electronics

MDPI

Article

Secured Big Data Analytics for Decision-Oriented Medical System Using Internet of Things

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

[1] Artificial Intelligence & Data Analytics Lab (AIDA), CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia; rkamjad@gmail.com (A.R.); drstanzila@gmail.com (T.S.)
[2] Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Khyber Pakhtunkhwa, Pakistan; khalid.haseeb@icp.edu.pk
[3] Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politenica de Valencia, 46022 València, Spain
[4] School of Computing and Digital Technologies, Staffordshire University, Stoke ST4 2DE, UK
[5] College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Alkharj 11942, Saudi Arabia; u.tariq@psau.edu.sa
* Correspondence: jlloret@dcom.upv.es

Abstract: The Internet of Medical Things (IoMT) has shown incredible development with the growth of medical systems using wireless information technologies. Medical devices are biosensors that can integrate with physical things to make smarter healthcare applications that are collaborated on the Internet. In recent decades, many applications have been designed to monitor the physical health of patients and support expert teams for appropriate treatment. The medical devices are attached to patients' bodies and connected with a cloud computing system for obtaining and analyzing healthcare data. However, such medical devices operate on battery powered sensors with limiting constraints in terms of memory, transmission, and processing resources. Many healthcare solutions are helping the community with the efficient monitoring of patients' conditions using cloud computing, however, mostly incur latency in data collection and storage. Therefore, this paper presents a model for the Secured Big Data analytics using Edge–Cloud architecture (SBD-EC), which aims to provide distributed and timely computation of a decision-oriented medical system. Moreover, the mobile edges cooperate with the cloud level to present a secure algorithm, achieving reliable availability of medical data with privacy and security against malicious actions. The performance of the proposed model is evaluated in simulations and the results obtained demonstrate significant improvement over other solutions.

Keywords: Internet of Medical Things; decision oriented medical systems; security; edge cloud; big data

Citation: 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. https://doi.org/10.3390/electronics10111273

Academic Editor: Jemal H. Abawajy

Received: 18 April 2021
Accepted: 24 May 2021
Published: 27 May 2021

1. Introduction

In recent years, the advent of the Internet of Things (IoT) has led to a paradigm shift in all areas of human-machine interaction, particularly healthcare and security [1–3]. IoMT is a subarea of the IoT, particularly related to healthcare systems and to solve medical-related issues distantly such as patient identity, diagnosis of diseases, and data storage in the cloud [4,5]. Its elements are comprised of wearable sensors, network devices, and smartphones that collect the vital signs of the patient. Afterwards, the medical data are forwarded to centralized database servers over the 5G network. The medical experts obtain the stored information and perform some analysis on it for appropriate decision making with regards to treatment [6,7]. However, the main issue in healthcare systems is the collaboration of the IoT environment in terms of energy constraint, storage range, accessible bandwidth, and rapid disturbance over the wireless medium [8,9]. Wireless Sensor Networks (WSNs) are the integral components of IoT technology and Body Sensor

Networks (BSNs) are the main underlying software for medical applications. A BSN is a network built in and around the human body by deploying sensors with restricted constraints. Such an enormous adoption is still ongoing, however, for early identification of diseases and diagnosis purposes [10,11]. Combining data analytics and the IoT makes it possible to analyze medical data with versatility and a high amount of contextual awareness. Now, mobile edge cloud computing with remote sensors is also an emerging area that has a significant contribution in smart medical systems for healthcare, security, and remote management. Moreover, in edge cloud computing [12–14], local data processing imposes the least computing power, which is a critical matter as the IoT-based nodes are conventionally low power in terms of energy and computational resources [15]. Moreover, as the processing unit becomes part of the network, the time for transmission between the edge devices and the processing units declines dramatically. At the edge or preprocessed at the edge, the data is then analyzed and offloaded to the remote processing unit. In all cases, the network's performance increases enormously in terms of latency. Furthermore, by isolating edge nodes from the central network, edge computing aims to provide multi-device interoperability. Therefore, these days researchers are focused on producing an IoT-based medical system to monitor the patients' health with an efficient storage paradigm. This work presents secure big data analytics with the collaboration of mobile edge–cloud architecture, which aims to decrease the data latency performance with the support of trusted communication among medical nodes.

The contributions of the proposed model are as follows:

i. It adopts a greedy search in proximity neighborhood graphs for optimizing with uniform rate transmissions and increases the energy efficiency of medical systems.
ii. The mobile edges have a direct or indirect association with the sink and cloud level to cope with big data analytics and offer interactive medical systems with nominal data latency.
iii. The mobile edges that are the bottleneck for forwarding the data to the cloud are immune to malicious actions and kept secure against network vulnerabilities. The proposed secured algorithm maintains the inaccessibility of medical transmission from network threats and offers certifiable data to end-users.
iv. The proposed model is verified with extensive experiments using simulations and it is proven to be a remarkable contribution compared to existing schemes.

The rest of the paper is organized as follows. Section 2 presents a discussion on related work. Section 3 develops the proposed model. Section 4 illuminates the simulation-based experiments with detailed discussion. Section 5 presents conclusions.

