applied sciences

MDPI

Article

Reliable Bidirectional Data Transfer Approach for the Internet of Secured Medical Things Using ZigBee Wireless Network

Amjad Rehman [1], Khalid Haseeb [2], Suliman Mohamed Fati [1], Jaime Lloret [3,4,*] and Lourdes Peñalver [3]

[1] Artificial Intelligence & Data Analytics Lab (AIDA), CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia; rkamjad@gmail.com (A.R.); smfati@yahoo.com (S.M.F.)
[2] Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Khyber Pakhtunkhwa, Pakistan; khalid.haseeb@icp.edu.pk
[3] Integrated Management Coastal Research Institute, Universitat Politenica de Valencia, Camino Vera sn, 46022 Valencia, Spain; lourdes@disca.upv.es
[4] School of Computing and Digital Technologies, Staffordshire University, Stoke-on-Trent, Staffordshire ST4 2DE, UK
* Correspondence: jlloret@dcom.upv.es

Abstract: Nowadays, the Internet of Things (IoT) performs robust services for real-time applications in monitoring communication systems and generating meaningful information. The ZigBee devices offer low latency and manageable costs for wireless communication and support the process of physical data collection. Some biosensing systems comprise IoT-based ZigBee devices to monitor patient healthcare attributes and alert healthcare professionals for needed action. However, most of them still face unstable and frequent data interruption issues due to transmission service intrusions. Moreover, the medical data is publicly available using cloud services, and communicated through the smart devices to specialists for evaluation and disease diagnosis. Therefore, the applicable security analysis is another key factor for any medical system. This work proposed an approach for reliable network supervision with the internet of secured medical things using ZigBee networks for a smart healthcare system (RNM-SC). It aims to improve data systems with manageable congestion through load-balanced devices. Moreover, it also increases security performance in the presence of anomalies and offers data routing using the bidirectional heuristics technique. In addition, it deals with more realistic algorithm to associate only authorized devices and avoid the chances of compromising data. In the end, the communication between cloud and network applications is also protected from hostile actions, and only certified end-users can access the data. The proposed approach was tested and analyzed in Network Simulator (NS-3), and, compared to existing solutions, demonstrated significant and reliable performance improvements in terms of network throughput by 12%, energy consumption by 17%, packet drop ratio by 37%, end-to-end delay by 18%, routing complexity by 37%, and tampered packets by 37%.

Keywords: reliable data transfer; internet of secured things; public health; mobility; ZigBee devices

Citation: 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. https://doi.org/10.3390/app11219947

Academic Editor: Davide Careglio

Received: 7 September 2021
Accepted: 21 October 2021
Published: 25 October 2021

1. Introduction

In recent decades, many developed solutions such as those for smart homes, security surveillance, healthcare, agriculture, etc., have been associated with wireless standards and physical objects. All these applications are designed to ensure trustworthiness, efficient resource management, and on-time data monitoring using IoT networks [1–3]. However, most of the applications based on IoT sensors only collect and forward the monitored information without guaranteed reliable performance in the event of communication faults or obstacles. The development of wireless sensor networks (WSNs) for medical applications [4–6] is gaining momentum due to IoT sensors that can track patients' locations and facilitate real-time health monitoring. Many solutions exist in the field of healthcare using IoT systems to support the interaction between physicians and patients while staying

remote [7–9]. These solutions interact with IoT networks and offer smart communications with faster and intelligent information management. Such solutions not only ease the efforts of medical experts in identifying the diseases of patients but also offer a smart communication system using lightweight devices. They help in communication among patients and medical experts without visiting hospitals or making prior appointments. However, the minimal boundaries for medical sensors in processing, storage, and battery power pose significant research problems for reliable healthcare data transmissions. Additionally, the unpredictable and unfixed communication structure of sensor nodes further highlights the security issues. The medical data are transmitted over a congested, open-air medium. As a result, unknown or malicious observers can compromise the patients' sensitive data [10–13]. Although many communication models using medical sensors have been developed, several challenges and open research problems are still faced by the research community in terms of communication standards, secure architecture, data reliability, resource management, etc. The reliable and resilient IoT network [14–17] ensures the ability of the communication system to recover and remain active after being affected by an unexpected incident. It not only continues offering network-oriented services but decreases the probability of data interruption among connected routes. Accordingly, medical applications should be developed with the resilience to improve the performance of wireless technologies and features for network maintenance and high accuracy with secure communication. Moreover, the integrity and privacy of IoT systems with a cloud structure are also necessary to avoid the misuse of the network data and avoid compromising performance [18,19].

The main contributions of this research work are summarized as follows.

i. It offers bidirectional routes for IoT-based Zigbee medical networks and supports low overhead with a applications interface. Such factors improve reliability and scalability for health devices even under conditions of high data traffic and decrease the convolution factor.
ii. It also presents lightweight mutual validation for medical information and supports data privacy among processes using the verified cryptosystem. This component excludes unauthenticated endeavors in the healthcare system with the incorporation of real keys.
iii. In the end, the network data is also securely transmitted from the cloud interface to physicians using a hybrid security model and gives resilient trustworthiness.
iv. Based on the security analysis and a set of extensive experiments, the proposed approach has demonstrated improved performance against security threats with increasing network reliability.

The organization of this research work was prepared as follows. Section 2 presents the literature work with problem findings. Section 3 illustrates the network assumptions and a detailed discussion of the proposed approach. Section 4 presents the security analysis and simulation-based experiments. Finally, Section 5 concludes the research work.

2. Related Work

Several real-time applications have been based on IoT sensors to develop an eHealth system to maintain medical data using wireless paradigms [20–22]. The eHealth systems are composed of many medical sensors to monitor the patient's physical state regarding different health data such as blood pressure, oxygen level, heartbeat, temperature, etc. The obtained readings of health data are further forwarded to medical experts for disease diagnosis and treatment. IoT-based health data are also stored on cloud machines to improve applications' scalability with efficient resource management [23–26]. In [27], the authors addressed the various security tasks of big data and proposed an efficient and secure big data storage system for cloud computing. The proposed solution offers a resilient encryption scheme. The analysis of formal security proofs shows that the proposed scheme can ensure users' data privacy even if the partial key is leaked in cloud computing. The performance comparisons illustrate the operability of the proposed solution for big

