energies

MDPI

Article

IoT Solution for AI-Enabled PRIVACY-PRESERVING with Big Data Transferring: An Application for Healthcare Using Blockchain

Mohamed Elhoseny [1,2,*], Khalid Haseeb [3], Asghar Ali Shah [4], Irshad Ahmad [3], Zahoor Jan [3] and Mohammed. I. Alghamdi [5]

[1] Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt
[2] Computer Information Technology and the Manager of the Research Support Department, American University in the Emirates, Dubai 503000, United Arab Emirates
[3] Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan; khalid.haseeb@icp.edu.pk (K.H.); irshad@icp.edu.pk (I.A.); zahoor.jan@icp.edu.pk (Z.J.)
[4] Department of Computer Science, Bahria University Lahore Campus, Lahore 54600, Pakistan; asgharali.bulc@bahria.edu.pk
[5] Department of Computer Science, Al-Baha University, Al Bahah 1988, Saudi Arabia; alghamdi@alumni.nmt.edu
* Correspondence: melhoseny@ieee.org

Abstract: Internet of Things (IoT) performs a vital role in providing connectivity between computing devices, processes, and things. It significantly increases the communication facilities and giving up-to-date information to distributed networks. On the other hand, the techniques of artificial intelligence offer numerous and valuable services in emerging fields. An IoT-based healthcare solution facilitates patients, hospitals, and professionals to observe real-time and critical data. In the literature, most of the solution suffers from data intermission, high ethical standards, and trustworthiness communication. Moreover, network interruption with recurrent expose of sensitive and personal health data decreases the reliance on network systems. Therefore, this paper intends to propose an IoT solution for AI-enabled privacy-preserving with big data transferring using blockchain. Firstly, the proposed algorithm uses a graph-modeling to develop a scalable and reliable system for gathering and transmitting data. In addition, it extracts the subset of nodes using the artificial intelligence approach and achieves efficient services for the healthcare system. Secondly, symmetric-based digital certificates are utilized to offer authentic and confidential transmission with communication resources using blockchain. The proposed algorithm is explored with existing solutions through multiple simulations and proved improvement in terms of realistic parameters.

Keywords: Internet of things; embedded applications; big data; insecure channels; constraint network

check for updates

Citation: Elhoseny, M.; Haseeb, K.; Shah, A.A.; Ahmad, I.; Jan, Z.; Alghamdi, M.I. IoT Solution for AI-Enabled PRIVACY-PRESERving with Big Data Transferring: An Application for Healthcare Using Blockchain. *Energies* **2021**, *14*, 5364. https://doi.org/10.3390/en14175364

Academic Editors: Francesco Bellotti and Riccardo Berta

Received: 18 July 2021
Accepted: 24 August 2021
Published: 28 August 2021

1. Introduction

In recent decades, wireless communication plays a vital role in the medical industry's growth, smart cities, vehicular and transportation systems using IoT networks [1–3]. The wireless nodes are dispersed in the observing field for collecting the related data and further transmit it towards the cloud paradigm. The application users using the internet and access the needed information directly on their smartphones and computing machines. Almost all critical applications need an on-time response from the sensing objects and facilitate their users. The architecture of wireless networks consists of small, less expansive, and low-powered intelligent sensors distributed either uniformly or randomly in various fields, i.e., military, agriculture, healthcare, smart cities, and grids for information observing [4–6]. The sensory data is collected based on particular events or periodic intervals and transmitted to centralized servers. In medical applications [7–9], the medical experts access the patients' information from centralized or distributed servers using the internet through some developing next-generation wireless techniques. However, the traditional data analysis techniques are incompatible to extract useful health information; therefore, most academics are focusing on intelligent methods with the internet of medical things for a precise and thorough exploration of patients' sensitive data. Health services widely adopt the internet of medical items due to its significant impact on diagnosing disease and facilitating treatments with the least communication cost. The medical applications are comprised of three main phases. In the first phase, wearable sensors collected the patients' data and forwarded them to a local administrator or coordinator. The second phase communicates the patients' data to the server or sinks node with the intermediate devices over the wireless transmission system. Finally, the medical data is stored on some cloud service providers; thus, medical professionals judge the patients' condition and provides suitable actions. In the flat-based structure with the same processing, receiving, forwarding, and storage capabilities. Moreover, in the flat-based structure, many researchers have been proposed a cluster-based solution [10–12] to divide the medical sensors into different clusters with one cluster head in each cluster. Some applications are also based on a hierarchical structure [13–15], and the data aggregation capabilities are separated based on different levels. The massive medical data is stored on cloud servers and moves wirelessly over the insecure forwarding medium. Therefore, secure and privacy-preserving solutions for sustainable systems are demanding factors and need to maintain the resources efficiently [16–19]. The purpose of this research work is to explore blockchain, which is an emerging technology [20,21] to improve the performance of the healthcare system against security extortions with efficient data management. The technology of blockchain is a distributed database, which is comprised of various blocks that are linked together using irreversible chains. A block is a single element, and it is composed of information related to a specific transaction. Recently, blockchain is an emerging technology and has been applied by many researchers to secure confidential data over insecure transmission systems [22,23].

The main contributions of our proposed solution are:

i. It presents a graph-oriented model for collecting and distributing network information with an accessible and efficient system.
ii. Artificial intelligence techniques are utilized for producing the least error-prone communication with decreasing delays by avoiding unnecessary malicious traffic.
iii. A reliable and authentic sharing system is modeled against threats by supporting symmetric digital certificates.
iv. The distributed security is provided by exploiting blockchain technology in which data is encrypted and dispersed in a decentralized model.
v. The measurement of the proposed work with a set of simulation-based experiments has demonstrated significant performance with other schemes in a trustless environment.

The rest of the research article is organized as follows. A discussion of related work is presented in Section 2. Section 3 offers and explains the main components of the proposed algorithm. Section 4 analyzes the performance of the proposed algorithm than existing work through simulations. Section 5 concludes the paper.

2. Related Work

In wireless technology using IoT [24–26], several smart sensors and physical objects are distributed in smart cities to support real-time systems. Furthermore, one or more Base Station (BS), which has unlimited resources, is connected to the internet, facilitating many application users simultaneously. In a wireless sensor network (WSN)-based medical system, the Denial of Service (DOS) attacks are categorized into three different approaches, i.e., standalone, distributive/cooperative, and hierarchical [27,28]. Each sensor node has been equipped with its defense agent in a standalone approach and can only identify the attack by itself. In the distributed defense approach, a global defense system is generated based on various agents' collaboration. Its performance is better than the standalone defense system and is usually preferred for flat topologies. In a hierarchical defense approach, the cluster head is responsible for detecting an attack for its members and performing appropriate security actions with efficient energy efficiency [29,30]. The authors [31] proposed intrusion detection in homogeneous and heterogeneous WSNs, proposing two detection models for classifying the malicious nodes. The detection probability is based on the distance traveled by the malicious node, the likelihood of detecting the malicious node, and the average distance traveled by the malicious node parameters. In [32], authors have proposed a multi-level intrusion detection system based on an immune theory known as Danger theory. The proposed solution uses the various functions of immune cells to design the multi-level intrusion detection system. The proposed solution is based on battery power, message or data size, and data transfer parameters to detect malicious activities.

