electronics

MDPI

Article

A Machine Learning SDN-Enabled Big Data Model for IoMT Systems

Khalid Haseeb [1], Irshad Ahmad [1], Israr Iqbal Awan [1], Jaime Lloret [2,3] and Ignacio Bosch [4,*]

[1] Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan; khalid.haseeb@icp.edu.pk (K.H.); irshad@icp.edu.pk (I.A.); israr.iqbal@icp.edu.pk (I.I.A.)
[2] Instituto de Investigacion Para la Gestion Integrada de Zonas Costeras, Universitat Politenica de Valencia, Campus de Gandia, C/Paranimf, 46370 Valencia, Spain; jlloret@dcom.upv.es
[3] School of Computing and Digital Technologies, Staffordshire University, Staffordshire ST4 2DE, UK
[4] Instituto de Telecomunicaciones y Aplicaciones Multimedia (iTEAM), Universitat Politènica de València, Camino Vera sn, 46022 Valencia, Spain
* Correspondence: igbosroi@dcom.upv.es

Abstract: In recent times, health applications have been gaining rapid popularity in smart cities using the Internet of Medical Things (IoMT). Many real-time solutions are giving benefits to both patients and professionals for remote data accessibility and suitable actions. However, timely medical decisions and efficient management of big data using IoT-based resources are the burning research challenges. Additionally, the distributed nature of data processing in many proposed solutions explicitly increases the threats of information leakages and damages the network integrity. Such solutions impose overhead on medical sensors and decrease the stability of the real-time transmission systems. Therefore, this paper presents a machine-learning model with SDN-enabled security to predict the consumption of network resources and improve the delivery of sensors data. Additionally, it offers centralized-based software define network (SDN) architecture to overcome the network threats among deployed sensors with nominal management cost. Firstly, it offers an unsupervised machine learning technique and decreases the communication overheads for IoT networks. Secondly, it predicts the link status using dynamic metrics and refines its strategies using SDN architecture. In the end, a security algorithm is utilized by the SDN controller that efficiently manages the consumption of the IoT nodes and protects it from unidentified occurrences. The proposed model is verified using simulations and improves system performance in terms of network throughput by 13%, data drop ratio by 39%, data delay by 11%, and faulty packets by 46% compared to HUNA and CMMA schemes.

Keywords: software-defined network; machine learning; internet of things; routing algorithm; network resources

check for updates

Citation: Haseeb, K.; Ahmad, I.; Awan, I.I.; Lloret, J.; Bosch, I. A Machine Learning SDN-Enabled Big Data Model for IoMT Systems. *Electronics* **2021**, *10*, 2228. https://doi.org/10.3390/electronics10182228

Academic Editor: Christos J. Bouras

Received: 4 August 2021
Accepted: 8 September 2021
Published: 11 September 2021

1. Introduction

Internet of Things (IoT) is a revolutionary paradigm that is equipped with sensors and physical objects to combine the real and digital worlds [1–3]. It is integrated with different mobile devices and offers smart solutions for the support of societies. Smart applications reshape the modern system with the delivery and reliability of academic and industrial data [4–6]. These systems are developed and integrated with various components of wireless communications, portable devices, and cloud computing [7,8]. The Internet of Medical Things (IoMT) represents wearable sensors that cooperate with other medical devices and clinical systems to support health activities. They provide remote access to a patient's condition such as management of chronic illness management, blood pressure, heartbeat, etc. [9,10]. However, modern health applications substantially increase the volume of medical data that needs to be managed efficiently, therefore demanding the incorporation of big data analytics for examining the data [11,12]. It is also observed from various research studies that although IoMT offers vast services to patients and the medical team, they have significant security and authentication risks in terms of privacy concerns, especially when health organizations cope with critical medical data [13–15].

Recently, machine learning techniques have been gaining popularity and they employ the analysis of statistics to learn from environmental data. This makes the network applications more intelligent and avoids operating on a predefined set of static rules [16–18]. The algorithm of machine learning simplifies the decision-making process and increases the performance for response time with optimized management of network resources along with security attacks [19,20]. SDN architecture is utilized by many approaches and decouples the control plane from the data plane to provide centralized control for efficient network management [21–24]. Additionally, due to the low-cost management of IoT devices, recently, many solutions have been suggested for integrating SDN in the health industry. However, it is a demanding issue to lower the communication overheads and automate security policies using SDN in various fields [25,26]. Therefore, this research presents a machine learning SDN-enabled big data model for IoMT systems that supervise the efficient management of network resources and improves the delivery of health data. Moreover, it reduces the management cost for the network operation and reduces the overhead of the control plane over the deployed sensors using SDN architecture. Moreover, the SDN-enabled security mechanism efficiently utilizes medical things for protecting critical data against security attacks. The contributions of the proposed model are as follows.

i. It utilizes the unsupervised machine learning technique to classify medical things into various collections. Unlike other traditional learning techniques, it does not require model assumptions.

ii. It develops a routing algorithm by predicting the link states based on updated network information and exploits the method of passive monitoring on the SDN controller. Such an algorithm refines the forwarding tables and lessens the routing cost and excessive network resources.

iii. Moreover, to avoid unpredictability in terms of anonymous attacks, the proposed model incorporates an intrusion detection algorithm and deploys the security using SDN architecture. It efficiently manages the network consumption in terms of power and decreases the operational overhead for critical structures.

iv. The proposed model is tested and verified in terms of dynamic network metrics as compared to existing work.

The research paper is organized in the following subsections. Section 2 provides the literature review of related studies. Section 3 illustrates the depiction of the proposed model. Section 4 discusses the performance experiments and their results. In the end, Section 5 provides the conclusion.

