sensor networks. *IEEE Access* **2020**, *8*, 112145–112159. [CrossRef]
12. 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. [CrossRef]
13. Mahajan, H.B.; Rashid, A.S.; Junnarkar, A.A.; Uke, N.; Deshpande, S.D.; Futane, P.R.; Alkhayyat, A.; Alhayani, B. Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Appl. Nanosci.* **2022**, 1–14. [CrossRef]
14. Zhou, M.; Hassan, M.M.; Goscinski, A. *Emerging Edge-of-Things Computing for Smart Cities: Recent Advances and Future Trends*; Elsevier: Amsterdam, The Netherlands, 2022; Volume 600, pp. 442–445.
15. 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]
16. Rosenkrantz, A.B.; Hanna, T.N.; Steenburg, S.D.; Tarrant, M.J.; Pyatt, R.S.; Friedberg, E.B. The current state of teleradiology across the United States: A national survey of radiologists' habits, attitudes, and perceptions on teleradiology practice. *J. Am. Coll. Radiol.* **2019**, *16*, 1677–1687. [CrossRef]
17. Kumar, S.; Fred, A.L.; Miriam, L.J.; Padmanabhan, P.; Gulyás, B.; Ajay, K.H. Applications of Image Processing in Teleradiology for the Medical Data Analysis and Transfer Based on IOT. In *Machine Learning Approaches for Convergence of IoT and Blockchain*; John Wiley & Sons: Hoboken, NY, USA, 2021; pp. 175–204. [CrossRef]
18. Islam, N.; Haseeb, K.; Rehman, A.; Alam, T.; Jeon, G. An adaptive and secure routes migration model for the sustainable cloud of things. *Clust. Comput.* **2022**, 1–12. [CrossRef]
19. Ramson, S.J.; Raju, K.L.; Vishnu, S.; Anagnostopoulos, T. Nature inspired optimization techniques for image processing—A short review. In *Nature Inspired Optimization Techniques for Image Processing Applications*; Springer: Cham, Switzerland, 2019; pp. 113–145. [CrossRef]
20. Karimi-Mamaghan, M.; Mohammadi, M.; Meyer, P.; Karimi-Mamaghan, A.M.; Talbi, E.-G. Machine Learning at the service of Meta-heuristics for solving Combinatorial Optimization Problems: A state-of-the-art. *Eur. J. Oper. Res.* **2022**, *296*, 393–422. [CrossRef]
21. Sundhari, R.M.; Jaikumar, K. IoT assisted Hierarchical Computation Strategic Making (HCSM) and Dynamic Stochastic Optimization Technique (DSOT) for energy optimization in wireless sensor networks for smart city monitoring. *Comput. Commun.* **2020**, *150*, 226–234. [CrossRef]
22. Nayak, P.; Swetha, G.; Gupta, S.; Madhavi, K. Routing in wireless sensor networks using machine learning techniques: Challenges and opportunities. *Measurement* **2021**, *178*, 108974. [CrossRef]
23. 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]
24. Ahmed, I.; Din, S.; Jeon, G.; Piccialli, F.; Fortino, G. Towards collaborative robotics in top view surveillance: A framework for multiple object tracking by detection using deep learning. *IEEE/CAA J. Autom. Sin.* **2020**, *8*, 1253–1270. [CrossRef]
25. Frustaci, M.; Pace, P.; Aloi, G.; Fortino, G. Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet Things J.* **2017**, *5*, 2483–2495. [CrossRef]
26. Kotenko, I.; Saenko, I.; Branitskiy, A. Framework for mobile Internet of Things security monitoring based on big data processing and machine learning. *IEEE Access* **2018**, *6*, 72714–72723. [CrossRef]

27. 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]
28. Zhang, Z.; Xiao, Y.; Ma, Z.; Xiao, M.; Ding, Z.; Lei, X.; Karagiannidis, G.K.; Fan, P. 6G wireless networks: Vision, requirements, architecture, and key technologies. *IEEE Veh. Technol. Mag.* **2019**, *14*, 28–41. [CrossRef]
29. Song, H.; Bai, J.; Yi, Y.; Wu, J.; Liu, L. Artificial intelligence enabled Internet of Things: Network architecture and spectrum access. *IEEE Comput. Intell. Mag.* **2020**, *15*, 44–51. [CrossRef]
30. Haseeb, K.; Saba, T.; Rehman, A.; Ahmed, Z.; Song, H.H.; Wang, H.H. Trust management with fault-tolerant supervised routing for smart cities using internet of things. *IEEE Internet Things J.* **2022**. [CrossRef]
31. Philip, N.Y.; Rodrigues, J.J.; Wang, H.; Fong, S.J.; Chen, J. Internet of Things for in-home health monitoring systems: Current advances, challenges and future directions. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 300–310. [CrossRef]
32. Oughton, E.J.; Lehr, W.; Katsaros, K.; Selinis, I.; Bubley, D.; Kusuma, J. Revisiting wireless internet connectivity: 5G vs Wi-Fi 6. *Telecommun. Policy* **2021**, *45*, 102127. [CrossRef]
33. Awoyemi, B.S.; Alfa, A.S.; Maharaj, B.T. Resource optimisation in 5G and internet-of-things networking. *Wirel. Pers. Commun.* **2020**, *111*, 2671–2702. [CrossRef]
34. Ansere, J.A.; Han, G.; Wang, H.; Choi, C.; Wu, C. A reliable energy efficient dynamic spectrum sensing for cognitive radio IoT networks. *IEEE Internet Things J.* **2019**, *6*, 6748–6759. [CrossRef]
35. Seyfollahi, A.; Ghaffari, A. Reliable data dissemination for the Internet of Things using Harris hawks optimization. *Peer-to-Peer Netw. Appl.* **2020**, *13*, 1886–1902. [CrossRef]
36. Liu, X.; Qiu, T.; Wang, T. Load-balanced data dissemination for wireless sensor networks: A nature-inspired approach. *IEEE Internet Things J.* **2019**, *6*, 9256–9265. [CrossRef]
37. Saranraj, G.; Selvamani, K.; Malathi, P. A novel data aggregation using multi objective based male lion optimization algorithm (DA-MOMLOA) in wireless sensor network. *J. Ambient Intell. Humaniz. Comput.* **2021**, 1–9. [CrossRef]
38. Younus, M.U.; Khan, M.K.; Anjum, M.R.; Afridi, S.; Arain, Z.A.; Jamali, A.A. Optimizing the lifetime of software defined wireless sensor network via reinforcement learning. *IEEE Access* **2020**, *9*, 259–272. [CrossRef]
39. Guo, W.; Yan, C.; Lu, T. Optimizing the lifetime of wireless sensor networks via reinforcement-learning-based routing. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719833541. [CrossRef]
40. Wang, J.X.; Kurth-Nelson, Z.; Tirumala, D.; Soyer, H.; Leibo, J.Z.; Munos, R.; Blundell, C.; Kumaran, D.; Botvinick, M. Learning to reinforcement learn. *arXiv* **2016**, arXiv:1611.05763.
41. Bellare, M.; Kilian, J.; Rogaway, P. The security of cipher block chaining. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1994. [CrossRef]