Furthermore, a few nodes were placed near BS to perform immune nodes' roles and specific processing capabilities. In [33], the authors proposed an improved secure authentication and data encryption scheme for medical systems using the Internet of things (IoT). It provides user anonymity and avoids network threats of replay and password/sensed data disclosure. Moreover, the authors modified the authentication process and decreasing the redundancy in the design phase. It was verified that the proposed solution is more efficient in terms of performance than other schemes. The authors of [34] established an association with body sensors using tokens, and afterward, a secret key is shared to provide data security. The proposed solution encrypts and decrypts the health data with two phases of the authentication method using the private key. The collected data is forwarded to the server using blockchain technology. The security analysis described the feasibility of the proposed solution for securing healthcare information. In [35], the authors proposed a user authentication scheme and data transmission mechanism to provide privacy and security. It offers efficient monitoring facilitates to medical experts and comprehensive treatment to patients. It uses smart cards and passwords, so only authorized medical experts can access patient information. In addition, a secure cryptosystem has been applied to form a data transmission mechanism. Furthermore, the proposed work can cope with common network attacks. The authors in [36], proposed a fine-grained EHR access control scheme and provides a secure standard model. The proposed solution generates offline encrypted data before knowing EHR data and access policies and it offers secure communication for the mobile cloud. The extensive simulation experiments are performed and it is proven effective performance in the comparison of other solutions. In [37], the authors emphasize flexible compute-intensive task offloading to a local cloud, which aims to improve the network performance for energy consumption, cost, and operation speed. They proposed a fruit fly optimization-based task offloading (FOTO) algorithm, which improves the data offloading and allocation of network resources with affordable energy consumption. Its performance is verified in terms of different realistic factors and demonstrates a significant improvement from other existing work.

The secure knowledge and cluster-based intrusion detection mechanism proposed in [38], aims to handle generated intrusions. It stores the particular events triggered by the node in the network field, and the knowledge base is situated on the BS. Based on inference engine cluster heads, the proposed solution stores the events data into the knowledge base. The authors of [39] proposed intrusion detection based on state context and hierarchical trust in WSN. The proposed solution is based on the dynamic state context and hierarchical trust of sensor nodes. In the proposed solution, the trust evaluation and the self-adaptation detection threshold are used to detect malicious nodes' behavior. In [40], the authors developed a biometric-based security framework using resource-constrain-oriented and wearable sensors. It extracts the heartbeats from ECG signals and analyses time-domain-based biometric features. The proposed framework is significantly optimizing the security and transmission for medical applications. In [41], the authors explored privacy-protected data collection challenges and presented a practical framework called Privacy Protector, patient privacy-protected data collection. It consists of secret sharing and shares repairing for compromised and lost patients' information. The proposed framework uses a distributed database, which comprises multiple cloud servers and guaranteed data privacy. The authors of [42] developed a secure data collection scheme for IoT-based healthcare systems named SecureData, which aims to cope with data security. It comprises four main layers. It utilizes a lightweight field-programmable gate array (FPGA) hardware-based cipher and secret cipher share algorithms. For the cloud computing layer, the proposed solution applied a distributed database technique that includes several cloud data servers to ensure privacy for patients' data. The performance results are validated through simulations and it is proven that the proposed solution is significantly efficient for saving security risks for IoT-based healthcare applications.

IoT technology is widely utilized for data collection and offers heterogeneous services for healthcare systems. The public health data collecting a vast number of patient's data, which need to be processed and evaluated to diagnose diseases for a timely and appropriate cure. However, due to the restricted structure and rapid collapse of medical sensors', there are many communication threats that expose patients' information, therefore, it is a demand for trustworthiness with a secured network. It is also noticed that most of the existing solution increases the management cost in sustaining and handling the network data. Moreover, many secured solutions have been developed for IoT networks and tackle with privacy-preserving, but with the unnecessary complexity and runtime overhead. Therefore, this research article presents an AI-enabled privacy-preserving with big data transferring using blockchain technology, which aims to offer a secured network and attain data confidentiality with optimized services. It also enhances the availability of network resources and provides reliability for public health data without compromising the constraint parameters and communication links.

3. Proposed Algorithm

In this section, we explain the detailed overview of our proposed algorithm. The proposed algorithm is based on two main components. The first component uses a graph-based modeling and artificial intelligence technique to arrange the network for stable communication, which is comprised of regions with cluster heads. The sub-graphs are also constructed to reduce the complexity and congestion in the forming of consistent routes from local sensors to sink nodes and eliminate the redundant links. On the other hand, the second component presents an authentication phase based on symmetric digital certificates, which increases the network strength against unauthorized nodes. Moreover, data security for integrity is obtained using blockchain technology, which leads to trustworthy communication in distributed approach and ensures a sustainable healthcare system. Figure 1 demonstrates the main components of the proposed algorithm. Moreover, its communication flow is depicted in Figure 2. For the convenience of describing the proposed solution, the used notations are summarized in Table 1.

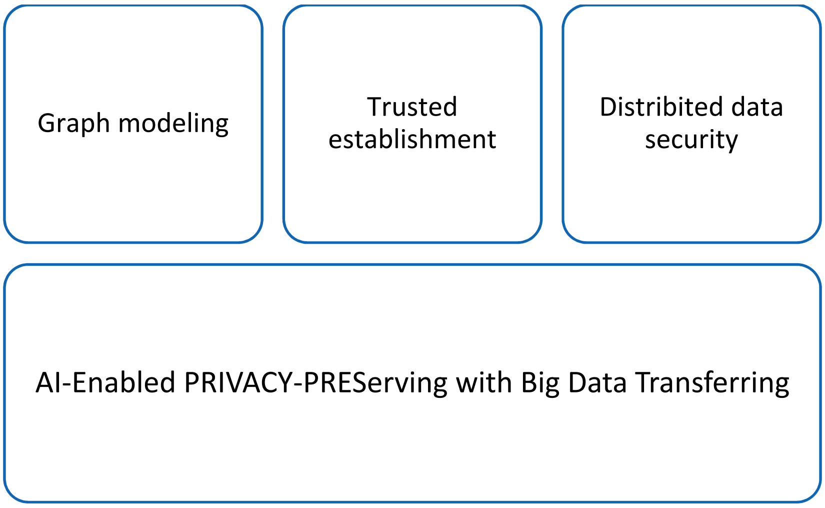
Graph modeling
Trusted establishment
Distribited data security
AI-Enabled PRIVACY-PREServing with Big Data Transferring

Figure 1. Components of the proposed algorithm.