2. Related Work

Smart medical systems [16,17] have proven productive for data analytics and security measurement of sensitive data. IoT-based networks can change the routine work of the community and recently a lot of researchers have investigated the potential of participating in the concepts of the IoT with smart cities and big data analytics [18,19]. The IoT has recently established countless considerations because of its potential and collaborated with many complex systems. In [20], the authors suggested a framework for structural health monitoring (SHM) based on IoT technologies with intelligent and consistent observation. Furthermore, the strategy for data routing is presented with the collaboration of big data analytics. The proposed framework improved the performance in terms of scalability and low latency. In smart medical systems, the IoMT, which is a subset of IoT, performs several different applications such as patient remote monitoring, medication, treatment satisfaction, etc. However, the confidentiality of patient records in medical systems is crucial in an IoMT environment. Therefore, protecting confidential health information (PHI) is a significant aspect of healthcare data protection. Big data is also an integral part of healthcare systems that holds all records of patients, reports, treatments records and so forth that is highly confidential. Cloud and edge computing are the paradigms that make IoT-enabled communication possible with nominal communication cost [21,22].

There are countless types of data in addition to the vast volumes of data that are generated by a large variety of devices. In implementing the IoMT, data interoperability is the principal challenge for the sector. Edge computing has been used in various solutions for reducing latency in real-time situations. However, data privacy is a significant issue. The authors of [23] proposed a lightweight privacy-preserving medical diagnosis mechanism on the edge called LPME which redesigns the extreme gradient boosting (XGBoost) model using an edge–cloud model and exploits parameters of the encrypted model rather than local data to reduce the computation overheads. Moreover, the proposed work secured diagnosis on the edge with privacy for sensitive data and timely finding. In [24], the authors proposed a resource preservation net (RPN) framework using Petri net with the collaboration of cloud and edge computing. It is applicable to real-world scenarios and its key and optimized performance parameters are the patient length of stay, resource utilization rate, and average waiting time of patients. The proposed framework is tested under various simulations and highlights the main contribution in different aspects. A framework of the cloud healthcare system based on digital twin healthcare (CloudDTH) is presented in [25]. It is a generalized, and extensible framework for cloud computing for observing and finding health issues using medical devices. The proposed framework introduced and implemented the concept of digital twin healthcare (DTH). Moreover, it demonstrates the feasibility of some application-based scenarios with a case study for real-time management. In [26], the authors proposed a decentralized cloud environment that utilizes blockchain technology to cope with the security of medical data. It offers digital signature schemes for the handling of data. Also, the technology of blockchain ensures that data could be split in the form of blocks and timestamps can be produced for the observation data which is stored or updated. The proposed work improves the performance in terms of cost and time compared to existing schemes. In [27], the authors proposed an Access Control Policy Algorithm for increasing data accessibility among healthcare providers. It assisted in the simulation environment and implemented the Hyperledger-based electronic healthcare record sharing system based on blockchain technology. The performance results are also optimized using different performance metrics in blockchain networks, such as latency, throughput, and round-trip time. New safety mechanisms and algorithms for the security of the health care system have been created by [28]. Moreover, their research implemented adaptive streaming techniques for the 3GPP packet switched streaming service, but in remote health monitoring applications, they did not consider rate control and offline algorithms for medical video transmission. The authors of [29] suggested various remote resource management methodologies, including checking health facilities, power and battery timing of small wearable devices. It proposed a mobility-aware optimal resource allocation architecture, namely Mobi-Het, to cope with remote big data task execution and management with higher efficiency in a timely and reliable manner. The simulated experiments illustrated the efficacy of the proposed Mobi-Het architecture in mobile big data applications. The authors of [30] proposed architecture and its security protocol to permit the exchanging of data, network services, computing, and storage resources between the connected mHealth clouds. The routing algorithm is based on the shortest path first (SPF) strategy. Moreover, the proposed solution is highly scalable and maintains a balanced load on the cloud. The performance tests have proven it to be a secure system design and controlled transmission system.

It can be seen from the discussion of related work that the IoMT has shown rapid growth in the development of medical applications and facilitates patients and medical teams. It collects the patient data and is forwarded towards medical databases; thus, medical professionals can access it and deal with patients' diseases. Recently, many solutions have been proposed to cope with data routing in healthcare systems but it is observed that most of them are not optimal in terms of communication cost and reliable data delivery. Based on the analysis, most of the solutions only consider the greedy heuristics based on the distance parameter and overlook link failures and channel latency parameters. Also, it is observed that some solutions achieved stable routing performance

at the expense of energy consumption and network load. Moreover, patients' data, which is sensitive and can be used for unauthorized statements, must be protected from network threats and maintains its integrity. Thus, the security mechanism should also be adopted in healthcare systems with trustworthy data accessibility.

3. The Proposed IoMT-Enabled Model

This section presents the detail of SBD-EC model and consists of two main phases. Figure 1 depicts the components of the proposed model. Initially, we consider that the medical devices are connected in the form of graph $G(V, N)$. Each node $n_i \ \varepsilon \ N$ and vertex $v_i \ \ \varepsilon \ V$. The individual vertex v_i is associated with directly connected neighbors by a particular cost. All the medical nodes are controlled by a local coordinator that performs the functions of data aggregation. Also, the local coordinator has an indirect association with sink nodes using intermediate devices that are connected wirelessly with each other. These intermediate nodes aim to forward the medical data towards the sink node and are further connected with cloud services using mobile edges.