data security in cloud computing. In [28], the authors proposed a secure leakage resilient s-health system, which aims to ensure safe data transmission in the medical field in the presence of data breaches and network attacks. It is secured against chosen plaintext attacks under the standard model using decisional linear and the Diffie-Hellman exponent assumptions. The large-scale concurrent data anonymous batch verification scheme [29] for mobile healthcare crowdsensing is proposed. It is based on an improved certificate-less aggregate signature and provides authentication for sensing bio-information at once in a confidential manner. It offers batch-wise data verification while hiding the actual identity of participants. The performance evaluation demonstrates that the proposed scheme is more highly efficient for mobile healthcare crowd sensing than other solutions. A secure demand-side management (DSM) engine is proposed [30] based on machine learning for an IoT-enabled grid. It provides energy conservation using priorities, and a specific resilient model is proposed to cope with intrusions in the smart grid. The resilient agent identifies false objects by using a machine learning classifier, and the interface of controlling agents is offered for energy optimization. The simulation-based experiments have been performed and illustrate that the proposed scheme is less vulnerable to intrusions with improved power utilization of the smart grid. An anonymous-based user authentication scheme [31] is proposed for e-health applications using wireless medical sensor networks. It aims to address the security issues and decreases the communication overhead of the constraints-oriented applications. It utilizes improved elliptic curve cryptography and offers efficient performance against password guessing and smart card lost/stolen verifier attacks. The proposed solution offers sufficient security along with strong authentication and low computational cost. The authors in [32] proposed a secure and efficient data delivery protocol to decrease the delay ratio and protect against malicious attacks on wireless signals. It is composed of three custom algorithms and the fog gateway association algorithm aids in improving the security and efficiency between the wireless body area network and the remote resources. The experimental results showed its improved evaluation compared to other solutions. A tractable analysis framework is proposed [33] to test and analyze the reliability, security, and secrecy energy efficiency (SEE) performance for wireless networks using mobile sink nodes. It uses the threshold-based access scheme and a multi-antenna technique. The proposed work assumes both the line-of-sight and non-line-of-sight paths with Rayleigh fading for the air-to-ground channel model. The simulation-based results revealed the better performance of the proposed work with mobile sinks and maximized SEE. Securing wireless sensor networks for improved performance in cloud-based environments is proposed [34] by modifying the low-energy adaptive clustering hierarchy (LEACH) protocol. The proposed solution has added intrusion detection functionality for securing the sensor nodes from sinkhole, black hole, and selective forwarding attacks. The simulation and numerical results of the modified protocol (LEACH++) have proven significant security, throughput, and energy consumption. Authors in [35] introduced a Secure Smart Health system with privacy-aware aggregate authentication and access control in IoT. The proposed solution enables a privacy-aware aggregate authentication using an anonymous certificateless aggregate signature scheme. Additionally, privacy-aware access control is based on anonymous attribute-based encryption technologies. The extensive experimental results demonstrate the improved performance relative to computational cost and communication overheads. In [36], research was performed and an IoT-based smart health framework was developed by focusing on interoperability issues. The particular requirements for IoT networks were analyzed and provided a basis for the design of the developed framework. The performed experiments exhibited that interoperability among various IoT devices, protocols and standards in a smart health system could be achieved using a specialized gateway device. Moreover, different web technologies could be used at the same time under restricted and Internet environments.

The discussion of the related work reveals that constraint resources have a significant role in gathering field data for further analysis for appropriate medical decisions. Most healthcare applications depend on such an IoT network to observe the patients'

data and deliver the information on time to the cloud paradigm. However, their limitations, especially in terms of limited resources, pose significant challenges for wireless and unpredictable communication models. Additionally, it is observed that most of the cloud-oriented solutions remarkably decrease the computational and communication costs for IoT-based transmission systems. However, providing security in the presence of leakage and malicious attacks imposes additional network overhead. It is also observed that minimal solutions have been proposed for network resiliency and offer data routing in a non-optimal manner in terms of longer constancy and heavy sensor traffic. Therefore, the research community is still focused on presenting a resilient approach to coping with data management integrated cloud systems to overcome vulnerabilities in the healthcare system and help patients and medical professionals [37–40].

3. Proposed Approach

In this section, we present a description of the proposed RNM-SC approach with its operating components and system model. It offers a fault-tolerant solution with an improved delivery ratio for patients' data over the insecure wireless medium with low power consumption. Moreover, as healthcare data are very critical in terms of data accuracy and transmitted on inconsistent channels, the proposed work therefore also presents privacy and authentication to deal with network resilience under different contingencies. Although several solutions have been proposed in the recent past to overcome network vulnerability, they are based on heavy-weight cryptographic computation. Such solutions imposed additional power consumption and uneven load distribution on IoT-based networks. In this regard, the proposed approach presents a lightweight authentication process between IoT sensors and decreasing computing power using the ZigBee wireless standards. The medical sensors collect patients' information and transmit it using the ZigBee devices for wireless communication. Along with mutual authentication before data transmission, the RNM-SC approach also overcomes security deficiencies. Furthermore, it acquires the secret generation and sensitive data from cloud systems to network applications and increases network resiliency. Figure 1 illustrates the research flow of the developed components in the proposed approach. In this work, the system model comprises the following assumptions.

i. All IoT-based sensors communicate with their local coordinator.
ii. The local coordinator transmits the network data towards a static base station.
iii. Each IoT-based sensor has restricted transmission power and residual energy.
iv. A malicious attacker may alter, drop, and re-route the monitored data over the wireless medium.

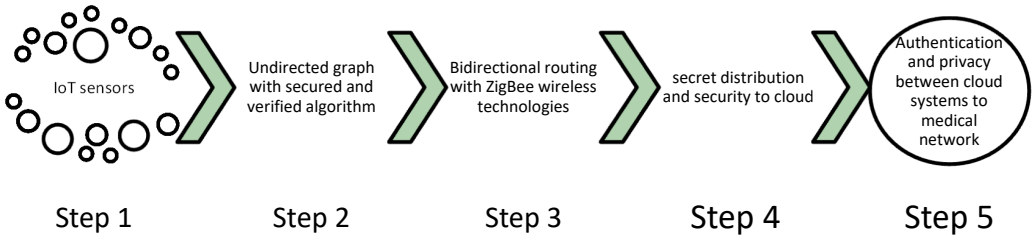

Figure 1. The research components of the proposed network-reliable approach with security.

The RNM-SC approach comprises two main components, and its procedural diagram is illustrated in Figure 2. First, a local nodes table is generated based on predefined distance measurement. In case no neighbors are found in the proximity of the node, then the sources node increases its communication threshold up to a certain limit. Afterward, the proposed approach utilizes the secure and authentic cryptosystem for the generation of private/public keys. Once nodes have their security keys, then they initiate the procedure of bidirectional data transfer. When any node receives an RREQ packet, they compute the heuristic value and share it with the source nodes. Upon receiving the heuristic value, the most optimal nodes are selected for data transfer while balancing load distribution

and energy consumption. The node that belongs to the optimal route is responsible for validating the incoming data packets and performing the process of diffusion to the nodes that are within its local table. These selected nodes forward the incoming packets to their neighbors until the packets are received to the sink node. In the end, verification and validation of the users are performed on network applications, so they can interact with cloud services and obtain the network data.