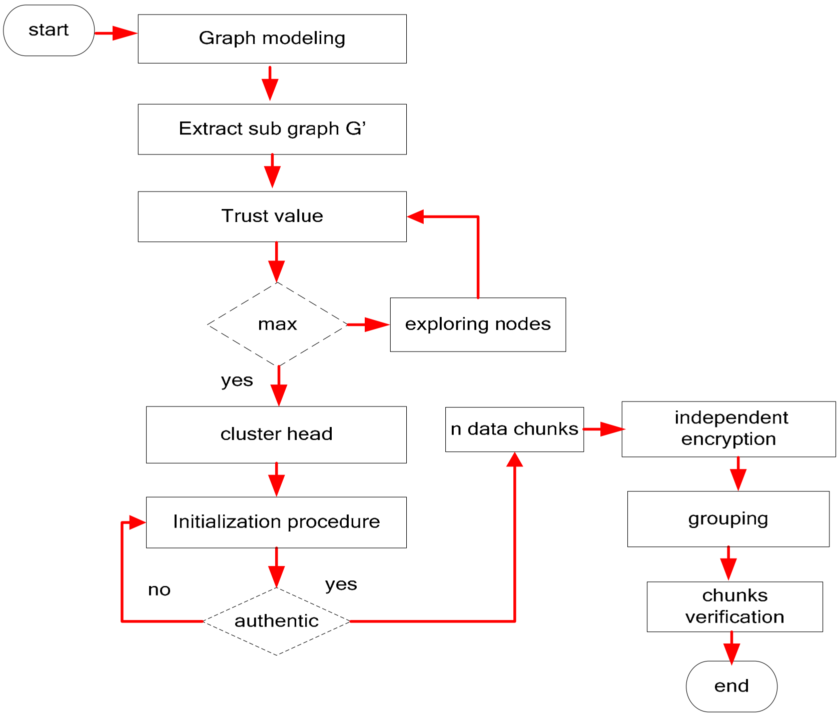

Figure 2. Communication flow of the AI-EPP algorithm.

Table 1. List of notations.

Notations	**Definitions**
$G(N, \epsilon)$	graph with N nodes and ϵ edges
$G'(N', \epsilon')$	The Subgraph with N' And ϵ' edges
W_i	Weighted edges
$T(v)$	trust value
NE_i	residual energy
ND_i	node density
Tx	transmission power
$RSSI$	received signal strength interference
M_k	beacon message threshold
d	distance
IV	initialization vector
Req_p	request packet
T_s	timestamp
$\oplus$	XoR function
S_k	Secret key
MS_k	Master secret key
$cert$	digital certificate
$M_0,\ M_1, \ldots .\ M_n$	chain of messages

With the ability to develop the proposed algorithm using IoT technology and capabilities of wireless sensors, we simulate the performance for a realistic scenario under the following assumptions:

i. The IoT-based network is restricted for battery power, memory, transmission, and processing factors.
ii. They are immobile and equipped with Global Positioning System (GPS).
iii. The wireless channels are asymmetric.
iv. Corresponding nodes can adjust the transmission power using the distance property.
v. Intruders are malicious objects and can generate bogus packets for the response.

3.1. Intellectual Graph-Based Modeling

The proposed algorithm's main aim is to use graph-based modeling and split the network nodes into various groups. Unlike most of the other techniques, the graph-based approach does not know the dimension for grouping and takes an input of undirected weighted graph $G(N, \epsilon)$, which comprises vertices N and bidirectional edges ϵ. Initially, nodes are placed on their appropriate positions in $G(N, \epsilon)$ using the cost function $f(c)$, which is comprised of distance and energy parameters. In addition, each node marks the entry of its neighbors on the local_table. After the formation of an undirected graph $G(N, \epsilon)$, the BS runs the Prims algorithm [43] to identify the subset of nodes without any redundant cycles and parallel edges ϵ. It gives sub-graph $G'(N', \epsilon')$, where N' is extracted vertices and ϵ' is extracted edges. It increases the size of $G'(N', \epsilon')$ by extracting one node at a time from $G(N, \epsilon)$ such that $N' = N$ and ϵ' is a subset of ϵ. The summation of weighted values $\sum W_i$ of extracted vertices and edges is minimized to obtain the optimal performance, where W_i can be computed as given in Equation (1).

$$W_i = W_i + f(c) \tag{1}$$

It aims to determine the subset of the edges that forms a tree, which comprises the subset of nodes. Such an approach explicitly decreases the overhead in developing an optimal delivery service for the e-health system by removing the redundant links. Next, the proposed algorithm computes the trust value $T(v)$ for the nodes in obtaining sub-graph $G'(N', \epsilon')$, and selects the trustworthy with the highest transmission power cluster heads. The trusted value of the sensor node i is computed in an aggregated manner using three-node parameters, i.e., residual energy NE_i, node density ND_i, and received signal strength interference $RSSI_i$ as given in Equation (2). The trust value increases the network performance in terms of least data distance and neighboring cost with high signal strength.

$$T(v_i) = NE_i + ND_i + RSSI_i \tag{2}$$

In Equation (1), NE_i is the fraction of residual energy over the initial energy at the end of the duty cycle. It increases the probability for the selection of cluster head when it increases from the preset threshold. Secondly, the density of the node ND_i denotes the relation tightness between the neighbors, and it is calculated using the derived $G'(N', \epsilon')$. The higher the nodes' density increases the probability of the node selecting the cluster head. In the end, the node i whose link estimation $RSSI$ value is on an extreme level than its neighbors is given a high probability for the selection of cluster head. Let us consider Tx is the transmission power, and α denotes the depleted radio power in transmitting the beacon messages M_k over the distance d, then $RSSI_i$ is computed as given in Equation (3).

$$RSSI_i = Tx - \alpha\,(M_k)\,.\,d \tag{3}$$

Accordingly, based on the highest $T(v_i)$ value, the proposed algorithm chooses the set of particular cluster heads. The cluster heads select the next-hop nodes from sub-graph $G'(N', \epsilon')$ and formulate individual clusters. Next, cluster heads send the status message to their members, and upon receiving the ACK messages, the particular cluster head constructs a cluster_table. Moreover, the IDs of the selected cluster heads are stored with the BS in its global table. Similarly, the member nodes also map the ID of their selected cluster heads in their local_tables. Furthermore, the neighboring cluster heads sharing their information, and accordingly, every cluster head makes an entry in the local cluster_table. All the tables are updated when any changes incur in the processes of network structure.

3.2. Secured Transmissions

This section presents the security component for the proposed algorithm and aims to prevent network intruders from the transmission system. It is comprised of registration, verification, and encryption phases. In this component, the BS is treated as a central authority (CA) and can be valuable for two-way mutual authentication along with privacy-preserving routing. All the selected cluster heads must be registered with BS and obtained digital certificates. Without the digital certificate, the particular cluster head can not participate in the routing phase. The registration and verification phases consist of the following steps.

Cluster head i generates a secret key S_k and shared it with BS over the secure channel. It embedded S_k with identity ID, timestamp T_s and create a request packet $Req_p(ID, S_k, U)$. The Req_p is forwarded to BS for issuing digital certificates. The Req_p is encrypted using a master secret key of MS_k of BS as given in Equation (4).

$$E(MS_k\ (ID||T_s||U)+r_0 \tag{4}$$

where r_0 denotes the random number.

Upon receiving the Req_p from cluster head, BS first verifies identities IDs from its global table, and accordingly, it generates the *cert* including RSA signature [44] S' to verify its authenticity as given in Equation (5).

$$BS \rightarrow i\ : cert(ID,\ T_s,\ S_k,\ S') \tag{5}$$

After obtaining the BS certificates, the cluster heads i and j exchange their certificates with each other to prove two-way mutual authentication before transmitting. Furthermore, the digital certificates are usable for only the particular period Δt, and afterward, the cluster heads are required to resend Req_p towards BS for the issuance of *cert*.