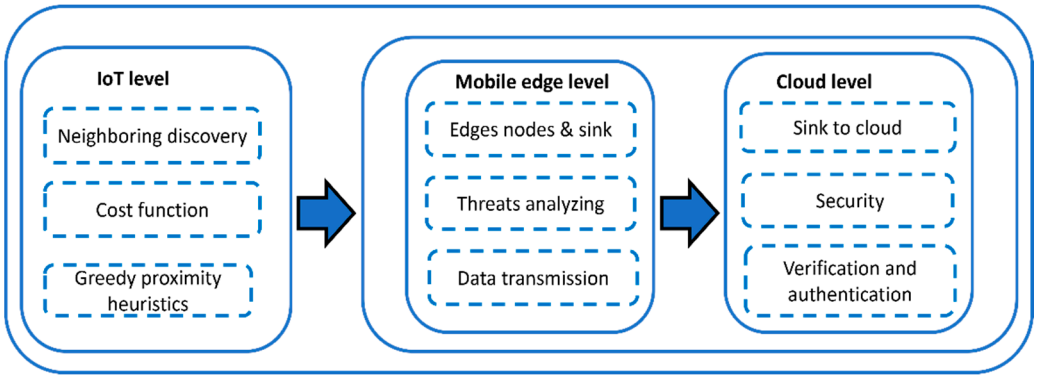

Figure 1. Components of the proposed medical model using IoT.

The SBD-EC model is comprised of three main layers. In the first layer, medical sensors are coordinated with the local coordinator. In the second layer, the local coordinator is linked indirectly with the sink node using various intermediate nodes. In the third layer, the mobile edges collaborate with cloud services, decreasing the latency in data storage and processing. Furthermore, as the edges are mobile, it takes the less time collecting the medical data from an upper layer. Moreover, it is seen that most of the existing work does not consider effective authentication methods on mobile edges, and ultimately malicious users could either relay the collected data on unauthorized routes or suspension the network services. Therefore, the proposed model also offers a security algorithm and provides secured communication from mobile edges to cloud services while minimizing the communication overhead and data latency. The SBD-EC model utilizes greedy traversing with the proximity neighboring method to explore reliable routes for forwarding medical data. The greedy heuristic follows the problem-solving strategy and offers the choice for the sub-optimal selection with minimum run-time and space complexity in each iteration. It simplifies the route formation process of the SBD-EC model with a nominal computational load on the constraint IoT nodes. It makes a locally optimal decisions and each iteration leads to a globally optimal solution. In the SBD-EC model, the cost function is computed using energy consumption (e), bi-directional distance (dis), and link latency (ln_t) parameters, which should be minimum and optimized. The cost function follows the principle of greedy routing such that medical data is transmitted towards the destination with bordering nodes and measurements of network status. Equation (1) formulates the cost function Cf for the greedy heuristic and operates on both intra-body and inter-body communication.

$$Cf \ = \ min(e \ + \ dis \ + ln_t) \tag{1}$$

The energy consumption of the medical sensors can be computed by the integration of transmitting (T_e) and receiving (R_e) factors as given in Equation (2).

$$e = T_e + R_e / G_e \tag{2}$$

where G_e denotes the global energy, which is comprised of maximum levels of nodes. It is declared at the time of network initialization. The minimum value of e indicates sufficient transmission power of a node for involvement in forwarding medical data. However, if the transmission power of a source node is not appropriate for direct data forwarding to the destination, then it adopts a multi-hop communication paradigm. Also, the distance factor is computed to adjust the transmission power in data forwarding and is determined using the Pythagorean theorem [31] as given in Equation (3).

$$dis = \sqrt{di^2 + dj^2} \tag{3}$$

where di denotes the distance of the source node to the neighbor and dj denotes the average distance of the source node to the coordinator and sink node. Moreover, the link latency is also added in the decision of cost function for improving delivery performance on time, as given in Equation (4).

$$ln_t = (R_\alpha - D_\alpha / T) \cdot \beta + P_d \tag{4}$$

where D_α denotes the transmitting time of hello packets towards the neighbors, R_α is receiving time of the hello packets, T is fixed time interval, β is available bandwidth for a wireless channel among connected nodes and P_d indicates the delay rate for the processing of data packet.

After the computing of the cost function, the SBD-EC model performs the greedy method to accomplish a reliable and optimal forwarding scheme, as discussed below.

i. The source node from the graph $G(V, N)$ computes the cost function for each neighbor connected with different vertexes V.
ii. It selects the vertex V with the minimum cost value. However, it stops on a stage if reaches a local minimum, which implies that the neighbors do not have the nearer vertex to the source node than the vertex itself.

Afterward, the SBD-EC model presents a secured edge–cloud algorithm for data collection and storage. The edge nodes are mobile and are connected to the sink node and cloud layer. The edge nodes collect the data from the sink node and are further forwarded towards the cloud level. The edge nodes are rotated at the rate R which can be computed as given in Equation (5).

$$R = d_n \pm d_{ini} / t \tag{5}$$

where d_n denotes the covered distance of the mobile edge node from sink node at a time t, and d_{ini} denotes its initial distance. Moreover, the SBD-EC model also secures edge cloud communication by using the Schmidt-Samoa cryptosystem [32]. In the SBD-EC model, the sink node, mobile edges, and cloud systems utilize pairs of public X and private Y keys for data encryption and decryption. The generated pair of keys ensures data security by using lightweight encryption and decryption mathematical functions. Firstly, the two large distinct prime numbers p and q are chosen, and security keys are generated as given in Equations (6) and (7).

$$X = p^2 \cdot q \tag{6}$$

$$Y = X^{-1} mod\ lcm(p-1, q-1) \tag{7}$$

where X and Y denote public and private keys. The data encryption C from the mobile edge towards a cloud system is computed using Equation (8).

$$C = D^X \cdot mod\ X + S_e(Y, D) \tag{8}$$

where D represents the medical data and S_e is a signature of the mobile edge node using the private key Y.

On the other hand, the encrypted data C is converted to its authentic form by the cloud servers using Equation (9).

$$D = c^{Y} \, mod \, p{\cdot}q + V_c(X, D) \tag{9}$$

where V_c is verification function performed by cloud system using the public key of mobile edge node X.