2. Related Work

In recent decades, health systems have been rapidly developed to monitor patients that cannot come to the hospital for daily routine checkups. Using technologies of the IoMT system, most of the smart applications facilitate medical experts and offer a quick response in emergency cases [27–29]. However, it is seen that IoMT devices are tightly constrained in terms of resources and limit the performance of the health system. Nowadays, healthcare systems are integrating with SDN architecture to lower resources usage and support a realistic environment. However, security is one of the main problems for real-time systems, especially to open space communication networks [30,31]. In the literature, different solutions have been proposed to improve the stability of data routing with nominal disruption using IoT networks [32–34]. However, most of them incur additional overhead on medical devices and imposing new security issues. Furthermore, due to the generation of massive data, mostly smart applications are not able to cope with efficient management of resources and lay down the communication performance. The authors in [35] proposed an efficient routing protocol based on machine learning techniques for an opportunistic network. To predict the successful deliveries, a neural network and decision tree were used.

The proposed machine learning-based framework is simulated and the results showed better performance in terms of data delivery ratio, overhead, and packet drop rates as compared to other networks. A Hierarchical Unsupervised Network Alignment (HUNA) is proposed in [36] to identify similar IoT devices. To achieve entity alignment under unsupervised conditions, the proposed scheme leverages the adversarial properties of the adversarial network. The proposed model is improved by developing a group structure aggregation optimization module that is responsible for the aggregation of nodes with similar attributes. The experimental results showed that the proposed scheme improves the parameter sensitivity and accuracy of the node alignment. The Machine Learning-based routing protocol proposed in [37] to automate routing decisions in Opportunist IoT network. The proposed method uses ML-based Gaussian Mixture Models that is a soft clustering method. The proposed protocol uses features of both context-aware and context-free routing protocols. The simulations results showed that the proposed routing protocol is outperformed in each performance parameter. The secure SDN IoT network architecture Black SDN is proposed in [38] to secure communication in IoT networks. The metadata and payload are secured via encryption. As a trustworthy third party, it employs the SDN centralized controller for secure routing and optimal management of network performance. The proposed architecture is successful in mitigating a range of attacks that includes traffic analysis and interference attacks. In [39], the authors proposed hybrid deep learning-driven SDN-enabled architecture to detect complex IoMT malware efficiently and quickly. In addition, the proposed approach utilizes the resource-constrained IoMT devices efficiently. The proposed hybrid model includes CNN (Convolution Neural Network) and LSTM (Long Short-Term Memory) models to detect advanced malware attacks. The proposed approach performs better in terms of the detection and prevention of advanced IoMT malware with low computational overhead. Authors in [40] proposed a clustering model for medical applications (CMMA), which aims for the selection of cluster head selection and provides real communication using IoMT technologies. Based on the various experiments, it is proven that the proposed solution increases the performance of the medical system as compared to the existing solutions. It not only balances the energy resources but also cluster heads are uniformly distributed and the network lifetime is increased. The authors in [41] proposed an SDN-enabled architecture leveraging hybrid deep learning detection algorithm, which aims at the detection of cyber threats efficiently and determines network attacks while considering the constrained resources of IoT networks. It reduces the additional load on the constrained resources and increases the scalability of network performance. The experimental results outperform the benchmark algorithm in terms of detection accuracy, speed efficiency and precision.

In recent years, IoMT technologies have been widely used by different researchers for the support of efficient network systems. These devices are integrated with the wireless network to collect the data from patients' bodies and process them using some intelligent methods. Additionally, the processed data are forwarded to the sink node and the medical specialists can analyze them for the diagnosis of any disease. However, it is observed that medical devices are very restricted and constrained for various resources and cannot perform high-cost processing and storage of massive data. Thus, different solutions have been proposed in the past to offer cloud-oriented services; however, it is also seen that some solutions are unable in saving sensitive information against threats. Moreover, traditional security approaches cannot be applied on limited constraint devices due to their dynamic and heterogeneous nature. However, few solutions have been proposed to achieve security problems with the additional overhead and management cost. Thus, this research proposed a machine learning SDN-enabled model for IoMT systems to improve the trustworthiness among medical objects and increase the performance of health systems in terms of delivery time. It also supports the integration of controllers to centralized complex computations and overcomes the communication load on medical things.

3. Proposed SDN-Enabled Model

This section explains the working flow of the proposed model. The proposed model is comprised of two main algorithms. Its developed components are illustrated in Figure 1, consisting of three main layers, i.e., sensing network, SDN architecture, and user applications. The sensing layer is comprised of sensors, actuators, and communication devices to collect the patients' data and interact with each other to accomplish the transmission system. In the second layer, SDN routers, switches, and controllers are utilized for the efficient management of IoT resources by optimizing their performance in terms of computing power and energy consumption. Moreover, instead of direct communication of IoT nodes with the application layer, the proposed model utilizes the intelligent capability of the SDN controller and avoids unnecessary resources usage with a controlled flooding mechanism. The application layer contains the e-health services that cooperate with IoT data and facilitate the medical team to diagnose the disease or any infection with appropriate treatment. Using a security scheme, the SDN controller also decreases the overheads on restricted resources for IoT devices in maintaining data privacy and centralized network management. Accordingly, all the layers interact cooperatively to increase the performance of IoMT systems intelligently and securely. In the proposed model, the control plane is designed to utilize centralized management of the network for data routing and security mechanisms. It supervised the data plane for maintaining the forwarding tables. The proposed model is comprised of two main algorithms. The first one is for classifying the IoT nodes using the machine learning technique and lessening the communication distance with management cost. Additionally, it reduces the computational overloads over the channels and avoids unnecessary data re-directing. The second algorithm is used for a centralized security system using the programmable structure of the SDN controller. The controller keeps track of the global data about the IoT layer and manages the resources of the node efficiently. It offers high-level security for the unpredictable environment by protecting sensitive data against threats with intelligent control and management of network resources. Initially, the proposed model executes the mean shift clustering [42], an unsupervised machine learning algorithm, which aims to group the IoT sensors in various collections. Unlike most of the other existing techniques, the proposed model does not consider the pre-defined network assumptions. We consider that IoT sensors X are deployed with a limited transmission radius. Initially, it picks a sensor randomly x_i and searches for a neighbor N such as $x_i \varepsilon\ X$ within its circular sliding window, whereas the circular sliding window is dependent on the transmission radius. The transmission radius moves slightly to enclose the neighbor nodes. Based on the positioning coordinates of enclosed sensors, the mean shift M_s for the node x can be computed as given in Equation (1).