In addition, the r_0 is useful to prevent the malicious node from resending the Req_p packet towards BS. Such a mechanism in the proposed algorithm prevents the replay threat and ensures reliable message forwarding between routing nodes. Further, digital certificates are digitally signed by the master secret key of BS MS_k that indicates its validity. Before transmitting the routing data, both clusters heads i and $i+1$ exchange *cert* with each other. Upon receiving, they are decrypted to recover the secret keys S_k as given in Equation (6).

$$S_k : D(cert(MS_k),\ i) \tag{6}$$

After the completion of the registration and mutual verification phases, the block of data messages $M_0,\ M_1, \ldots.,\ M_n\ \epsilon\ M$ set as encrypted blocks C_i independently by using S_k and XoR $\oplus$ function as given in Equation (7).

$$C_i\ = M\ \oplus\ S_k \tag{7}$$

The cluster head $i+1$ is selected from the chain and decodes the incoming encrypted blocks with the same S_k. Later, it performs the same hashing procedure to generate C_{i+1} with its actual data message M and $\oplus$ operation. Furthermore, received hash code C_i is linked to ensuring blockchain and distributed security E to support data integrity as given in Equation (8).

$$E = Xor(C_i\ , \ldots.\ C_n) \tag{8}$$

Afterward, the pattern of C_i blocks are encrypted using MS_k of BS and forwarded to cloud systems. Upon receiving, the decryption function is applied to integrate the C_i and MS_k.

Algorithm 1 gives the flow of the proposed work.

Algorithm 1: AI-enabled privacy-preserving big data algorithm.

```
Initialization
Input: sensors, data messages
Output: graph-oriented transmission paths
for Sensor $S_i$ ϵ $G(N, \epsilon)$ do
extract subset of nodes
initial routes to sink
end
for Sensor $S_i$ ϵ $G'(N', \epsilon')$ do
compute trust $T(v_i) = NE_i + ND_i + RSSI_i$
generate sub-regions
end
BS generates digital certificates
encryption function
If decryption is successful then
cert is validated
Else
cert is rejected
end
end
block of data $M_0,\ M_1, \ldots.,\ M_n$ ϵ $M$
for $M_{\mathrm{i}}$ ϵ $M$ do
produce cipher blocks $C_i$
$C_i\ = M \oplus k_{i+1}$
end
hashes with end-to-end encryption
$E = Xor(C_i\,, \ldots.\ C_n)$
End
```

4. Performance Analysis

This section explains the comparative analysis of the proposed work along with the simulation environment. To verify the complexity and energy usage of the proposed work, the experiments were conducted using two different scenarios, i.e., with the varying number of nodes and varying data rates. The performance is evaluated using various network metrics such as network delivery ratio, network latency, energy consumption, malicious attacks, runtime overhead, link disconnectivity, and complexity. The number of nodes varied from 50 to 250, and data rates increased from 8 bytes to 40 bytes per second. We increased the data generation rates to verify the runtime and processing overheads of the proposed algorithm on nodes as compared to other solutions. Initially, the energy level was set to 2j. In the implementation phase, a discrete event-based network simulator NS-3 was used, which is widely utilized in [45,46]. The simulation was run for 2000 sec. The transmission power was set to 5 m. The number of jamming nodes was assumed as 5. The default simulation parameters are displayed in Table 2.

In Figures 3 and 4, the experimental analysis shows that the proposed AI-EPP has improved network delivery by 14% and 15% than the existing solutions. Such improvement is the choice of the graph-based artificial intelligence technique for splitting the observing field. It eliminates the process of direct data delivery toward a destination and utilizes the constraint resources efficiently. Moreover, the clusters cooperate in multi-hop with a secure strategy and reduce the probability of packet drop rate in the presence of malicious and unexpected events. The proposed AI-EPP algorithm produces much more stable and consistent data transportation because of using the up-to-date measurement of the network field. It decreases the chances to adopt the longer route and distribute the forwarders load in a balanced manner by splitting it into various chunks. In Figures 5 and 6, the experimental results have shown that the proposed AI-EPP pointedly decreases the ratio of network latency by 41% and 39% than other solutions. The existing solutions incur high blockage and interruption costs under varying network nodes. Therefore, such a solution increases the ratio of anonymous calls of route maintenance and route re-adjustment. Furthermore, such solutions do not determine the reliability of wireless channels under a dynamic environment, which results in the inability to transmit sensors' data on a robust route. Accordingly, the most processing time is wasted in computing the optimal route and leads to high data delay. However, the proposed AI-EPP algorithm separates the IoT network into various regions using hop count and network data is transmitted by multi-tiers. Further, it minimizes the route breakages and the re-establishment of alternate routes in case of a high data generation rate. Moreover, it efficiently manages wireless links' and their available capacity for the delivery of sensitive data on time.

In Figures 7 and 8, the experimental analysis presents the improvement in terms of energy consumption of proposed AI-EPP by 28% and 30% than the existing solutions. This is due to selecting the most competent nodes in terms of resource as cluster heads with the least transmission distance to both centroid and BS. The proposed AI-EPP offers a graph-based technique based on dividing the nodes into different clusters, reducing the proportion of energy consumption on the node level. The public key certificate-based cryptography mechanism in the proposed AI-EPP significantly reduces the chances of intrusions for re-directing the data packets towards prohibited points and decreases the unnecessary energy consumption of nodes. The proposed solution also exploits the lightweight computing functions for providing data security and avoids the chances for a malicious node to generate high intrusion on the transmission channels. In Figures 9 and 10, the experimental analysis shows that the proposed AI-EPP reduces the ratio of malicious packets by 40% and 37% compared to existing solutions. This is due to the proposed AI-EPP algorithm incorporating the public key-based digital certificates for routing nodes, and accordingly, only the authorized nodes are eligible for data transmission. The computed trust value in the proposed AI-EPP is based on the nodes' local information rather than the global facts of the entire network field that significantly increases the strength for identifying the malicious nodes with nominal cost. Furthermore, AI-EPP offers centralized authority for digital certificates' issuance and manages data routing, minimizing malicious activities.

Figures 11 and 12 illustrate the analysis of the proposed AI-EPP algorithm with other solutions in terms of runtime overhead. The results have proven its significant improvement by 33% and 21%, respectively. It is due to providing the minimum routing cost solution in determining the optimal routes for medical data. In addition, a graph-based approach imposes the least overheads on exchanging the control messages among sensors and increases the routes' strength. Moreover, the BS acts as a central authority to provide the selected routes' authorization and avoid the extra messages among neighbors to negotiate. Unlike other solutions that enforce high control overhead for achieving data security, the proposed AI-EPP algorithm preserves privacy among medical sensors using the least computational-powered exclusive-OR function. Figures 13 and 14 demonstrate the performance analysis of the proposed AI-EPP algorithm than existing solutions for link disconnectivity under a varying number of nodes. It is seen that the AI-EPP algorithm improved by 13% and 17%, respectively. The cost function operates on multiple factors and each time its archives optimal data routing even in the presence of network threats. The symmetric digital certificates offer trustworthiness criteria for mutual authentication among nodes with the collaboration BS. Unlike other solutions that impose an unbalanced load on routing nodes, the proposed AI-EPP algorithm efficiently utilizes the link performance in terms of interference and strength of the transmission system. Figures 15 and 16 depict the performance analysis of the complexity for the AI-EPP algorithm against an existing solution. To analyze the complexity, we estimate the processing time while requesting the needed data from the application user and obtain the process data back to their ends. It is seen that the proposed solution reduces the processing time by 37% and 23% as compared to other solutions. This is due because it optimizes the communication services for time and constraint resources. Furthermore, flooding of control messages is reduced that significantly decreased the complexity time for data processing. Moreover, BS performed the role of establishing trust monitoring and authorization policies among the IoT network, which ultimately decreases the overheads on the nodes and offers timely service for application users.