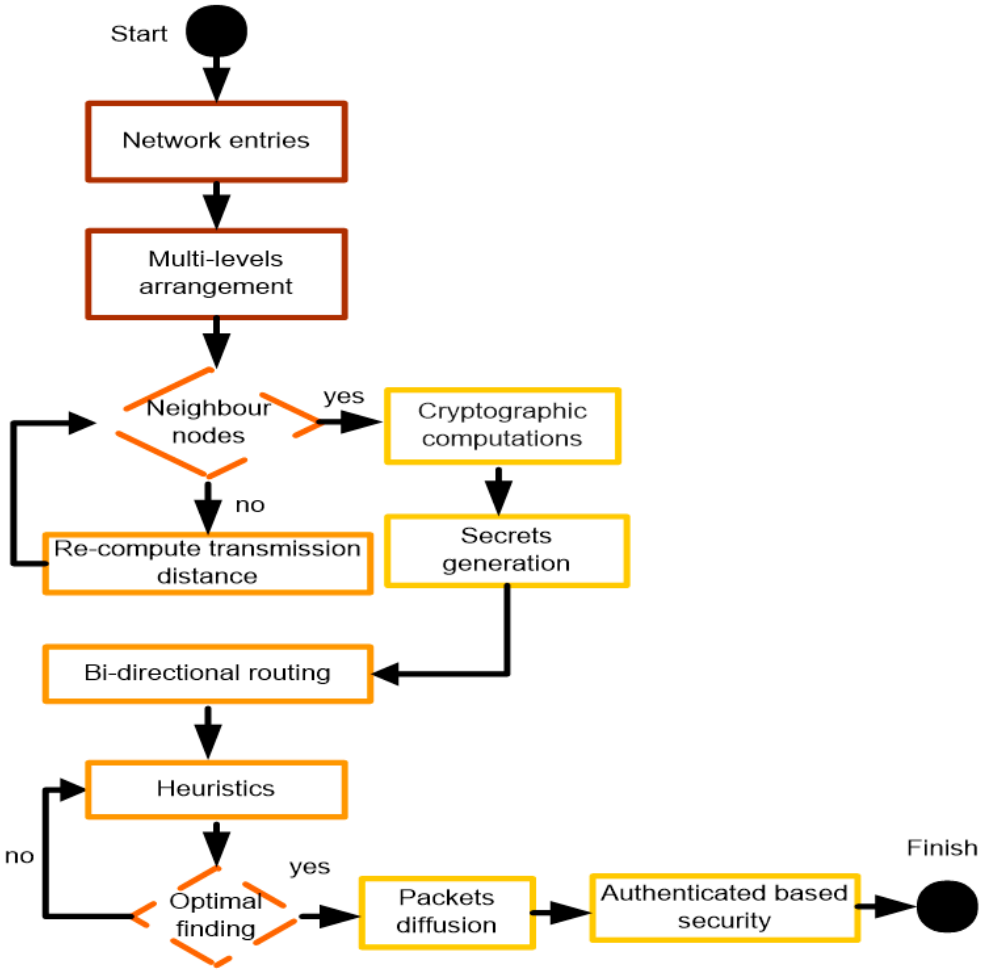

Figure 2. Procedural diagram of the proposed approach.

In the first component, each node maintains entries and constructs a node table. The node table comprises distance to the neighbor node, distance to sink node, residual energy, and unique identity ID. For accomplishment, each node floods the "Hello" packet in its transmission radius. If no response is received, then the node increases its transmission range by an amount of σ distance. If the same node falls in the multiple transmission ranges, then the least distance is considered. After forming the node tables, they are arranged in its undirected graph $G(N, \epsilon)$, which comprises neighbors and edges. Moreover, the constructed graph is organized into different levels. The nodes with the same distance value from the root node are considered in a single level L_i. Accordingly, the level whose distance is closer to the local coordinator requires the least communication cost for routing the health data. Let us consider that $L_0, L_1, L_2, \ldots L_n$ is the set of levels that belongs to the graph $G(N, \epsilon)$. In each level, there is some set of nodes N_i that lies in the specific transmission range. Based on the constructed node table, each node transmits the route request (RREQ) to neighbors, and upon receiving the response, the virtual links are formed for the process of initial routing with the local coordinator. Afterward, the local coordinator initiates the process of key generation and nodes at level L_0 with level L_1 negotiate with each

other for securing data transmission. The local coordinator utilizes Station-to-Station (STS) protocol that uses a key agreement scheme [41]. It is based on the classic Diffie–Hellman algorithm to offer an authentication process for mutual key distribution and confirmation. The local coordinator generates a random number x and transmits the exponential g^x to the sensor node i. Upon receiving, i generates a random number y and exploits exponential g^y to compute the exchanged key $k = g^{xy}$. Moreover, i responds with the exponential g^y and an encrypted token that comprises its signature DS, i.e., $Ek(DS(g^x, g^y)$. Afterward, the local coordinator computes a key k, decrypts the token and confirms the DS using i public key R. Similarly, the local coordinator transmits encrypted digital signature on the exponentials such as $Ek(DS'(g^x, g^y)$. At the end, i confirms the encrypted signature of the local coordinator using k and the public key R of the local coordinator. The RNM-SC approach makes use of the Blum–Goldwasser cryptosystem, which is a semantically secure and asymmetric encryption system [42] for the generation of private-public keys. It chooses two large and independent prime numbers p and q, and computes n as given in Equation (1).

$$n = p \cdot q \tag{1}$$

where n is Blum integer as public-key R and pair of (p, q) ϵ private key P. Its security is based on the difficulty of factoring in the Blum integers. It is known as the most efficient probabilistic encryption algorithm comparable to the RSA encryption scheme for the measurement of speed and data increases [43].