$$M_s = \sum_{i=1}^{N} Y \times [(x_i - x)x_i / (x_i - x)] \tag{1}$$

where Y is the number of iterations. Additionally, the neighbors are updated in each iteration using the transmission radius of the source node. Accordingly, the proposed model iteratively groups each IoT sensor to the nearest centroid point of the cluster. Afterward, it makes use of the distance and link estimation factors for the selection of cluster heads. Each cluster head is associated only with particular nodes and acts as a manager inside the edge. Let us consider that $d(n)$ is the distance of the node n from centroid and $lk(n)$ is the measurement of link performance, then the selection method for cluster head $f(n)$ is defined in Equation (2).

$$f(n) = min(d(n)) \times max(lk(n)) \tag{2}$$

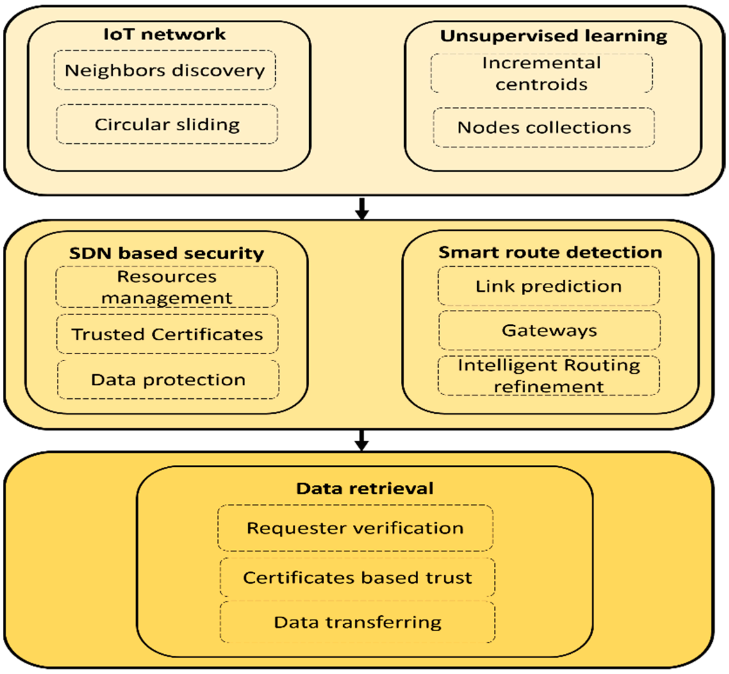


Figure 1. Block diagram of the proposed model.

Using SDN, a control plane is separated from the data plane and the controller has a global view of the entire network structure. In the proposed model, the control plane maintains the network entries that are comprised of nodes statistics, the priority of wireless channels, and routes information. The stored entries are updated dynamically on certain events. Using such information, the control plane is designed and programmed to decide how routes are selected for achieving network routing and support to an intelligent decision-making system. The controller obtains the stored information efficiently and exploits the network resources in terms of energy efficiency, communication bandwidth, and load sharing. Later, the data plane utilizes the network devices and sensors to follow the implanted rules by the control plane to accomplish data flow. It uses the nodes statistics to determine the condition of links using the status function $c(n)$ for a node n and accomplished forwarding process. The computation of $c(n)$ is dependent on the realistic metrics such as round trip latency $rtl(n_i)$ and packet reception rate $prr(n_i)$ for beacon packets in a time interval T_i as given in Equation (3). Using the updated values of such realistic metrics, the proposed model is trained under the control of SDN to predict the efficient links as a source of routing. Additionally, at the end of the preset interval, the latest information is provided to the control plane to make the network records up to date.

$$c(n) = min(rtl(n_i)) + max(prr(n_i)) \tag{3}$$

Accordingly, the link whose round trip latency is minimum and packet reception ratio is high will be considered as the more suitable link. Afterward, the IoT data move to the SDN layer that consists of switches, routers, and the central controller. All the switches and central controllers communicate with each other using the Open Flow protocol. The switches perform the role of gateways and offer opportunities for dual-level services. Firstly, it manages the trust-oriented communication with a centralized controller, and secondly, it secures the network data against threats for IoT networks. The SDN controllers execute the high-cost security algorithm and lower the computation power for gateways and IoT nodes. In the beginning, the SDN controller generates trusted certificates for the gateways and distributed them securely in an authentic manner. The trusted certificates offer reliable communication to avoid packet disturbing and flooding of malicious traffic. The certificate consists of two parts: one is data and the other is signature. The data part is comprised of ID and associated public key using an RSA algorithm [43] for the particular gateway node, while the signature part is comprised of the digital signature using the private key of the centralized controller C_r. Let us suppose that a and b are gateways and obtain the trusted certificates as defined in Equations (4) and (5).

$$C_r \longrightarrow \; Cert_a = E\_pr\ (ID_a\ ,\ K_{au}) \tag{4}$$

$$C_r \longrightarrow \; Cert_b = E\_pr\ (ID_b\ ,\ K_{bu}) \tag{5}$$

Upon receiving the trusted certificates, the gateway nodes can interchange them for authentication and later can become a part of the network services. In such a system, the generated public keys may be distributed and store securely against anonymous threats and remain its validity with authenticity. Moreover, the proposed model makes use of a randomized encryption function E for the IoT layer that maps the nodes data D_i to encrypted form C_i using the random number r_i, as defined as Equation x.

$$E\!:\; C_i = D_i \times k_i(r_i) + v \tag{6}$$

where $k_i \varepsilon$ keyspace K, r_i ε space of random numbers R.