Table 2. Simulation parameters.

Parameters	Values
Initial energy	2j
Deployment	Random
Jamming nodes	3–15
Traffic type	CBR
Transmission power	5 m
Medical sensors	50–250
Cloud servers	2
Simulation interval	2000 sec
Round	25 sec
Packet size	32 bits
Control bits	20 bits

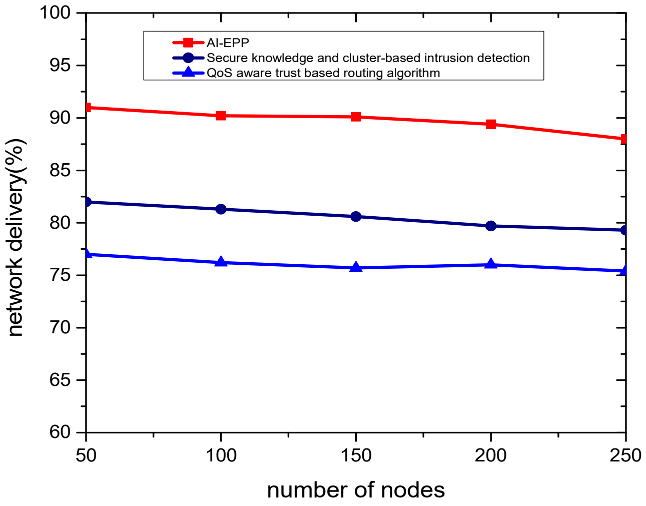

Figure 3. Network delivery comparison using simulations with a varying number of nodes.

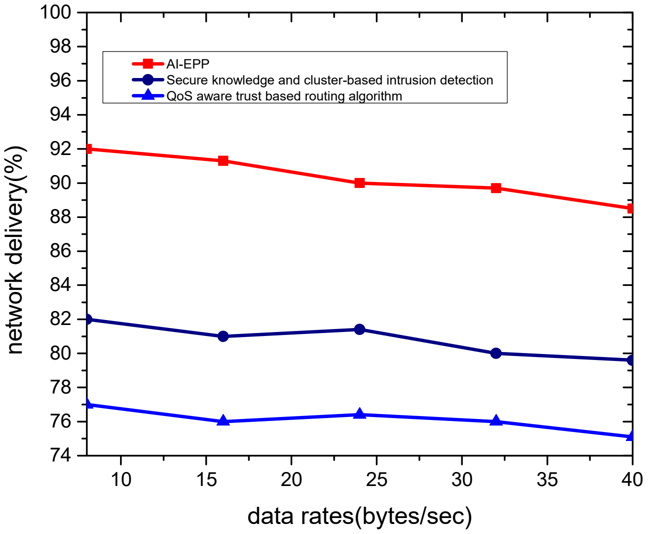

Figure 4. Network delivery comparison using simulations with varying data rates.

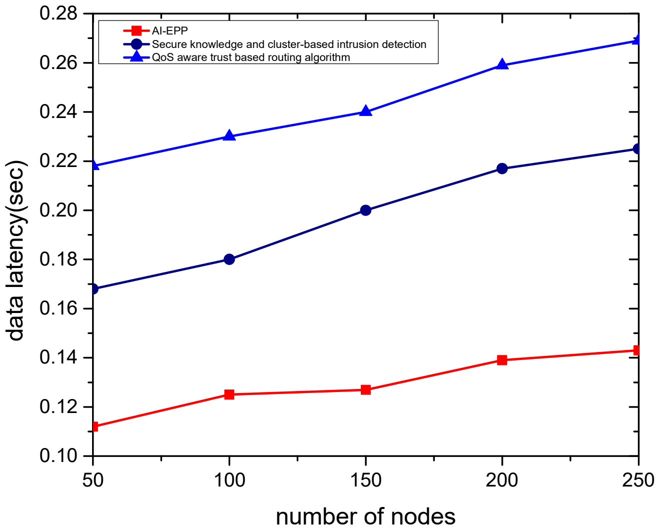

Figure 5. Data latency comparison using simulations with varying number of nodes.

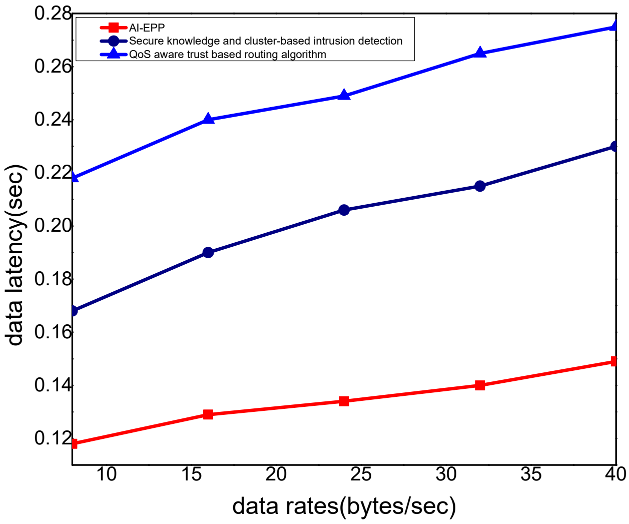

Figure 6. Data latency comparison using simulations with varying data rates.

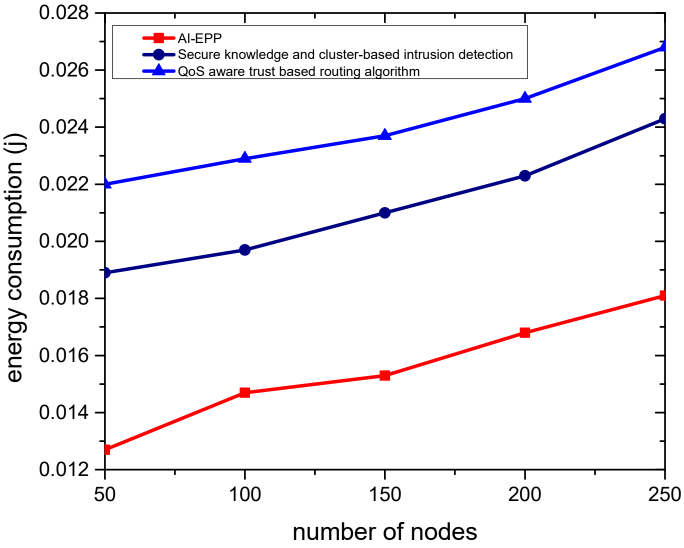

Figure 7. Energy consumption comparison using simulations with varying number of nodes.