In the next component, the RNM-SC approach utilizes the bidirectional search algorithm to determine the finest and next phased shortest path. Unlike most of the other solutions, it determines the optimal route in two stages simultaneously using the bidirectional method. One stage executes from the source node to the local coordinator, and the other stage from the local coordinator to the source node. The computation of the path from both directions depends on the heuristic function $X(n)$. It is based on three factors, i.e., distance, transmission loss, and nodes' trust. To compute the distance, we use the Euclidean method from a source node to its neighbors $D_{i,n}$. The transmission risk T_r is a product of transmitted packets over time t with a packet reception ratio (PRR). Let us consider if σ denotes the transmission rate and computed as given in Equation (2).

$$\sigma = T_{pkts}/t \tag{2}$$

where T_{pkts} denotes total transmitted packet from source to neighbor. Then, T_r is computed as given in Equation (3).

$$T_r = \sigma \cdot (1/PRR) \tag{3}$$

In Equation (3), if the value of PRR is increasing, then the transmission risk is lower. Accordingly, such a link is given high weightage for data transfer. In the end, node trust N_{tr} denotes its frequency, whose value is fetched from a local table to indicate how many times a particular node is selected for data forwarder. Accordingly, the higher frequency signifies the most reliable node for performing data routing. Thus, $X(n)$ is computed as given in Equation (4).

$$X(n) = D_{i,n} + T_r + N_{tr} \tag{4}$$

The heuristic function not only optimizes the routing performance and increases network resiliency, but due to the adaptation of the bidirectional searching criteria, it also decreases the complexity. Let us consider that m is the midpoint from the initial node to the local coordinator and from the local coordinator to the initial node. Using a bidirectional search algorithm [44], the time complexity t_c is $O\left(b^{\frac{d}{2}}\right)$, where b is the branching factor and d is the distance. In the RNM-SC approach, the local coordinator is further connected with the ZigBee network using wireless routers. The ZigBee routers receive the collected medical information and transmit it towards the sink node using a multi-hop system. Additionally, the ZigBee routers keep track of active routes and eliminate the inactive wireless devices from its routing tables by measuring the status of the link. In the next component, the

RNM-SC approach utilizes Blum–Goldwasser cryptography, an asymmetric key encryption algorithm for securing patients' sensitive data against network attackers. It is an iterative process until biosensing data is delivered to cloud systems. Initially, the sensors' data D is divided into a sequence of k blocks $m_1, m_2, \ldots \ldots, m_k$, selecting a random number r, such that $r < n$ and computes Z_0 as given in Equation (5).

$$Z_0 = r^2 \; mod \; n \tag{5}$$

where, n is a public key of the selected next-hop. Later, using the Blum Blum Shub key generator [45], the values for $Z_1, Z_2, \ldots, \; Z_{i-1}$ are generated as given in Equation (6).

$$Z_i = {Z_{i-1}}^2 \; mod \; n \tag{6}$$

The least significant h bits are determined from the computed Z_i, denoted as l_i and performing Exclusive-OR (XoR) operation with each sensors' data m_i to obtain cipher block C_i at each level, as given in Equation (7).

$$C_i = m_i, l_{i,} \; xor \tag{7}$$

This process is repeated for k blocks of a message M to ensure data encryption and integrity. As the proposed work is based on multi hopping, the obtained ciphertext C_i is reassembled on a cloud system to generate actual M as given in Equation (8).

$$M = C_1 \; ||C_2||C_2||, \ldots .||C_k \tag{8}$$

Moreover, to ensure data confidentiality and authentication among cloud systems and end-users, the proposed approach utilizes a hybrid security mechanism. Firstly, the cloud system generates a secret key S_k and encrypts it with a public key of each end-user P_u for the generation of a session key K_i as given in Equation (9).

$$K_i = E \cdot P_u(S_k) \tag{9}$$

Secondly, upon receiving, the end-user decrypts it using a private key P_k and obtains the session key K_i . Therefore, now both can send/receive the data by performing an encryption operation, as given in Equation (10).

$$D_i = m_i \oplus K_i \tag{10}$$

Algorithm 1 explains the pseudocode of the proposed approach. It comprises three procedures. Firstly, the nodes are organized into an undirected graph and extract the neighbors of the source node. After the extraction of sub-nodes from the constructed graph, the proposed approach executes the process of key distribution and confirmation between the extracted nodes based on the STS algorithm. Secondly, a bidirectional routing procedure is executed and utilizes the weighted heuristics to form the optimal data transferring using IoT devices. It uses the transmission risk, node's trust, and distance parameter to strengthen the routing performance by using Zigbee wireless standards. In the end, the procedure for packet diffusion is initiated and using the security methods, the data is routed towards the cloud tier. After receiving the data packets, node-to-node sessions are created to establish security between the cloud tier and remote IoT device.

Algorithm 1

```
Input:
                    sensor nodes, undirected graph G(ὴ, ϵ)
Output:
                    weighted heuristics, secured devices, authentic sessions
do              nodes i ϵ N
                  if adjacent nodes ! = null then
                        edge ϵ = node(i, j)
                    else
                        return graph G(ὴ, ϵ)
end for
do              extract neighbors i ϵ G(ὴ, ϵ)
                    if i ! = null then
                        compute key generation and confirmation using STS
                    else
                        set transmission distance
                  Repeat step 12
            end if
end for
do bi-directional routing
                X(n) = D_{i,n} + T_r + N_tr
                weighted heuristics
                RREQ to selected X(n) node
end for
do sec_forwarding
                C_i = m_i ⊕ l_i
            M ← C_1 | |C_2| |C_2| | , . . . .| |C_k
end for
        do sec_cloud
                    session key K_i for each user
                    K_i = E·P_u(S_k)
                    applying xor function
                D_i = m_i ⊕ K_i
        end for
end procedure
```

4. Performance Evaluation

We ran a set of experimental tests to validate the operations of the proposed approach and its performance. The RNM-SC approach is based on the Zigbee wireless technology that was designed for the IEEE 802.15.4 standard. It allows battery-powered sensors for information sensing and forwarding by ZigBee devices towards cloud systems in a multi-hop structure. This section presents the simulated execution of the RNM-SC approach using discrete-event simulator NS-3 [46,47]. These experiments evaluated the security and routing resiliency of the RNM-SC approach against other solutions under dynamic conditions for observing medical healthcare. The results were compared with LEACH++ [34] and DSM [30]. The RNM-SC performance was tested using energy consumption, network throughput, packet drop ratio, data threats, and end-to-end delay under the number of jamming nodes. The role of jamming nodes was to obstruct the wireless channels, floods the route request packets and drop the sensors' data. The simulation parameters are defined in Table 1.

Table 1. Simulation parameters.