Along with the randomized encryption function, each node adds the authentication code v to verify data records on the other end. Afterward, the counter of data routing increases by 1, i.e., $D_i + 1$, and data of IoT network are routed to the cloud systems in an increment by combining the cipher blocks in the form of blockchain. It significantly increases the trust level of data protection and integrity with the least resources usage and attains nominal computing energy of nodes. Once data are stored on cloud systems, the proposed model secures the access of IoT data for authorized users and ensures the retrieval of data. Each node that needs to access the data from the cloud declares its identification ID. Upon receiving the ID, the cloud server first verifies its maliciousness from the logged history. In this case, if it is found to be malicious then the cloud server denies its request for data access. After the verification of the trusted node, the cloud server cs_r utilizes secure exchanges for the signed keys s_i with authorized users u_i using public-private cryptography and obtains encrypted blocks as given in Equation (7).

$$cs_r \longrightarrow u_i\!:\; k_u(k_r\,(s_i, ID,\,) + r_0 \tag{7}$$

where k_u is a public key, k_r is private key and r_0 is the random number.

This security is executed with the identification of the trustee node using its unique ID that needs to collect the data from a cloud server. If it is found to be faulty on the cloud server, then it is marked as malicious and further requests will not be accepted.

Figure 2 illustrates the working flowchart of the proposed model. Its main components are data collection from IoT networks and repeat-generated centroids using neighbors until IoT nodes are organized into collections. Next, near-optimal routes are predicted from the IoT network layer to SDN switches without predefined assumptions. The SDN component in the proposed model manages the network resources and offers a balancing load for the IoT network. The SDN gateways are collaborated with the centralized controller to deploy the security against malicious and unauthentic nodes. It supervises the network operations using trusted certificates and initiates the routing phase in a systematic approach. Upon receiving the request from application users to facilitate its request, the proposed model first verifies its authentication and, in case of authorized status, the cloud servers offer the needed service. However, if the requestee node is found to be malicious, its identity is marked as faulty, and received requests are not accepted. Additionally, signed keys are generated among cloud servers and application users to producing encrypted blocks and attains privacy with authentication. Algorithm 1 illustrates the pseudocode of the proposed model.

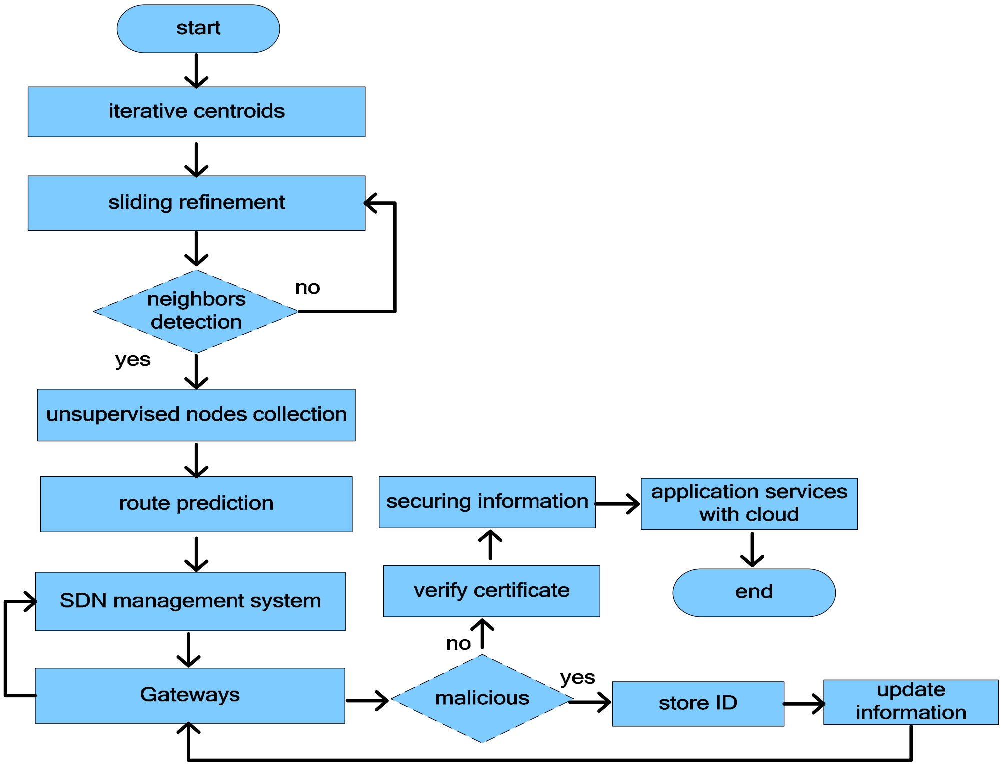


Figure 2. Flow chart of the proposed model.