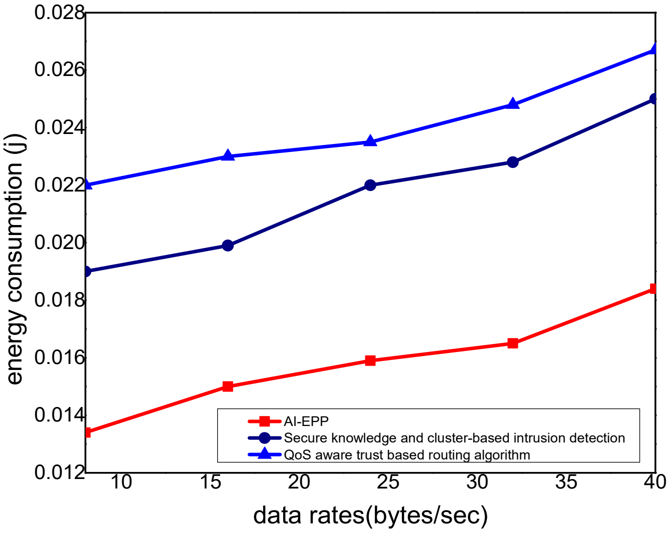

Figure 8. Energy consumption comparison using simulations with varying data rates.

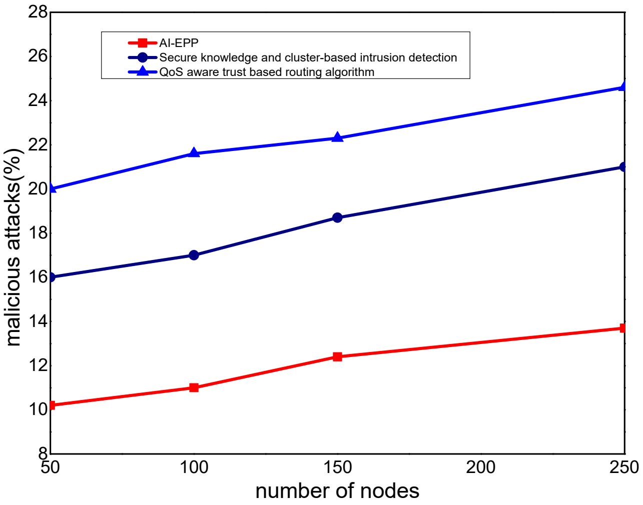

Figure 9. Malicious attacks comparison using simulations with varying number of nodes.

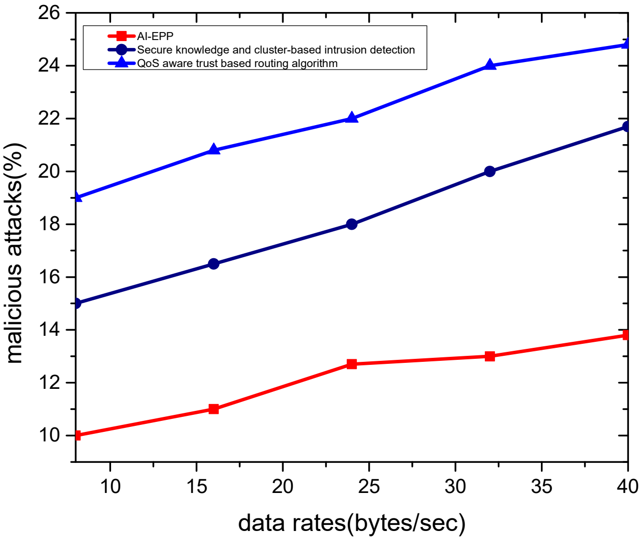

Figure 10. Malicious attacks comparison using simulations with varying data rates.

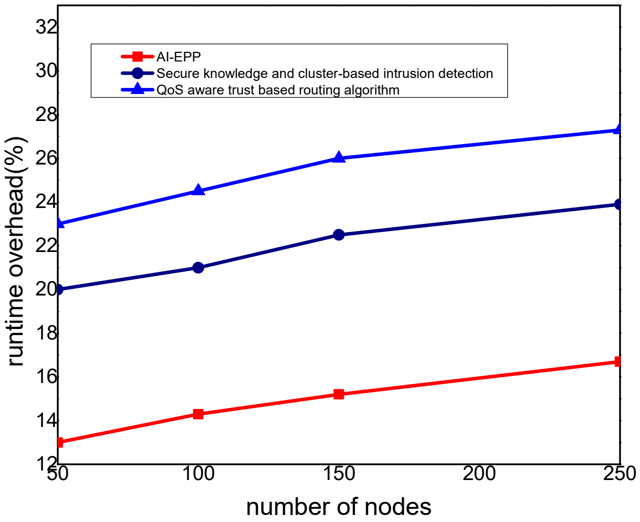

Figure 11. Runtime overhead comparison using simulations with varying number of nodes.

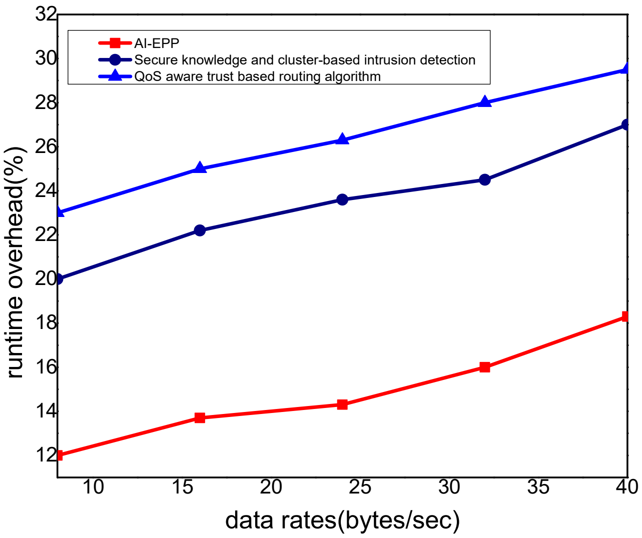

Figure 12. Runtime overhead comparison using simulations with varying data rates.

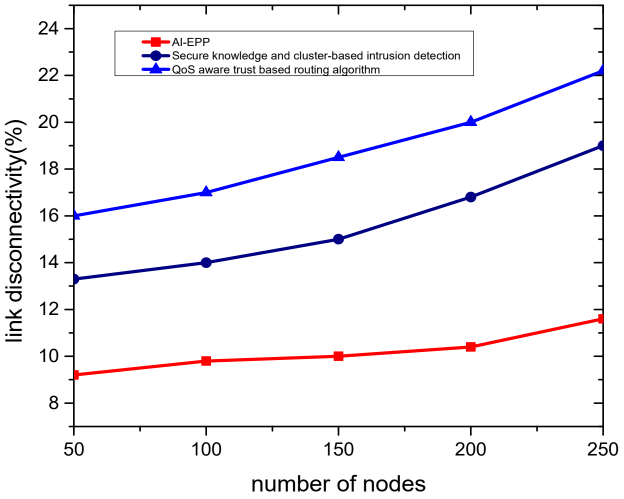

Figure 13. Link disconnectivity comparison using simulations with varying number of nodes.