Parameters	Values
Initial energy	2 j
IoT sensors	250
Deployment	Random
Jamming nodes	3–15
Traffic type	CBR
Transmission power	10 mA
Reception power	15 mA
ZigBee routers	10
Control bits	20 bits
Simulation interval	200 s
Network standard	IEEE 802.15.4
Packet size	64 bits

4.1. Security Analysis

This section provides the security analysis of the RNM-SC approach for key generation, data privacy, integrity, and node-level authentication. Our RNM-SC approach coped with the secure distribution of key management among medical devices and achieved security objectives. It authenticates the communicating sensors while routing the healthcare data using private-public keys. Moreover, the session keys are generated for peer nodes and are valid up to a definite interval. Afterward, the session keys are revoked and associated nodes have to resend the request for the generation of new session keys. The unique nonce is added in the request/response packets of session keys; this avoids their re-generation for unknown nodes. Unlike most other solutions that impose a high computational cost in obtaining data secrecy, the RNM-SC approach uses the Blum–Goldwasser algorithm to distribute private-public asymmetric keys for achieving data privacy and integrity. Additionally, IoT data are divided into chunks, and each chunk is encrypted using a lightweight encryption mathematical function. The encryption process over the unreliable channel imposes less computing overhead on each level based on XoR operation. The proposed security scheme provides data privacy and integrity by utilizing the Blum Blum Shub pseudo numbers generator. Each time the healthcare data arrives towards the next hop using heuristics $X(n)$, it must be carried through an XoR operation with h least significant bits of the key with data bits. Accordingly, the proposed approach increases the security limits iteratively from IoT sensors to cloud servers using hashes. Our proposed security scheme also reduces complexity because it is based on bidirectional routing methods and security assessments. Such a proposed method decreases the number of RREQ messages and makes communicating links less congested. Furthermore, it ensures data security from medical sensors to the cloud systems and provides privacy and shared authentication between cloud systems and end-users using a hybrid security algorithm. The generated session key is for a particular data send/receive, which is further encrypted and decrypted using private-public keys of the cloud system and end-users. The secret key is used for encrypting and decrypting the user request and cloud response. Table 2 illustrates the most common security attacks on network data for constraint nodes and how our proposed approach avoids them.

Table 2. Security analysis of our proposed approach.

Attacks	How the Proposed Approach Avoids Them
Access to network	Unique ID private keys
Request of the key by a malicious node	Nonce and time
Confidentiality	Cipher using public keys
Data disclosure	Decipher with the linked private key
Specious packets delivery	Block the device
Storage overload	Distributed data chunks and diffusion
Data reliability	Data transfer by trusted intermediate nodes
Data integrity	Ciphered in iterative hashes
Complexity	Bidirectional heuristics
Authenticity	Digital signatures

4.2. Results and Discussion

Figure 3 depicts the tested results of the RNM-SC approach with LEACH++ and DSM in terms of network throughput. It is referred to as the transmission of successful data packets from medical sensors to sink nodes. The numerical analysis demonstrates its improved performance by 9% and 14%, respectively. It is because of exploiting the bidirectional routing method to determine the optimal forwarders and avoid direct transmission. The proposed approach most avoided utilizing the direct link due to the limited transmission range and adopted multi-hop communication, which remarkably achieves high throughput. Additionally, it incorporates transmission risk in active routes, which significantly contributes to network throughput. Based on the results, it is observed that other solutions incur additional costs in terms of data delivery performance and decrease the ratio of network throughput. Moreover, most of the other solutions overlook resource constraints, and as a result, that affects the node's lifetime, thereby resulting in reduced throughput performance.

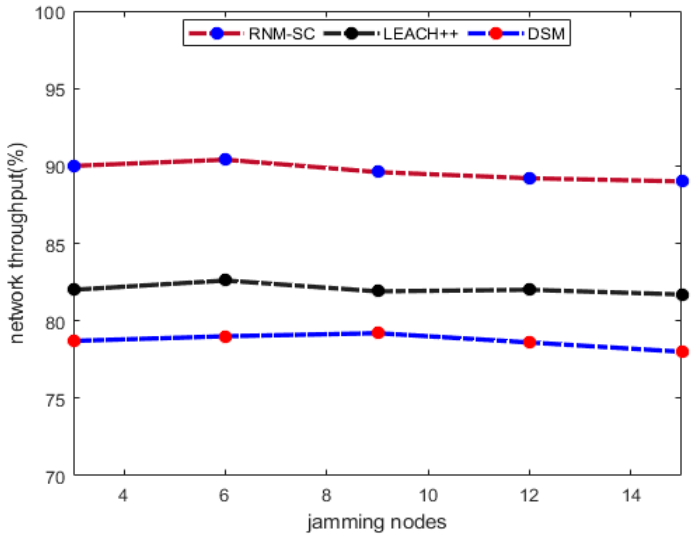

Figure 3. Network throughput and jamming nodes.

Figure 4 describes the tested results of the RNM-SC approach with other solutions in terms of energy consumption and reveals improved performance by 12% and 22%, respectively. The existing solutions consumed extra energy resources in determining the resilient paths and rapidly generated route request packets. Such approaches have seen overloaded communication paths with the existence of jamming nodes and suffer additional consumption of energy resources in timely data delivery. Furthermore, the transmission links are not identified either as risky or normal in the presence of heavy data traffic, and most of the network energy is misused to deal with packet retransmissions.

It is also seen that in routing the healthcare data from medical sensors to the cloud, due to ignoring nodes' trust, few nodes are appointed continually for the role of routing, and ultimately this causes data leakages. Such methods consume unnecessary energy on the part of sensors and affect network performance. The RNM-SC approach decreases the excessive change of control messages in constructing and maintaining data routes from medical sensors to the cloud, which greatly stabilizes the nodes' energy consumption.

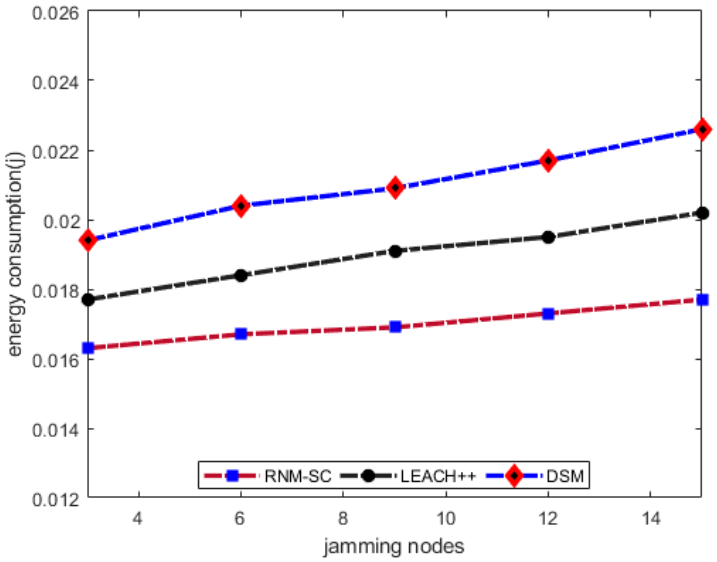

Figure 4. Energy consumption and jamming nodes.