Algorithm 1 Machine learning SDN-enabled secured model.

```
Input: sensors X, SDN controller $C_{SDN}$, SDN switches $S_{SDN}$
Output: $f(n)$, $route(i,j)$ $cert(i)$, $C_i$, $E(D,K)$
randomly chooses $x_i$ and searches
identify neighbor $N$, $x_i \varepsilon\ X$
procedure iterative centroids
for each node $N \in [1{:}X]$
do
compute mean shift $M_s$ for $y$ iterations
$m_i$ broadcast beacons to $N_i$
arrange nodes to the nearest centroid
end for
for each $C_i$ $N \in [1{:}X]$
do
compute $f(n) = min(d(n)).\ max(lk(n))$
adv.info $(f(n))$
end for
$C_r \ \rightarrow G_{SDN}(i)$: $Cert(i)$
$node\ i\ \ \rightarrow node\ j:\ cert(i)\ \longrightarrow\ cert(j)$
initiate routing phase after verification of $Cert$
for each $D_i$ $N \in [1{:}n]$
$E\!:\ C_i = D_i \times k_i(r_i) + v$
end for
$cs_r \rightarrow u_i$ \\ Requestee send Req packet to the application user
$k_u(k_r(s_i, ID) + r_0$ \\ $generate\ signed\ key$
call encryption $E(D,K)$
end procedure
```

4. Experiments

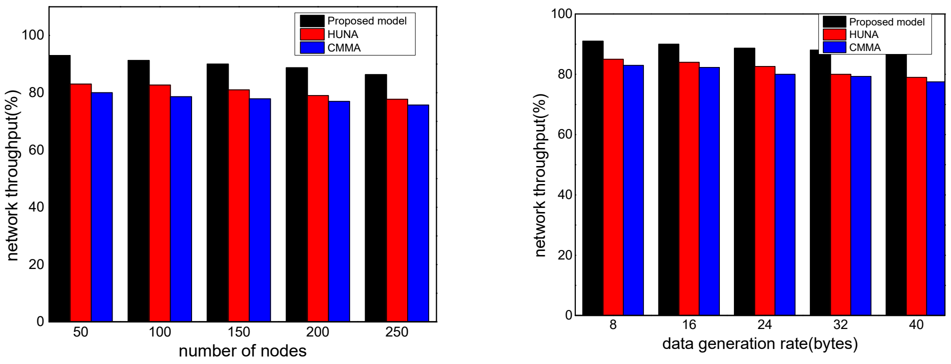
The proposed model utilizes the Open Network Operating System (ONOS) [44], an open-source controller in a Linux platform, which is developed for high performance and scalability. It offers a high-level programmatic interface for the design and development of SDN applications and manages the topology and activities of the network systems. The experiments are discussed in terms of network throughput, packet drop ratio, data delay, and faulty packets among the proposed model, HUNA and CMMA. To verify the performance of the proposed model, we deployed two scenarios. One is varying data generation and the other is varying number of nodes. The varying number of nodes is fixed to 50 to 250, and the varying data generation rate is 8 bytes to 40 bytes. The energy level of all the IoT nodes is set to 5 j with a transmission power of 5 m. Some SDN switches are deployed to perform the role of gateways. Nodes are randomly deployed, and some nodes are considered malicious. The positioning coordinates are used to determine the distance among nodes. Additionally, high-power wireless devices are incorporated into the scenario for the performance of gateway nodes with limited mobility. Table 1 illustrates the default simulation configurations for the analysis of the proposed model and other solutions.

Table 1. Simulation configurations.

Parameters	Values
Initial energy	5 j
Sensors	varying 50–250
Nodes position	Random
Malicious nodes	10
Data bytes	8–40
Simulation time	2000 s
Transmission power	5 m
Wireless standard	IEEE 802.11

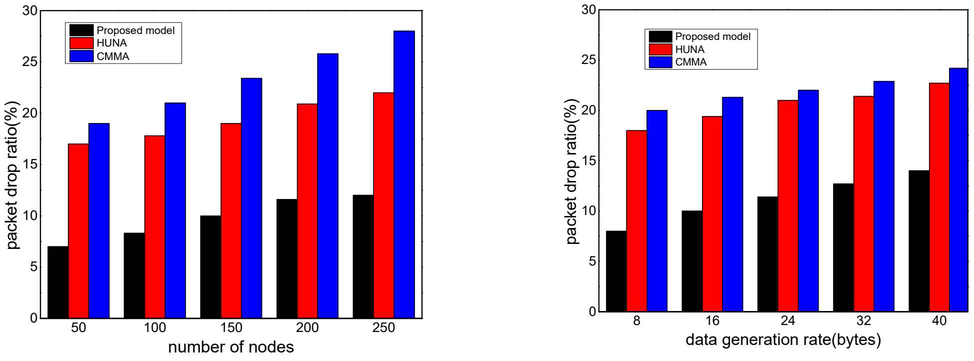
In Figure 3a,b, the experimental results illustrate that the proposed model increases the network throughput by an average of 13% and 10% as compared to other solutions in terms of a varying number of nodes and data generation rate. Due to this, the proposed model utilizes an iterative centroid approach to group the nodes in a particular cluster. Additionally, each cluster is managed by a particular cluster head that is more optimal than other nodes. The multi-hop transmission system for routing the IoT data not only optimizes the performance but also decreases the energy hole problem by balancing the network load using robust links. Additionally, the machine learning approach predicts an intelligent strategy to identify the neighbors with nominal computing resources with the support of SDN architecture. Furthermore, the transmission system is secure, using a controller that supervised the data forwarding by identifying the reliable paths with better network management. Moreover, the proposed model makes use of SDN gateways for interaction with IoT networks and controllers which highly improves the delivery ratio.