The flow chart of the SBD-EC model is described in Figure 2.

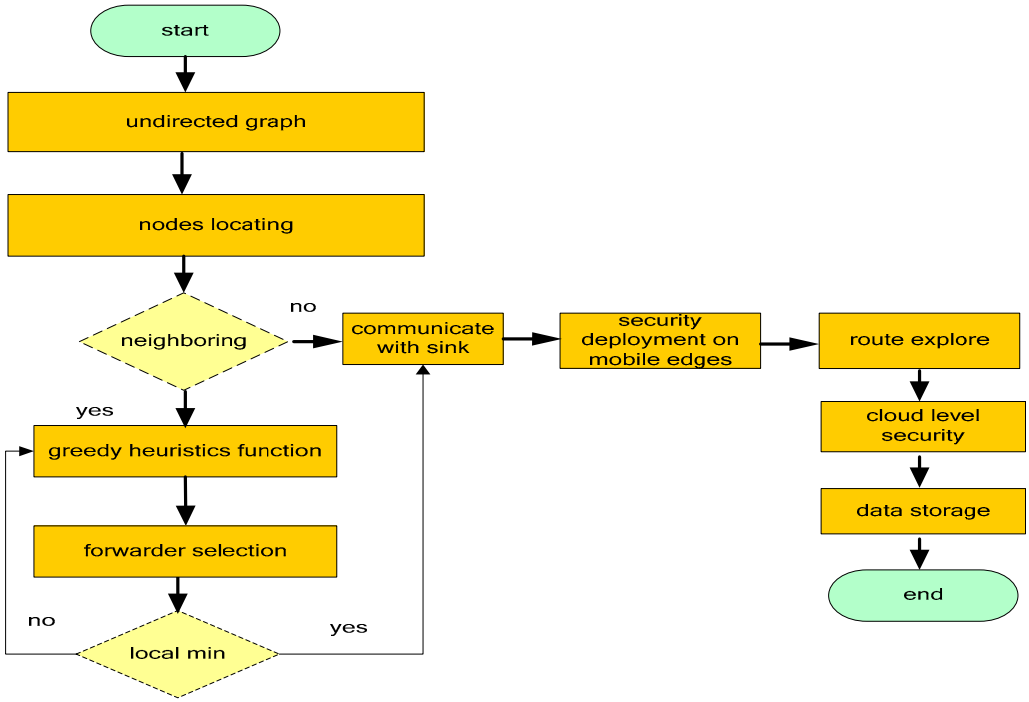

Figure 2. Working flow of the proposed model.

Security Analysis of SBD-EC Model

This section provides security analysis achieved by the SBD-EC model against network threats.

i. Confidentiality All the information that has to be kept confidential among sink node, mobile edges, and the cloud server is encrypted using a lightweight encryption function. Also, the encrypted data is concatenated with the unique identifier to the source node Id. The message m, security key K along with $S(Id)$ is passed through the encryption function. Since K is mathematically related to its private key, the intruder cannot recover the original message. Also, Id is digitally signed S by the data owner, which reflects its authentication on the receiving end.

ii. Mutual Authentication In the registration phase of the SBD-EC model, sink node, mobile edges, and cloud servers generate security keys and exchange the public keys with each other using the Schmidt-Samoa cryptosystem. The public keys are used for data encryption and their related mathematical private key is used for data decryption. The private keys perform the dual role of authentication along with data confidentiality. The combination of a pair of public-private keys along with a unique identity Id i.e., $(N, d)+ Id$ denotes the authentication packets for communicating node.

iii. Integrity The collected data is divided into n sized blocks with the combination of the padding method. Each block has a unique hash h_i and it is interconnected with hashing value of the previous block h_{i-1} shown as $h_i = h_{i-1}$ xor m. If an intruder changes any data block, then the receiver recomputes and compares with the received hash value. In case of mismatch, it assumes the incoming data is false. Moreover, the

arrangement of hashing values in the form of a sequence makes it not possible for intruders to damage the integrity of data.

4. Simulations

This section presents the simulation scenarios and the obtained results. The experiments were performed using 15 medical sensors and one coordinator node that is placed on the patient body. The performance tests are evaluated using two different scenarios (i) the number of iterations in terms of network throughput, data retrieval latency, normalized routing overhead, energy consumption, and packet drop ratio (ii) the speed of mobile edges in terms of packet disruption, retransmitted packets, data delivery ratio, and breaches attack. In the implementation phase, we considered a platform with medical sensors, mobile edges, sink nodes, and cloud servers. Initially, the energy level of all the medical sensors was 2 j. The data flow among healthcare devices was considered at a constant bit rate (CBR). A few high-powered nodes were randomly deployed in the vicinity of sink and cloud systems that acted as mobile edges. The transmission range of medical sensors was set to 2 m. We considered 5 to 10 nodes as malicious to evaluate the security performance in the presence of network threats. To simulate the proposed model with existing schemes, a well-known network simulator NS-3 was utilized, as considered in different work [33,34]. The performance evaluation was carried out using the simulation parameters as illustrated in Table 1.

Table 1. Simulation parameters.