Figure 5 clarifies the tested results of the RNM-SC approach with an existing solution in terms of packet loss ratio. Based on the analysis, it is observed that the RNM-SC model decreases the fraction of packet loss by 30% and 43%, respectively. This improvement is due to the incorporation of nodes' trust and assessment of link risk during the computation of heuristic function. Such incorporation not only strengthened the routes but also offered a robust system for handling the malicious nodes in dropping the actual data packets. Moreover, due to the utilization of bidirectional routing heuristics, the proposed approach decreased the load distribution on the entire route and significantly increased the performance of the packet. Due to the lightweight computing resources, the RNM-SC approach consumes the least energy resources and increases the lifetime of data transmission, which decreases route breakages and packet loss rates. Unlike other solutions that cannot cope with secret generation and distribution only with the authorized nodes, the RNM-SC approach uses the Blum–Goldwasser cryptosystem to avoid malicious entries and increase the packet delivery performance from medical sensors to the cloud servers.

Figure 6 illustrates the performance evaluation of the RNM-SC approach in terms of end-to-end delay against existing work. It was noticed that with the increase in jamming nodes, the interval of data delay also increased. This is due to the flooding of malicious packets and depletion of the nodes' energy with unnecessary processing. However, the tested results showed that the proposed approach improves the evaluation of end-to-end delay by 14%, and 22%, respectively, in the comparison with existing solutions. It is due to the use of the bidirectional searching technique in exploring the shortest and least risky route from the source node towards a destination. It executes two concurrent searches, i.e., one from the medical sensor to a cloud system and one that operates in reverse condition from the cloud system. It is seen from the experiments' analysis that the existing solution causes most of the route failures, and as a result, most of the time is wasted in route re-construction. Such practice is avoided in the RNM-SC approach by increasing the route stability period based on heuristic function, and as a result, the fraction of end-to-end delay is minimized by decreasing the chances of route re-generation from the initial to the goal node. Additionally, with the mutual authentication of the medical sensors based on

private–public keys, the RNM-SC approach declines the false route request packet from the malicious node, and ultimately offers on-time healthcare data transmissions.

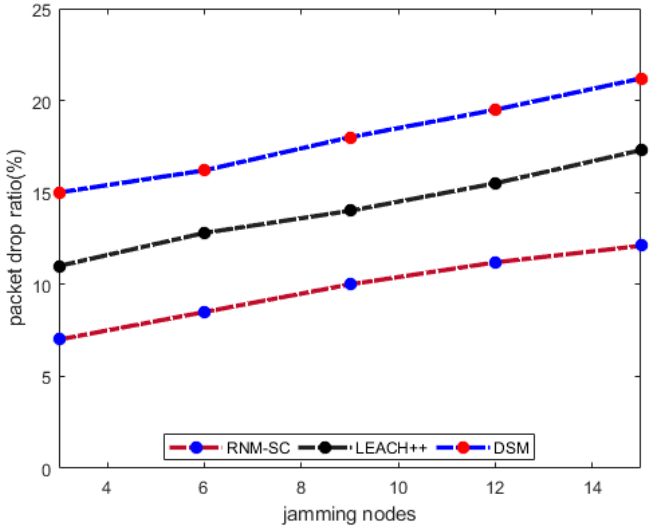

Figure 5. Packet drop ratio and jamming nodes.

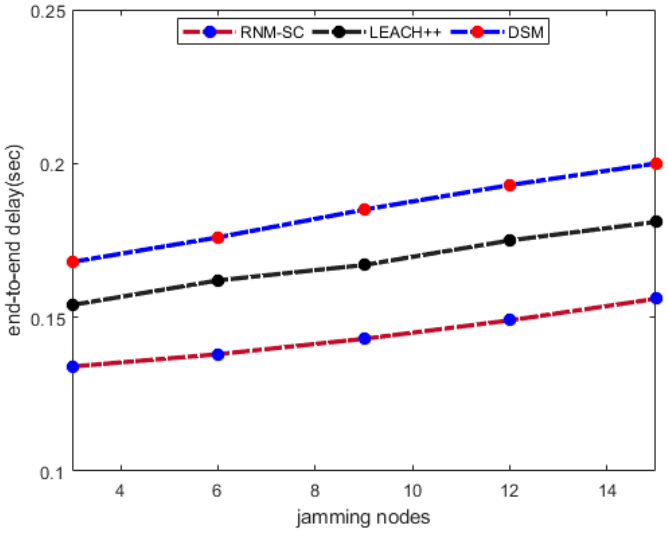

Figure 6. End-to-end delay and jamming nodes.

In Figure 7, the tested results of the RNM-SC approach are compared with an existing solution in terms of routing complexity. The routing complexity increases with the additional overhead of jamming nodes and imposes an unnecessary packet drop ratio. However, analysis of the results demonstrates that the RNM-SC approach significantly decreases routing complexity by 32% and 43%, respectively, compared to other solutions. This is because it imposes the lowest manageable processing costs in finding the medical forwarders to the cloud using a heuristic function in terms of distance, link risk, and nodes' trust. Furthermore, the bidirectional search technique decreases the complexity and determines the optimal routes towards cloud servers in a fraction of time with lower overhead. Unlike other solutions that impose extra control overhead packets while applying security on observing data, our proposed RNM-SC approach iteratively performs data encryption among h least significant bits and secret keys using lightweight XoR operation and also minimizes the overhead on the medical sensors and contributes to network performance.

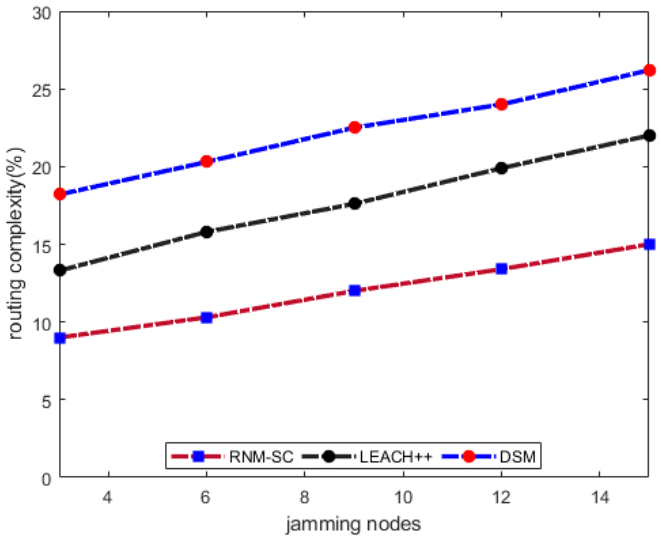

Figure 7. Routing complexity and jamming nodes.