In Figure 4a,b, the experimental results are demonstrated for the packet drop ratio in terms of a varying number of nodes and data generation rate. It is observed that the proposed model improves the packet drop ratio by an average of 39% and 41% in the comparison of the existing solution. It is due to the make use of machine learning approach to guide the nodes for forwarding the data packets with minimum congestion and realistic parameters based on the cooperative work of SDN switches and controllers. Additionally, malicious entries are marked as defective for the next communication, and unknown nodes are not allowed for becoming a part of the routing system. The gateways on the SDN layer not only support the security for the IoT network but on the other hand, facilitates the controller to update the global knowledge of the network. Such a system improves the process for the identification of faulty links and efficiently utilizes the communication bandwidth. Moreover, it decreases the unauthentic sessions with the IoT network, and data is safely forwarded to cloud servers using secured routes. Unlike other solutions, the proposed model utilizes the constraint resources very efficiently with the support of SDN architecture and manages the delivery of nodes' data smoothly.



(**a**) (**b**)

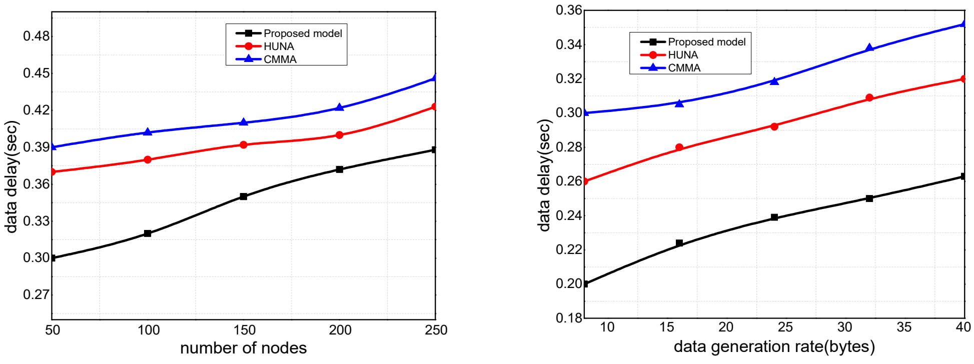
Figure 3. Performance of network throughput with the number of nodes (**a**) and packet generation rate (**b**).



(**a**) (**b**)

Figure 4. Performance of packet drop ratio with the number of nodes (**a**) and packet generation rate (**b**).

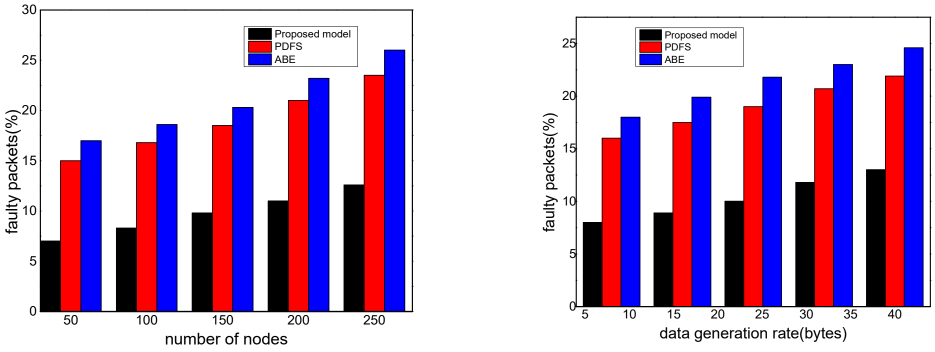
Figure 5a,b demonstrate the performance results of the proposed model with other solutions in terms of data delay. It is observed that it improves the ratio of network data effectively and timely. The experimental results show that the proposed model improves the result by an average of 11% and 21% as compared to other solutions. It incorporates the congestion status to predict the optimal channels for sending the data from the IoT layer to the cloud layer under the management of the SDN controller. Additionally, the architecture of SDN facilitates the constraint-oriented nodes to lower their battery usages and send the data promptly with a longer route lifetime. Moreover, due to balancing the energy and link and transmission load in routing between generated clusters, the network performance avoids frequent network disconnectivity. The proposed model efficiently utilizes the robust architecture of SDN using gateways and updates the stored information of links on the controller. Accordingly, the proposed model decreases the unbearable delay in data delivery. Additionally, the trusted certificates identify the malicious nodes timely, and accordingly, faulty nodes are not able to drop the actual data, thus significantly improving the data delay.



(**a**) (**b**)

Figure 5. Performance of data delay with varying number of nodes (**a**) and packet generation rate (**b**).

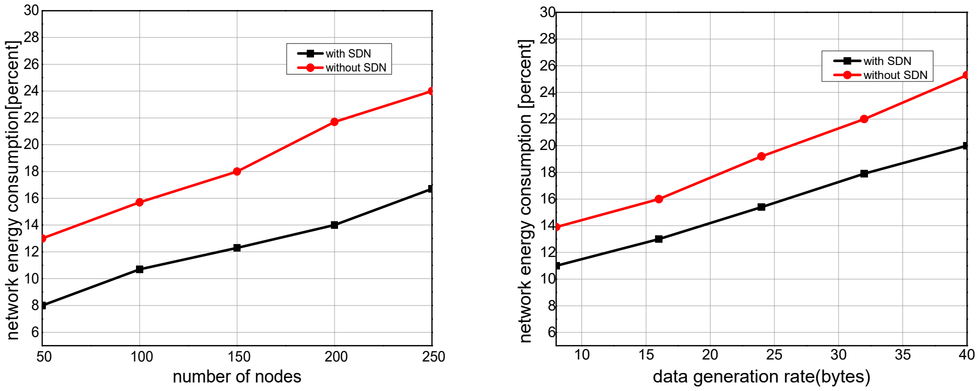
Figure 6a,b explain the verified result of the proposed model against the existing solution in terms of faulty data packets. It is seen that the proposed model improves the ratio of faulty data packets by an average of 46% and 49%. In the proposed model, the centralized controller and SDN gateway are responsible to establish trust and maintain data security among constraint nodes. It not only reduces the load of the IoT network but also manages the privacy and authentication for selected routes with the centralized management of SDN. Accordingly, only trustee nodes are allowed on IoT networks to send and receive route requests on the fault-tolerant links. Additionally, trusted nodes exchange their key information securely for data encryption and integrity, which ensures data access only by authentic users. Moreover, the cloud servers and application users make use of the generation of signed secret keys that support identifying the malicious users on time and provide a low-cost data security algorithm. Such an algorithm denies the request of malicious nodes and marked them faulty, so subsequent requests from the same identity are not accepted.