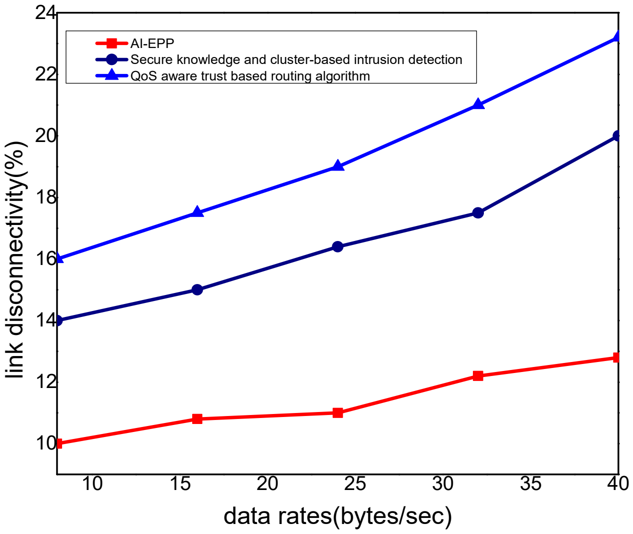

Figure 14. Link disconnectivity comparison using simulations with varying data rates.

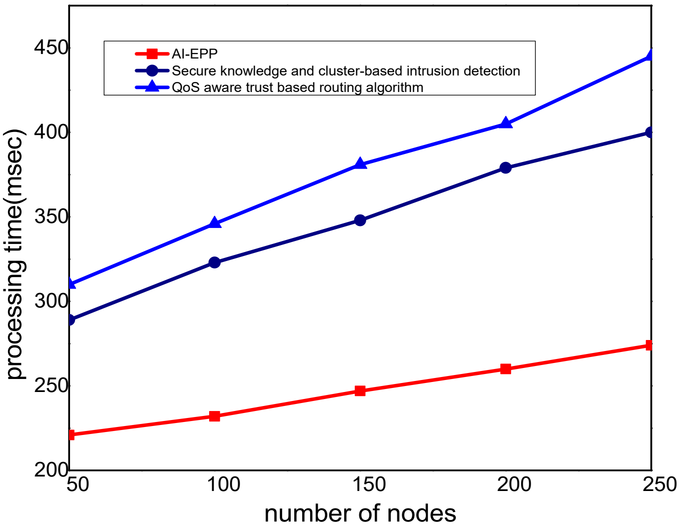

Figure 15. Processing time comparison using simulations with varying number of nodes.

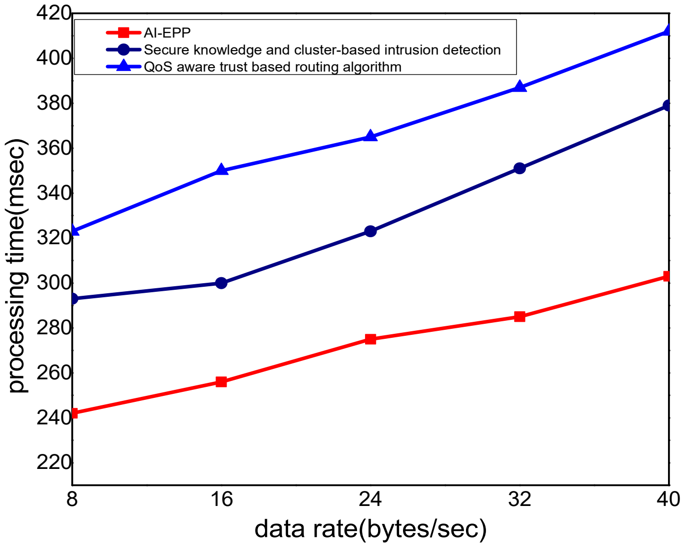

Figure 16. Processing time comparison using simulations with varying data rates.

5. Conclusions

In this work, an IoT solution is proposed by utilizing AI-enabled privacy-preserving with big data transferring using blockchain. The proposed work improves the management of data forwarding and offers a secure network infrastructure to maintain information privacy along authorize access against unusual events. It is seen that most of the existing work developed a solution for improving the public health system and facilitated the connected users in terms of optimal services. However, most of them are unreliable in terms of data controlling, especially when the load is increasing and communication channels are overburdened. Moreover, it is also observed that the existing solution offered security services to constraint devices but compromised the network performance for runtime overheads, energy consumption, and data latency. On the other hand, the proposed AI-EPP algorithm uses graph-based optimal modeling to produce trusted nodes for routing the data. It also performs registration, verification phases by using symmetric digital certificates and increasing the transmission credibility with a cloud platform. In addition, it provides integrity by incorporating blockchain technology in distributed development with minor computing overheads on network nodes. The results are tested and analyzed by simulations and the AI-EPP algorithm outperforms existing solutions with consistent and sustainable communication. In the future, we would like to exploit the machine learning approach to optimize the training process of the AI-EPP algorithm with real data sets. Moreover, we aim to collaborate with multiple cloud platforms for data accessibility and computational intelligence.

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

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All Data is available in the article.

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

References

1. Kumar, L.; Sharma, V.; Singh, A. Feasibility and modelling for convergence of optical-wireless network–A review. *AEU-Int. J. Electron. Commun.* **2017**, *80*, 144–156. [CrossRef]
2. Mohamed, E. The relation of artificial intelligence with internet of things: A survey. *J. Cybersecur. Inf. Manag.* **2020**, *1*, 24–30.
3. Emira, H.H.A. Authenticating IoT Devices issues based on Blockchain. *J. Cybersecur. Inf. Manag. (JCIM)* **2020**, *1*, 35–40.
4. Yildiz, H.U.; Bicakci, K.; Tavli, B.; Gultekin, H.; Incebacak, D. Maximizing Wireless Sensor Network lifetime by communication/computation energy optimization of non-repudiation security service: Node level versus network level strategies. *Ad Hoc Netw.* **2016**, *37*, 301–323. [CrossRef]
5. Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of things and big data analytics for smart and connected communities. *IEEE Access* **2016**, *4*, 766–773. [CrossRef]
6. Haseeb, K.; Bakar, K.A.; Abdullah, A.H.; Ahmed, A.; Darwish, T.; Ullah, F. A dynamic Energy-aware fault tolerant routing protocol for wireless sensor networks. *Comput. Electr. Eng.* **2016**, *56*, 557–575. [CrossRef]
7. Aktas, F.; Ceken, C.; Erdemli, Y.E. IoT-based healthcare framework for biomedical applications. *J. Med. Biol. Eng.* **2018**, *38*, 966–979. [CrossRef]
8. Sodhro, A.H.; Luo, Z.; Sangaiah, A.K.; Baik, S.W. Mobile edge computing based QoS optimization in medical healthcare applications. *Int. J. Inf. Manag.* **2019**, *45*, 308–318. [CrossRef]
9. Deebak, B.D.; Al-Turjman, F.; Aloqaily, M.; Alfandi, O. An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. *IEEE Access* **2019**, *7*, 135632–135649. [CrossRef]
10. Ali, A.; Khan, F.A. Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. *EURASIP J. Wirel. Commun. Netw.* **2013**, *2013*, 216. [CrossRef]