Parameter	Value
Medical sensors	15
Malicious nodes	5–10
Transmission power	2 m
Time interval	2 s
Mobile edge nodes	10
No. of the sink node	1
Payload size	512 bytes
Initial energy	2 j
Observing field	15 m × 15 m
Simulation time	400 s

Figure 3 depicts the performance analysis of the SBD-EC model in terms of energy consumption against other schemes. Based on the simulation experiments, it can be seen that the SBD-EC model improves energy consumption by 18% and 32% compared to other models. This is due to utilizing greedy heuristics for the selection of the next hop for forwarding medical data. Furthermore, the stability period of medical sensors is increased due to the computation of cost function which decreases the additional overheads on it. Moreover, as the SBD-EC model employs a multi-criteria selection for the computing of cost function which is more adjustable in constraint-oriented applications as compared to other solutions. The proposed strategy not only confirms data routing via reliable nodes, but it also balances the energy consumption in negotiating through shorter routes. Unlike other solutions, the SBD-EC model decreases the calls for route maintenance and exchange of beacon messages based on network needs, and thereby results in the least energy consumption among selected forwarders.

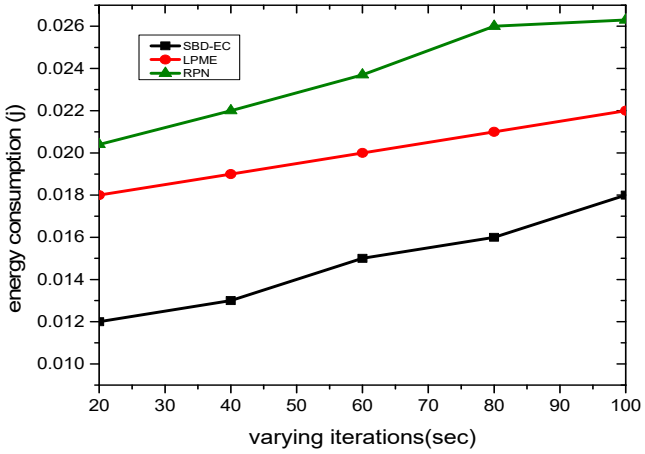

Figure 3. Energy consumption and iterations.

Figure 4 illustrates the performance of the SBD-EC model against existing solutions in terms of data retrieval rate. Based on the results, it can be observed that it significantly improves the data retrieval rate over the existing solutions by 37% and 46% respectively. This is due to the fact that the SBD-EC model avoids forwarding the data on interrupted routes and utilizes the constraints of medical sensors very efficiently. Also, the SBD-EC model utilizes a smaller number of hops in transmitting the medical data by evaluating the neighbors' information. With the consideration of more reliable paths using greedy heuristics, the SBD-EC model decreases the chances for route re-construction and network faults, which improves the data retrieval rate from storage servers. Moreover, by making use of security algorithms among mobile edge and cloud storage, the SBD-EC model avoids the possibility of malicious actions altering the route directions while forwarding the data. Furthermore, the proposed model is constantly monitoring the link latency and in case of network congestion, it removes such a node from routing decisions and maintains the timely delivery of sensitive patient data.

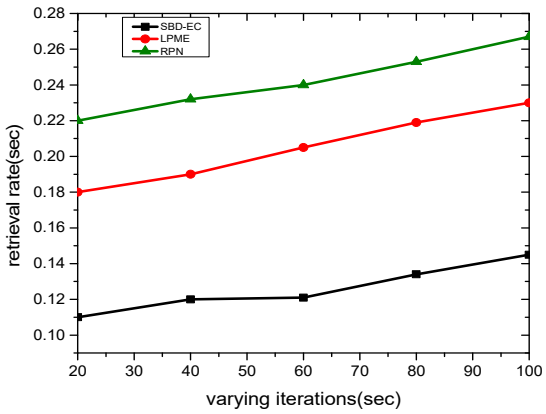

Figure 4. Data retrieval rate and iterations.

Figure 5 illustrates the performance analysis of the proposed model in terms of packet drop ratio as compared to existing models in varying iterations. It can be seen from the experimental results that the SBD-EC model decreases the packet drop ratio by 26%, and 59% compared to other solutions. This is due to the incorporation of energy and link latency factors, which chooses data forwarders more reliably with the updated values of the network communication system. Moreover, it selects the wireless channels for forwarding medical data with the least congestion and avoids channels with interference, which results in minimizing the packet drop ratio. Using weighted and minimized cost, only more optimal nodes can participate in the route discovery process, accordingly, the SBD-EC model decreases the probability of routing faults and high congestion levels.

Such constraints improved the packet drop ratio over unreliable communication media. Furthermore, it utilizes mobile edges for the collection of medical data intelligently from the sink node and securely transmits it to the cloud layer.

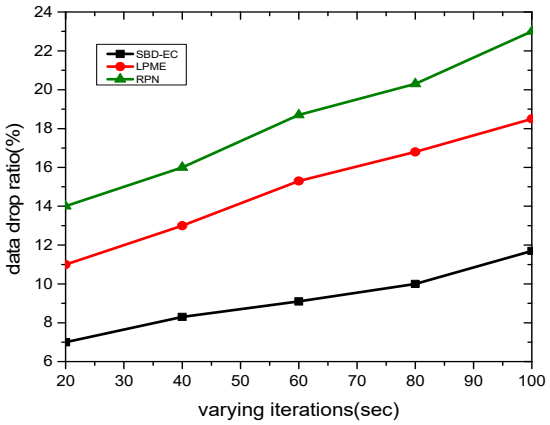

Figure 5. Data drop ratio and iterations.