(**a**) (**b**)

Figure 6. Performance of faulty packets with a varying number of nodes (**a**) and packet generation rate (**b**).

Figure 7a,b explain the verified result of the proposed model against the existing solution for the usage of energy resources with and without an SDN controller. The experimental results demonstrate that the scenario with the deployment of SDN efficiently utilizes energy efficiency and decreases the consumption amount by 30% and 21%. The experiments are performed under a varying number of nodes and data generation rate. It is observed that the proposed model is based on SDN technology and OpenFlow protocol, which offers centralized management for the network infrastructure. In the proposed model, the controller monitors the data plane entities using the method of passive monitoring and updates the information of wireless channels with valid routes entries. Accordingly, by exploiting the network conditions, the SDN controller dynamically controls the constraint nodes and gateways. It explicitly decreases the overheads and improves energy efficiency by using the obtained information from the lower layer. Additionally, the programmed control plane utilizes the set of rules explicitly and decides the forwarder nodes to balance the load of energy consumption. Moreover, the controller fetches the stored information from the data plane for efficient bandwidth and resource management. On the other hand, the scenario without SDN consumed too much energy consumption in various activities because there is no global database on the central point and each node interacts with others using its resources. Furthermore, due to the absence of a centralized controller, most of the sensors' data are dropped or even retransmitted and consumed additional resources of the constraint network.



(**a**) (**b**)

Figure 7. Performance of network energy consumption under a varying number of nodes (**a**) and packet generation rate (**b**) with and without SDN.

5. Conclusions

This paper presents a machine-learning model with SDN-enabled security for the improvement of network consumption and delivery of the IoT services on time. The SDN centralized model is used to reduce control plane overhead over the deployed IoT network. It uses the machine learning iterative centroid computation to group the nodes and optimizes the routing performance in a realistic environment. The developed routing scheme is collaborated with the SDN controller in establishing the security chain with nominal overheads and energy resources. Additionally, in the evaluation of the status function, the overload links are not utilized in routing decisions. Moreover, to protect network services from malicious attacks, the intelligent centralized controller supports the data from disclosure and decreases the usage of nodes' power with efficient management operations for critical infrastructure. The experimental results demonstrated that the proposed model improved the performance for varying packet generation rates in terms of data delay and network throughput by 21% and 10%. In future work, we aim to introduce multiple controllers to enhance the scalability of the proposed model. Additionally, we would like to utilize the deep learning technique to improve the accuracy of IoT services.

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

Funding: This research has no external funding.