11. Han, T.; Zhang, L.; Pirbhulal, S.; Wu, W.; de Albuquerque, V.H.C. A novel cluster head selection technique for edge-computing based IoMT systems. *Comput. Netw.* **2019**, *158*, 114–122. [CrossRef]
12. Guo, X.; Lin, H.; Wu, Y.; Peng, M. A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems. *Future Gener. Comput. Syst.* **2020**, *113*, 407–417. [CrossRef]
13. Suresh, A.; Udendhran, R.; Balamurgan, M. Hybridized neural network and decision tree based classifier for prognostic decision making in breast cancers. *Soft Comput.* **2020**, *24*, 7947–7953. [CrossRef]
14. Aich, S.; Younga, K.; Hui, K.L.; Al-Absi, A.A.; Sain, M. A nonlinear decision tree based classification approach to predict the Parkinson's disease using different feature sets of voice data. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 11–14 February 2018; pp. 638–642.
15. Manikandan, R.; Patan, R.; Gandomi, A.H.; Sivanesan, P.; Kalyanaraman, H. Hash polynomial two factor decision tree using IoT for smart health care scheduling. *Expert Syst. Appl.* **2020**, *141*, 112924. [CrossRef]
16. Dadhich, P. Security of Healthcare Systems with Smart Health Records Using Cloud Technology. In *Machine Learning with Health Care Perspective*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 183–198.
17. Lu, Y.; Sinnott, R.O. Security and privacy solutions for smart healthcare systems. In *Innovation in Health Informatics*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 189–216.
18. Haseeb, K.; Islam, N.; Almogren, A.; Din, I.U. Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. *IEEE Access* **2019**, *7*, 185496–185505. [CrossRef]
19. Saba, T.; Haseeb, K.; Ud Din, I.; Almogren, A.; Altameem, A.; Fati, S.M. EGCIR: Energy-Aware Graph Clustering and Intelligent Routing Using Supervised System in Wireless Sensor Networks. *Energies* **2020**, *13*, 4072. [CrossRef]
20. Thakker, U.; Patel, R.; Tanwar, S.; Kumar, N.; Song, H. Blockchain for Diamond Industry: Opportunities and Challenges. *IEEE Internet Things J.* **2020**, *8*, 8747–8773. [CrossRef]
21. Cao, B.; Wang, X.; Zhang, W.; Song, H.; Lv, Z. A many-objective optimization model of industrial internet of things based on private blockchain. *IEEE Netw.* **2020**, *34*, 78–83. [CrossRef]
22. Pourvahab, M.; Ekbatanifard, G. An efficient forensics architecture in software-defined networking-IoT using blockchain technology. *IEEE Access* **2019**, *7*, 99573–99588. [CrossRef]
23. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
24. Miraz, M.H.; Ali, M.; Excell, P.S.; Picking, R. A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT). In Proceedings of the 2015 Internet Technologies and Applications (ITA), Wrexham, UK, 8–11 September 2015; pp. 219–224.
25. Haseeb, K.; Lee, S.; Jeon, G. EBDS: An energy-efficient big data-based secure framework using Internet of Things for green environment. *Environ. Technol. Innov.* **2020**, *20*, 101129. [CrossRef]
26. Mohamed, M. A comparative study on Internet of Things (IoT): Frameworks, Tools, Applications and Future directions. *J. Intell. Syst. Internet Things* **2020**, *1*, 13–39.
27. Mamun, M.S.I.; Kabir, A. Hierarchical design based intrusion detection system for wireless ad hoc network. *arXiv* **2012**, arXiv:1208.3772.
28. Shin, S.; Kwon, T.; Jo, G.-Y.; Park, Y.; Rhy, H. An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. *IEEE Trans. Ind. Inform.* **2010**, *6*, 744–757. [CrossRef]
29. Sharma, A.; Tayal, S.; Bansal, R.; Verma, S. Energy Efficiency Techniques in Heterogeneous Networks. *J. Cybersecur. Inf. Manag.* **2021**, *2*, 13–19.
30. Haseeb, K.; Islam, N.; Almogren, A.; Din, I.U.; Almajed, H.N.; Guizani, N. Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs. *IEEE Access* **2019**, *7*, 79980–79988. [CrossRef]
31. Wang, Y.; Wang, X.; Xie, B.; Wang, D.; Agrawal, D.P. Intrusion detection in homogeneous and heterogeneous wireless sensor networks. *IEEE Trans. Mob. Comput.* **2008**, *7*, 698–711. [CrossRef]
32. Alaparthy, V.T.; Morgera, S.D. A multi-level intrusion detection system for wireless sensor networks based on immune theory. *IEEE Access* **2018**, *6*, 47364–47373. [CrossRef]
33. Li, C.-T.; Wu, T.-Y.; Chen, C.-L.; Lee, C.-C.; Chen, C.-M. An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system. *Sensors* **2017**, *17*, 1482. [CrossRef]
34. Islam, A.; Shin, S.Y. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. *Comput. Electr. Eng.* **2020**, *84*, 106627. [CrossRef]
35. Liu, C.-H.; Chung, Y.-F. Secure user authentication scheme for wireless healthcare sensor networks. *Comput. Electr. Eng.* **2017**, *59*, 250–261. [CrossRef]
36. Liu, Y.; Zhang, Y.; Ling, J.; Liu, Z. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 1020–1026. [CrossRef]
37. Lin, K.; Pankaj, S.; Wang, D. Task offloading and resource allocation for edge-of-things computing on smart healthcare systems. *Comput. Electr. Eng.* **2018**, *72*, 348–360. [CrossRef]
38. Mehmood, A.; Khanan, A.; Umar, M.M.; Abdullah, S.; Ariffin, K.A.Z.; Song, H. Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks. *IEEE Access* **2017**, *6*, 5688–5694. [CrossRef]

39. Zhang, Z.; Zhu, H.; Luo, S.; Xin, Y.; Liu, X. Intrusion detection based on state context and hierarchical trust in wireless sensor networks. *IEEE Access* **2017**, *5*, 12088–12102. [CrossRef]
40. 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]
41. Luo, E.; Bhuiyan, M.Z.A.; Wang, G.; Rahman, M.A.; Wu, J.; Atiquzzaman, M. Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Commun. Mag.* **2018**, *56*, 163–168. [CrossRef]
42. Tao, H.; Bhuiyan, M.Z.A.; Abdalla, A.N.; Hassan, M.M.; Zain, J.M.; Hayajneh, T. Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet Things J.* **2018**, *6*, 410–420. [CrossRef]
43. Prim, R.C. Shortest connection networks and some generalizations. *Bell Syst. Tech. J.* **1957**, *36*, 1389–1401. [CrossRef]
44. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
45. Apriani, M.; Rousstia, D.; Rifai, F.A.; Harwahyu, R.; Sari, R.F. Implementation of Secure Work From Home System Based on Blockchain using NS3 Simulation. In Proceedings of the 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), Yogyakarta, Indonesia, 1–2 October 2020; pp. 54–59.
46. Foytik, P.; Shetty, S.; Gochhayat, S.P.; Herath, E.; Tosh, D.; Njilla, L. A blockchain simulator for evaluating consensus algorithms in diverse networking environments. In Proceedings of the 2020 Spring Simulation Conference (SpringSim), Fairfax, VA, USA, 18–21 May 2020; pp. 1–12.