Figure 6 depicts the experimental results of the SBD-EC model for network throughput against existing work. It is defined as aggregate data to the receiving side and reflects the efficiency of any routing solution. It is revealed that the SBD-EC model increases the network throughput by 17% and 21% compared to other models. This is because of the proposed communication strategy of the SBD-EC model, which is split into multiple layers and each layer operates independently with the least communication overhead. Also, the multi-hop paradigm is utilized by the proposed model when needed and makes use of the cost function in the selection criteria of the data forwarder. Moreover, due to the incorporation of the link latency in the cost function, the SBD-EC model judges the transmission flow on selected time t, and offers an appropriate contribution for the selection of next-hop in medical data. Such a method significantly increases the acceptance rate of medical data over unreliable communication routes with efficient energy management

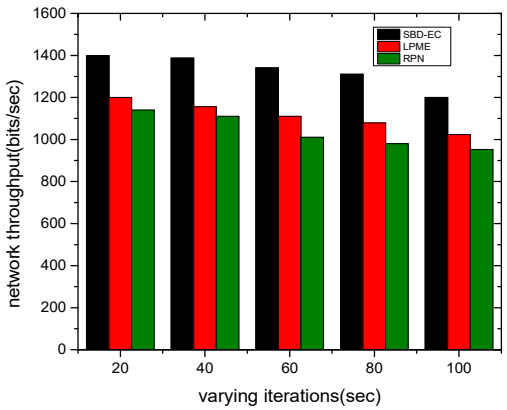

Figure 6. Network throughput and iterations.

Figure 7 illustrates the performance of the SBD-EC model in the comparison of normalized routing overhead with varying iterations. Based on the results, it can be seen that it reduces the routing overhead by 41 % and 47% over the existing solutions. It is due to the fact that most of the network operations such as aggregation, fusion, etc., are performed on high-powered edge nodes. Also, most of the management of security functions is executed on the sink node that has unlimited resources and ensures network privacy against malicious threats. Furthermore, it operates a multi-criteria cost function, which minimizes the number of attempts for data retransmission and, significantly, produces a low routing overhead. Moreover, it can be seen that unlike most of the schemes that are vulnerable to

high network overheads due to the exchange of several control messages regularly, the SBD-EC model decreases such practice and only transmits the node and network-related information based on certain criteria.

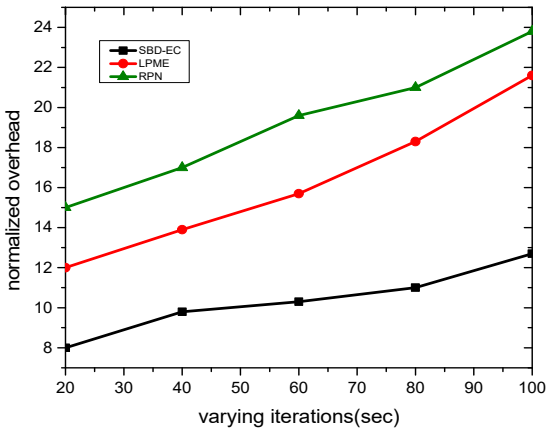

Figure 7. Normalized overhead and iterations.

Figure 8 illustrates the performance analysis of the SBD-EC model for second scenario in terms of packet disturbance, in comparison with other schemes. Based on the results, it is proven that the SBD-EC model improves the packet disturbance ratio by 37% and 45%. This is due to the use of heuristic cost function based on three parameters i.e., energy consumption, bi-directional distance, and link latency parameters for data routing. Such a strategy maintains the packet reception ratio among nodes and increases the efficacy for network performance. Moreover, it maintains the routes' consistency by considering the limited constraints of nodes with nominal communication load.

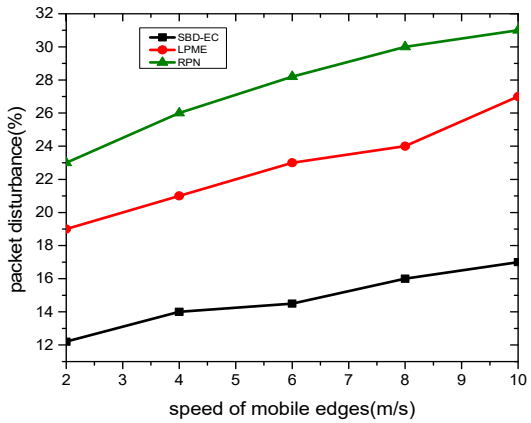

Figure 8. Packet disturbance and mobility.

Figure 9 illustrates the performance of the SBD-EC model against other solutions for second scenario. It can be seen from the experimental results that the SBD-EC model decreases the ratio of retransmitted packets by 37% and 45% compared to other models. This is due to the fact that the SBD-EC model decreases the probability of choosing non-optimal routes for forwarding healthcare data even in the case of mobility of medical edges. The incorporation of latency values increases the ratio of routes that can decrease the delivery ratio, thus the SBD-EC model is continuously searching for another route until it finds the optimal performance. Moreover, a properly secured and mutual authentication-based solution is offered by the SBD-EC model, which strengthens the communicating nodes in terms of packet delivery performance with the least transmission distance.

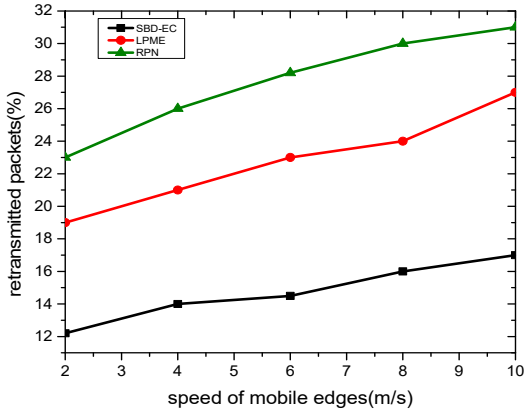

Figure 9. Retransmitted packets and mobility.