In Figure 8, the tested results of the RNM-SC approach are compared to other solutions in the presence of jamming nodes. It is seen that with increasing numbers of jamming nodes, the ratio of tampered packets also increases. However, the experimental results show that the RNM-SC approach significantly decreased the ratio of tampered packets by 33% and 40%, respectively, compared to the other solutions due to the incorporation of security and authentication algorithms. The proposed approach can tackle malicious objects and achieve reliable forwarding of sensor data even if links are overloaded by malicious packets. Furthermore, the secured cloud model provides trusted communication among cloud systems and connected users with a hybrid mechanism. The proposed security strategy offers an efficient minimum of computing power to analyze the tampered packets and avoid malicious events that disrupt system performance in terms of privacy, authentication, and data integrity. It initiates the process of generating and distrusting the private keys among associated devices. Additionally, the private keys are valid for a certain session and afterward, they are revoked. If any node tries to connect with neighbors without a valid session key, then it is blocked and accordingly, the chances of malicious attacks are nominal in the proposed approach.

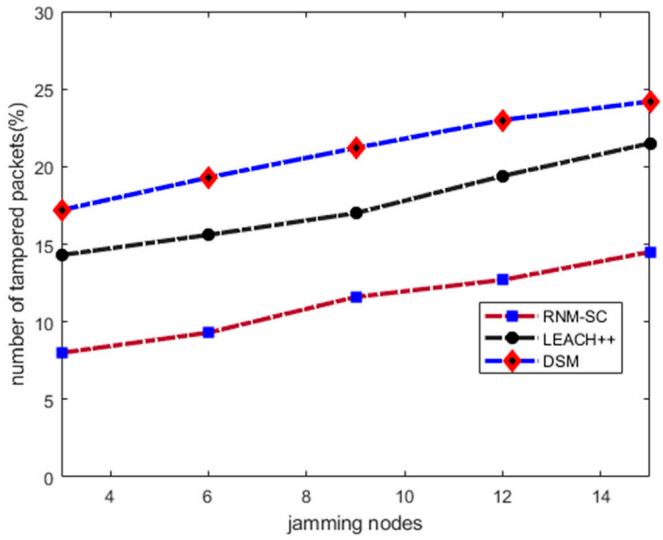

Figure 8. Tampered packets and jamming nodes.

5. Conclusions

Many advanced wireless technologies deal with health management to monitor patients and predict risks regarding their condition. The medical data are transmitted to the care center, and a team of professional doctors receives alerts regarding their patients. This paper presents a reliable network management approach with bidirectional routing for Cloud-based networks using the internet of secured medical things, which aims to decrease the complexity factor in data transmission for medical applications with the least processing cryptosystem. It distributes the secured and verified keys between medical sensors using the STS algorithm, and performs the lesson overhead for achieving privacy and authentication. Additionally, it offers a bidirectional routing method and minimizes the time factor in transferring the medical data towards the cloud tier. Moreover, it also provides a hybrid security mechanism to protect and authenticate the medical store among cloud to physician communication. The proposed model was tested, and numerical results demonstrated its significant improvements in network resiliency and security. However, it has been observed that the proposed model lacks information about medical devices when the IoT network is mobile. In such situations, sensitive information can be easily or erroneously used, and physicians can obtain inaccurate readings of medical data. Thus, in future work, we aim to improve the proposed model's ability to predict channel error rates before forwarding data by using a robust mobility support scheme and further minimizing the computational overhead for both on-body and off-body communication. Moreover, a testbed will be needed to evaluate the proposed approach under realistic network technologies.

Author Contributions: Conceptualization, A.R., K.H. and S.M.F.; Methodology, A.R., K.H.; Software, A.R., S.M.F.; Validation, J.L., L.P.; Formal Analysis, J.L.; Investigation, A.R., L.P.; Resources, J.L.; Data Curation, S.M.F., K.H.; Writing—Original Draft Preparation, A.R., K.H.; Writing—Review & Editing, S.M.F., J.L.; Visualization, L.P.; Supervision, J.L.; Project Administration, A.R.; Funding Acquisition, A.R., J.L. All authors have read and agreed to the published version of the manuscript.

Funding: There is no external funding for this research work.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

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

Conflicts of Interest: Authors declared no conflict of interest.

References

1. 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.* **2019**, *54*, 101995. [CrossRef]
2. Alsamhi, S.H.; Ma, O.; Ansari, M.S.; Meng, Q. Greening internet of things for greener and smarter cities: A survey and future prospects. *Telecommun. Syst.* **2019**, *72*, 609–632. [CrossRef]
3. Alrajeh, N.A.; Khan, S.; Lloret, J.; Loo, J. Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 374796. [CrossRef]
4. Shanthi, G.; Sundarambal, M. FSO–PSO based multihop clustering in WSN for efficient medical building management system. *Clust. Comput.* **2019**, *22*, 12157–12168. [CrossRef]
5. Verma, V.K.; Gupta, P.; Jha, A.V.; Barbhuiya, P.N. Recent trends in wireless sensors for medical applications. In Proceedings of the 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 6–8 April 2017.
6. Shahraki, A.; Taherkordi, A.; Haugen, Ø.; Eliassen, F. A survey and future directions on clustering: From WSNs to IoT and modern networking paradigms. *IEEE Trans. Netw. Serv. Manag.* **2020**, *18*, 2242–2274. [CrossRef]
7. 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]
8. Sodhro, A.H.; Sangaiah, A.K.; Pirphulal, S.; Sekhari, A.; Ouzrout, Y. Green media-aware medical IoT system. *Multimed. Tools Appl.* **2019**, *78*, 3045–3064. [CrossRef]