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

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

References

1. 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]
2. 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]
3. Sun, X.; Ansari, N. EdgeIoT: Mobile edge computing for the Internet of Things. *IEEE Commun. Mag.* **2016**, *54*, 22–29. [CrossRef]
4. 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]
5. Ahmed, S.F.; Islam, R.; Nath, T.D.; Ferdosi, B.J.; Hasan, A.S.M.T. G-TBSA: A Generalized Lightweight Security Algorithm for IoT. In Proceedings of the 2019 4th International Conference on Electrical Information and Communication Technology (EICT), Khulna, Bangladesh, 20–22 December 2019.
6. Dhanvijay, M.M.; Patil, S.C. Optimized mobility management protocol for the IoT based WBAN with an enhanced security. *Wirel. Netw.* **2021**, *27*, 537–555. [CrossRef]
7. Sodhro, A.H.; Pirbhulal, S.; Sangaiah, A.K. Convergence of IoT and product lifecycle management in medical health care. *Future Gener. Comput. Syst.* **2018**, *86*, 380–391. [CrossRef]
8. Aktas, F.; Ceken, C.; Erdemli, Y.E. IoT-based healthcare framework for biomedical applications. *J. Med Biol. Eng.* **2018**, *38*, 966–979. [CrossRef]
9. Thamilarasu, G.; Odesile, A.; Hoang, A. An Intrusion Detection System for Internet of Medical Things. *IEEE Access* **2020**, *8*, 181560–181576. [CrossRef]
10. Islam, S.M.R.; Kwak, D.; Kabir, H.; Hossain, M.; Kwak, K.-S. The internet of things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
11. Páez, D.G.; Aparicio, F.; de Buenaga, M.; Ascanio, J.R. Big data and IoT for chronic patients monitoring. In *International Conference on Ubiquitous Computing and Ambient Intelligence*; Springer: Berlin/Heidelberg, Germany, 2014.
12. 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]
13. Yin, H.; Jha, N.K. A health decision support system for disease diagnosis based on wearable medical sensors and machine learning ensembles. *IEEE Trans. Multi-Scale Comput. Syst.* **2017**, *3*, 228–241. [CrossRef]
14. Verma, V.K.; Gupta, P.; Jha, A.V.; Barbhuiya, P.N. Recent trends in wireless sensors for medical applications. In Proceedings of the 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 6–8 April 2017.
15. Bharti, V.; Biswas, B.; Shukla, K.K. A novel multiobjective gdwcn-pso algorithm and its application to medical data security. *ACM Trans. Internet Technol.* **2021**, *21*, 1–28. [CrossRef]
16. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721. [CrossRef]
17. Sliwa, B.; Piatkowski, N.; Wietfeld, C. LIMITS: Lightweight machine learning for IoT systems with resource limitations. In Proceedings of the ICC 2020–2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020.
18. Gkountis, C.; Taha, M.; Lloret, J.; Kambourakis, G. Lightweight algorithm for protecting SDN controller against DDoS attacks. In Proceedings of the 2017 10th IFIP Wireless and Mobile Networking Conference (WMNC), Valencia, Spain, 25–27 September 2017.
19. 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]
20. Babar, M.; Tariq, M.U.; Jan, M.A. Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid. *Sustain. Cities Soc.* **2020**, *62*, 102370. [CrossRef]
21. Rahman, A.; Chakraborty, C.; Anwar, A.; Karim, R.; Islam, J.; Kundu, D.; Rahman, Z.; Band, S.S. SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic. *Clust. Comput.* **2021**, 1–18. [CrossRef]
22. Cicioğlu, M.; Çalhan, A. Energy-efficient and SDN-enabled routing algorithm for wireless body area networks. *Comput. Commun.* **2020**, *160*, 228–239. [CrossRef]
23. Ahmed, O.; Ren, F.; Hawbani, A.; Al-Sharabi, Y. Energy optimized congestion control-based temperature aware routing algorithm for software defined wireless body area networks. *IEEE Access* **2020**, *8*, 41085–41099. [CrossRef]
24. Jimenez, J.M.; Romero, O.; Lloret, J.; Diaz, J.R. Energy savings consumption on public wireless networks by SDN management. *Mob. Netw. Appl.* **2019**, *24*, 667–677. [CrossRef]
25. von Rechenberg, M.; Rettore, P.H.L.; Lopes, R.R.F.; Sevenich, P. Software-Defined Networking Applied in Tactical Networks: Problems, Solutions and Open Issues. In Proceedings of the 2021 International Conference on Military Communication and Information Systems (ICMCIS), The Hague, The Netherlands, 4–5 May 2021.
26. Priya, I.D.; Silas, S. A survey on research challenges and applications in empowering the SDN-Based Internet of Things. In *Advances in Big Data and Cloud Computing*; Springer: Singapore, 2019; pp. 457–467.
27. 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.* **2020**, *4*, 149–168. [CrossRef]
28. Alex, S.; Pattathil, D.P.; Jagalchandran, D.K. SPCOR: A secure and privacy-preserving protocol for mobile-healthcare emergency to reap computing opportunities at remote and nearby. *IET Inf. Secur.* **2020**, *14*, 670–682. [CrossRef]

29. Noel, A.B.; Abdaoui, A.; Elfouly, T.; Ahmed, M.H.; Badawy, A.; Shehata, M.S. Structural health monitoring using wireless sensor networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1403–1423. [CrossRef]
30. De Assis, M.V.; Carvalho, L.F.; Rodrigues, J.J.; Lloret, J.; Proença, M.L., Jr. Near real-time security system applied to SDN environments in IoT networks using convolutional neural network. *Comput. Electr. Eng.* **2020**, *86*, 106738. [CrossRef]
31. Nivaashini, M.; Thangaraj, P.; Sountharrajan, S.; Suganya, E.; Soundariya, R.S. Effective Feature Selection for Hybrid Wireless IoT Network Intrusion Detection Systems Using Machine Learning Techniques. *Adhoc Wirel. Sens. Netw.* **2021**, *49*, 175–206.
32. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
33. Sollins, K.R. IoT big data security and privacy versus innovation. *IEEE Internet Things J.* **2019**, *6*, 1628–1635. [CrossRef]
34. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and privacy in smart cities: Challenges and opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]
35. Sharma, D.K.; Dhurandher, S.K.; Woungang, I.; Srivastava, R.K.; Mohananey, A.; Rodrigues, J.J.P.C. A machine learning-based protocol for efficient routing in opportunistic networks. *IEEE Syst. J.* **2016**, *12*, 2207–2213. [CrossRef]
36. Zhu, D.; Sun, Y.; Du, H.; Cao, N.; Baker, T.; Srivastava, G. HUNA: A method of hierarchical unsupervised network alignment for IoT. *IEEE Internet Things J.* **2020**, *8*, 3201–3210. [CrossRef]
37. Vashishth, V.; Chhabra, A.; Sharma, D.K. GMMR: A Gaussian mixture model based unsupervised machine learning approach for optimal routing in opportunistic IoT networks. *Comput. Commun.* **2019**, *134*, 138–148. [CrossRef]
38. Chakrabarty, S.; Engels, D.W.; Thathapudi, S. Black SDN for the Internet of Things. In Proceedings of the 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, Dallas, TX, USA, 19–22 October 2015.
39. Khan, S.; Akhunzada, A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). *Comput. Commun.* **2021**, *170*, 209–216. [CrossRef]
40. 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]
41. Javeed, D.; Gao, T.; Khan, M. SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT. *Electronics* **2021**, *10*, 918. [CrossRef]
42. Cheng, Y. Mean shift, mode seeking, and clustering. *IEEE Trans. Pattern Anal. Mach. Intell.* **1995**, *17*, 790–799. [CrossRef]
43. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
44. Berde, P.; Gerola, M.; Hart, J.; Higuchi, Y.; Kobayashi, M.; Koide, T.; Lantz, B.; O'Connor, B.; Radoslavov, P.; Snow, W. ONOS: Towards an open, distributed SDN OS. In Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, Chicago, IL, USA, 22 August 2014.