Figure 10 depicts the performance of the SBD-EC model for second scenario in the comparison with other solutions. Based on the experimental results, it is revealed that it increases the packet delivery ratio by 13%, and 17%. This is due to the fact that the SBD-EC model minimizes the number of hops and data latency in forwarding the nodes' data. Also, the weighted cost values give uniform contributions from each parameter and optimize the performance. In the SBD-EC model, the mobile medical edge performs a key role in data collecting and forwarding toward cloud services. Moreover, due to the mobility factor, the SBD-EC model decreases the data retrieval rate from nodes and offers a significant improvement in message delivery. Furthermore, with proper management of crowding control on the selected route, the SBD-EC model maintains the well-timed distribution of health data to medical servers.

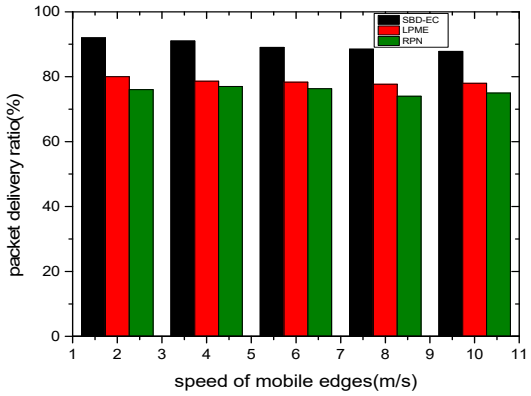

Figure 10. Delivery ratio and mobility.

Figure 11 illustrates the performance analysis of the SBD-EC model compared with other solutions in the case of breach attack. It can be seen from the experimental results that the SBD-EC model decreases the malicious attacks by 41%, and 49% and increases the trustworthiness among nodes. The generation of security keys by high computing nodes guarantees secure transmission in real-time scenarios even in the existence of intruders. Moreover, mathematical and related keys are utilized by directly connected nodes for data confidentiality and mutual authentication. Furthermore, the sequence of unique hashes gives little time to intruders for destruction and compromising the sensors' data. The SBD-EC model sets up the routing paths with data security along with reliable delivery, thus increases the trustworthiness for medical data without ignoring the resource constraints. Communication routes are such that energy consumption is balanced.

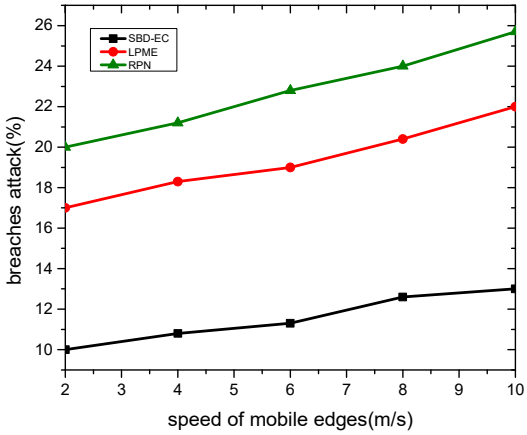

Figure 11. Breaches attack and mobility.

5. Conclusions

In recent decades, healthcare technologies such as biosensors, communication devices, and medical apps have been integrated with cloud computing to enable effective communication systems. However, most of the solutions have simply addressed the forwarding scheme to handle the healthcare data without considering constraint-oriented networks. Although some solutions cope with data security, they impose additional overheads in terms of processing and computation. In this paper, a model for the IoMT with Big Data Analytics using Edge–Cloud architecture is introduced which aims to increase the trust level of connected medical sensors. The computed cost function using greedy heuristics decreases the data retrieval rate based on mobile edges and improves the management of big data analytics. Moreover, the high-cost security computations are implemented on the sink and mobile edges that lower the overhead on the IoT network. Furthermore, it provides data privacy and authentication before arranging the medical data on cloud systems. The SBD-EC model was analyzed, and experimental tests revealed its significant performance in dynamic scenarios. In the future, we aim to provide security against some other potential network vulnerabilities. The scalability factor also needs to improve for mobile users connected with multiple clouds.

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

Funding: This paper has no funding.

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

References

1. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294.
2. Sadoughi, F.; Behmanesh, A.; Sayfouri, N. Internet of things in medicine: A systematic mapping study. *J. Biomed. Inform.* **2020**, *103*, 103383. [CrossRef]
3. Saeed, M.E.S.; Liu, Q.-Y.; Tian, G.; Gao, B.; Li, F. AKAIoTs: Authenticated key agreement for Internet of Things. *Wirel. Netw.* **2019**, *25*, 3081–3101. [CrossRef]
4. Dimitrov, D.V. Medical internet of things and big data in healthcare. *Healthc. Inform. Res.* **2016**, *22*, 156. [CrossRef] [PubMed]
5. Li, W.; Chai, Y.; Khan, F.; Jan, S.R.U.; Verma, S.; Menon, V.G.; Kavita; Li, X. A Comprehensive Survey on Machine Learning-Based Big Data Analytics for IoT-Enabled Smart Healthcare System. *Mob. Netw. Appl.* **2021**, *26*, 234–252. [CrossRef]
6. Zeadally, S.; Siddiqui, F.; Baig, Z.; Ibrahim, A. Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. *PSU Res. Rev.* **2019**, *4*, 149–168. [CrossRef]
7. Yuan, Y.; Cheah, T. A study of internet of things enabled healthcare acceptance in Malaysia. *J. Crit. Rev.* **2020**, *7*, 25–32.
8. Saba, T.; Haseeb, K.; Ahmed, I.; Rehman, A. Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *J. Infect. Public Health* **2020**, *13*, 1567–1575. [CrossRef] [PubMed]