9. Celesti, A.; Ruggeri, A.; Fazio, M.; Galletta, A.; Villari, M.; Romano, A. Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds. *Sensors* **2020**, *20*, 2590. [CrossRef]
10. Cui, Z.; Fei XU, E.; Zhang, S.; Cai, X.; Cao, Y.; Zhang, W.; Chen, J. A hybrid BlockChain-based identity authentication scheme for multi-WSN. *IEEE Trans. Serv. Comput.* **2020**, *13*, 241–251. [CrossRef]
11. Alzahrani, B.A.; Irshad, A.; Albeshri, A.; Alsubhi, K. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. *Wirel. Pers. Commun.* **2021**, *117*, 47–69. [CrossRef]
12. Abouelmehdi, K.; Beni-Hessane, A.; Khaloufi, H. Big healthcare data: Preserving security and privacy. *J. Big Data* **2018**, *5*, 1. [CrossRef]
13. Elhoseny, M.; Ramírez-González, G.; Abu-Elnasr, O.M.; Shawkat, S.A.; Arunkumar, N.; Farouk, A. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access* **2018**, *6*, 20596–20608. [CrossRef]
14. Oteafy, S.M.A.; Hassanein, H.S. Resilient IoT architectures over dynamic sensor networks with adaptive components. *IEEE Internet Things J.* **2016**, *4*, 474–483. [CrossRef]
15. Benkhelifa, E.; Welsh, T.; Hamouda, W. A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3496–3509. [CrossRef]
16. Sterbenz, J.P. Smart city and IoT resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities. In Proceedings of the 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM), Alghero, Italy, 4–6 September 2017.
17. Khan, M.A.; Khan, S.; Shams, B.; Lloret, J. Distributed flood attack detection mechanism using artificial neural network in wireless mesh networks. *Secur. Commun. Netw.* **2016**, *9*, 2715–2729. [CrossRef]
18. Garcia, M.; Lloret, J.; Sendra, S.; Lacuesta, R. Secure communications in group-based wireless sensor networks. *Int. J. Commun. Netw. Inf. Secur.* **2010**, *2*, 8.
19. Haseeb, K.; Ud Din, I.; Almogren, A.; Islam, N. An energy efficient and secure IoT-based WSN framework: An application to smart agriculture. *Sensors* **2020**, *20*, 2081. [CrossRef] [PubMed]
20. Krishnamoorthy, S.; Dua, A.; Gupta, S. Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–47. [CrossRef]
21. 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]
22. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Ahmed, Z. Ahmed, Mobility Support 5G Architecture with Real-Time Routing for Sustainable Smart Cities. *Sustainability* **2021**, *13*, 9092. [CrossRef]
23. Rashid, M.; Parah, S.A.; Wani, A.R.; Gupta, S.K. Securing E-Health IoT Data on Cloud Systems Using Novel Extended Role Based Access Control Model. In *Internet of Things (IoT)*; Springer: Cham, Switzerland, 2020; pp. 473–489. [CrossRef]
24. Butpheng, C.; Yeh, K.H.; Xiong, H. Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry* **2020**, *12*, 1191. [CrossRef]
25. Sengupta, S.; Bhunia, S.S. Secure Data Management in Cloudlet assisted IoT Enabled e-Health Framework in Smart City. *IEEE Sens. J.* **2020**, *20*, 9581–9588. [CrossRef]
26. 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]
27. Zhang, Y.; Yang, M.; Zheng, D.; Lang, P.; Wu, A.; Chen, C. Efficient and secure big data storage system with leakage resilience in cloud computing. *Soft Comput.* **2018**, *22*, 7763–7772. [CrossRef]
28. Zhang, Y.; Lang, P.; Zheng, D.; Yang, M.; Guo, R. A secure and privacy-aware smart health system with secret key leakage resilience. *Secur. Commun. Netw.* **2018**, *2018*, 1–13. [CrossRef]
29. Liu, J.; Cao, H.; Li, Q.; Cai, F.; Du, X.; Guizani, M. A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing. *IEEE Internet Things J.* **2018**, *6*, 1321–1330. [CrossRef]
30. Babar, M.; Tariq, M.U.; Jan, M.A. Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid. *Sustain. Cities Soc.* **2020**, *62*, 102370. [CrossRef]
31. Ever, Y.K. Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks. *IEEE Syst. J.* **2018**, *13*, 456–467. [CrossRef]
32. Hayajneh, T.; Griggs, K.; Imran, M.; Mohd, B.J. Secure and efficient data delivery for fog-assisted wireless body area networks. *Peer-to-Peer Netw. Appl.* **2019**, *12*, 1289–1307. [CrossRef]
33. Qi, X.; Li, B.; Chu, Z.; Huang, K.; Chen, H.; Fei, Z. Secrecy energy efficiency performance in communication networks with mobile sinks. *Phys. Commun.* **2019**, *32*, 41–49. [CrossRef]
34. Farooqi, A.H.; Khan, F.A. Securing wireless sensor networks for improved performance in cloud-based environments. *Ann. Telecommun.* **2017**, *72*, 265–282. [CrossRef]
35. Zhang, Y.; Deng, R.H.; Han, G.; Zheng, D. Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things. *J. Netw. Comput. Appl.* **2018**, *123*, 89–100. [CrossRef]
36. Pasha, M.; Shah SM, W. Framework for E-Health systems in IoT-based environments. *Wirel. Commun. Mob. Comput.* **2018**, *2018*. [CrossRef]
37. Pirbhulal, S.; Samuel, O.W.; Wu, W.; Sangaiah, A.K.; Li, G. A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Gener. Comput. Syst.* **2019**, *95*, 382–391. [CrossRef]

38. Al-Janabi, S.; Al-Shourbaji, I.; Shojafar, M.; Shamshirband, S. Shamshirband, Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt. Inform. J.* **2017**, *18*, 113–122. [CrossRef]
39. Haghighi, S.M.; Torabi, S.A. Torabi, A novel mixed sustainability-resilience framework for evaluating hospital information systems. *Int. J. Med. Inform.* **2018**, *118*, 16–28. [CrossRef]
40. Petrellis, N.; Birbas, M.; Gioulekas, F. On the design of low-cost IoT sensor node for e-health environments. *Electronics* **2019**, *8*, 178. [CrossRef]
41. Diffie, W.; Van Oorschot, P.; Wiener, M.J. Wiener, Authentication and authenticated key exchanges. *Des. Codes Cryptogr.* **1992**, *2*, 107–125. [CrossRef]
42. Blum, M.; Goldwasser, S. An efficient probabilistic public-key encryption scheme which hides all partial information. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1984.
43. Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1996.
44. Pearl, J.; Korf, R.E. Search techniques. *Annu. Rev. Comput. Sci.* **1987**, *2*, 451–467. [CrossRef]
45. Blum, L.; Blum, M.; Shub, M. A simple unpredictable pseudo-random number generator. *SIAM J. Comput.* **1986**, *15*, 364–383. [CrossRef]
46. Coudron, M.; Secci, S. An implementation of multipath TCP in ns3. *Comput. Netw.* **2017**, *116*, 1–11. [CrossRef]
47. Kumar, A.A.; Rao, S.; Goswami, D. Ns3 simulator for a study of data center networks. In Proceedings of the 2013 IEEE 12th International Symposium on Parallel and Distributed Computing, Bucharest, Romania, 27–30 June 2013.