9. Lloret, J.; Parra, L.; Taha, M.; Tomás, J. An architecture and protocol for smart continuous eHealth monitoring using 5G. *Comput. Netw.* **2017**, *129*, 340–351. [CrossRef]
10. Kalaiselvi, K.; Suresh, G.; Ravi, V. Genetic algorithm based sensor node classifications in wireless body area networks (WBAN). *Clust. Comput.* **2019**, *22*, 12849–12855. [CrossRef]
11. Salayma, M.; Al-Dubai, A.; Romdhani, I.; Nasser, Y. Wireless body area network (WBAN) a survey on reliability, fault tolerance, and technologies coexistence. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 1–38. [CrossRef]
12. Pan, J.; McElhannon, J. Future edge cloud and edge computing for internet of things applications. *IEEE Internet Things J.* **2017**, *5*, 439–449. [CrossRef]
13. Wang, T.; Zhao, D.; Cai, S.; Jia, W.; Liu, A. Bidirectional prediction-based underwater data collection protocol for end-edge-cloud orchestrated system. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4791–4799. [CrossRef]
14. Haseeb, K.; Din, I.U.; Almogren, A.; Ahmed, I.; Guizani, M. Intelligent and Secure Edge-enabled Computing Model for Sustainable Cities using Green Internet of Things. *Sustain. Cities Soc.* **2021**, *68*, 102779. [CrossRef]
15. Lopes, I.M.; Silva, B.M.; Rodrigues, J.J.; Lloret, J.; Proença, M.L. A mobile health monitoring solution for weight control. In Proceedings of the 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Xi'an, China, 23–25 October 2019; pp. 1–5.
16. Aktas, F.; Ceken, C.; Erdemli, Y.E. IoT-based healthcare framework for biomedical applications. *J. Med. Biol. Eng.* **2018**, *38*, 966–979. [CrossRef]
17. 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]
18. Nazir, S.; Khan, S.; Khan, H.U.; Ali, S.; García-Magariño, I.; Atan, R.B.; Nawaz, M. A comprehensive analysis of healthcare big data management, analytics and scientific programming. *IEEE Access* **2020**, *8*, 95714–95733. [CrossRef]
19. Hasan, W.K.; Ran, Y.; Agbinya, J.; Tian, G. A survey of energy efficient IoT network in cloud environment. In Proceedings of the 2019 Cybersecurity and Cyberforensics Conference (CCC), Melbourne, Australia, 7–8 May 2019; pp. 13–21.
20. Tokognon, C.A.; Gao, B.; Tian, G.Y.; Yan, Y. Structural health monitoring framework based on Internet of Things: A survey. *IEEE Internet Things J.* **2017**, *4*, 619–635. [CrossRef]
21. Muhammad, G.; Alhamid, M.F.; Alsulaiman, M.; Gupta, B. Edge computing with cloud for voice disorder assessment and treatment. *IEEE Commun. Mag.* **2018**, *56*, 60–65. [CrossRef]
22. Haseeb, K.; Almogren, A.; Ud Din, I.; Islam, N.; Altameem, A. Sasc: Secure and authentication-based sensor cloud architecture for intelligent internet of things. *Sensors* **2020**, *20*, 2468. [CrossRef] [PubMed]
23. Ma, Z.; Ma, J.; Miao, Y.; Liu, X.; Choo, K.-K.R.; Yang, R.; Wang, X. Lightweight privacy-preserving medical diagnosis in edge computing. *IEEE Trans. Serv. Comput.* **2020**. [CrossRef]
24. Oueida, S.; Kotb, Y.; Aloqaily, M.; Jararweh, Y.; Baker, T. An edge computing based smart healthcare framework for resource management. *Sensors* **2018**, *18*, 4307. [CrossRef]
25. Liu, Y.; Zhang, L.; Yang, Y.; Zhou, L.; Ren, L.; Wang, F.; Liu, R.; Pang, Z.; Deen, M.J. A novel cloud-based framework for the elderly healthcare services using digital twin. *IEEE Access* **2019**, *7*, 49088–49101. [CrossRef]
26. Nagasubramanian, G.; Sakthivel, R.K.; Patan, R.; Gandomi, A.H.; Sankayya, M.; Balusamy, B. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Comput. Appl.* **2020**, *32*, 639–647. [CrossRef]
27. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
28. Frustaci, M.; Pace, P.; Aloi, G.; Fortino, G. Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet Things J.* **2017**, *5*, 2483–2495. [CrossRef]
29. Enayet, A.; Razzaque, M.A.; Hassan, M.M.; Alamri, A.; Fortino, G. A mobility-aware optimal resource allocation architecture for big data task execution on mobile cloud in smart cities. *IEEE Commun. Mag.* **2018**, *56*, 110–117. [CrossRef]
30. Lloret, J.; Sendra, S.; Jimenez, J.M.; Parra, L. Providing security and fault tolerance in P2P connections between clouds for mHealth services. *Peer-to-Peer Netw. Appl.* **2016**, *9*, 876–893. [CrossRef]
31. Maor, E. *The Pythagorean Theorem: A 4000-Year History*; Princeton University Press: Princeton, NJ, USA, 2019.
32. Schmidt-Samoa, K. A new rabin-type trapdoor permutation equivalent to factoring. *Electron. Notes Theor. Comput. Sci.* **2006**, *157*, 79–94. [CrossRef]
33. Ismail, L.; Materwala, H.; Zeadally, S. Lightweight blockchain for healthcare. *IEEE Access* **2019**, *7*, 149935–149951. [CrossRef]
34. 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]