# Efficient Data Uncertainty Management for Health Industrial Internet of Things using Machine Learning

**Khalid Haseeb[1], Tanzila Saba[2], Amjad Rehman[3], Imran Ahmed[4], Jaime Lloret[5,6]**

[1] Department of Computer Science, Islamia College University, Peshawar, Pakistan; email: khalid.haseeb@icp.edu.pk
[2] Artificial Intelligence & Data Analytics Lab (AIDA) CCIS Prince Sultan University Riyadh Saudi Arabia; email: drstanzila@gmail.com
[3] Artificial Intelligence & Data Analytics Lab (AIDA) CCIS Prince Sultan University Riyadh Saudi Arabia; email: rkamjad@gmail.com
[4] Institute of Management Sciences, Peshawar, Pakistan; email: imran.ahmed@imsciences.edu.pk
[5] Universitat Politenica de Valencia, Spain; email: jlloret@dcom.upv.es
[6] Staffordshire University, Stoke, UK

***Abstract*—** In modern technologies, the Industrial Internet of Things (IIoT) has gained rapid growth in the fields of medical, transportation, and engineering. It consists of a self-governing configuration and cooperated with sensors to collect, process, and analyze the processes of a real-time system. In the medical system, Healthcare Industrial IoT (HIIoT) provides analytics of a huge amount of data and offering low-cost storage systems with the collaboration of cloud systems for the monitoring of patient information. However, it faces certain connectivity, nodes failure, and rapid data delivery challenges in the development of e-health systems. Therefore, to address such concerns, this paper presents an efficient data uncertainty management model for HIIoT using machine learning (EDM-ML) with declining nodes prone and data irregularity. Its aim to increase the efficacy for the collection and processing of real-time data along with smart functionality against anonymous nodes. It developed an algorithm for improving the health services against disruption of network status and overheads. Also, the multi-objective function decreases the uncertainty in the management of medical data. Furthermore, it expecting the routing decisions using a machine learning-based algorithm and increases the uniformity in health operations by balancing the network resources and trust distribution. Finally, it deals with a security algorithm and established control methods to protect the distributed data in the exposed health industry. Extensive simulations are performed and their results reveal the significant performance of the proposed model in the context of uncertainty and intelligence than benchmark algorithms.

***Index Terms*—** Data management, Distributed algorithms, Industrial Internet of Things, Machine learning, Risk assessment

## 1. INTRODUCTION

Communication systems, wireless structures, and sensors are integrated [1, 2] in different modern networks for the collection and processing of continuous data [3]. Most of the network objects are self-configured and versatile in terms of energy, processing, and storing resources. It collects running data from the real-time system and utilizes various switches for the transmission towards sink node. All the application users that are connected to network systems are obtained real-time data based on their demand. IIoT enables a smooth observing and communication system for e-health industries [4, 5] based on wearable devices and manages the sensitive data for patient records. Wireless body area network (WBAN) [6, 7] is a developing technology that is applied to various sectors such as healthcare, emergency rescue, sports, and entertainment, etc. The data is gathered using small-sized sensors and communication machines that are linked using 5G wireless broadband technologies to facilitate various operations of the health industry. Later, it is transmitted towards storage clouds for computing and processing and decreasing response time for critical and emergency applications. The emergency centers and medical experts retrieved the collected data using smart devices and analyze it for the recovery of patient health. As medical applications are very crucial and need a timely response by medical experts, therefore, such systems normally claim for the efficient and organized solution with low response time and trustworthiness [8, 9]. In the medical system, most of the applications exploited the multi-hop paradigm for transmitted the patients' data over the Internet and need to protect its prohibited operations against anonymous objects. Since applications of the health industry are based on the constraint-oriented IoT network, therefore most of the existing routing protocols of ad-hoc networks are not feasible for it. In the health industry, data transmission is comprised on three distinct phases. In the first phase, HIIoT sensors and computing devices interact with the patient body that collects and process the information. Also, it transfers the patients' data to the central server using next-hop or forwarding nodes. In the second phase, the local coordinator interacts with sink node through the wireless medium and need a high level of security from malicious attacks due to its open system architecture. In the third phase, single or multiple cloud centers are exposed for the storage of medical information [10, 11]. All the connected medical experts can collect the patients' data and initiate the process of remote monitoring and on-time treatment. Therefore, providing robust connectivity so that IoT devices can interconnect with each other without losing sensitive data, routing maintenance with nominal communication cost, improving data security and lightweight integrity of patient records are some demanding tasks for the health industry [12,

13]. The paradigm of the health industry using network technologies and medical sensors is depicted in Figure 1. This research study presents the efficient model for data uncertainty management for health systems using machine learning with securing the transmission services. It offers trustworthiness and decreasing the insecurity among medical sensors and improves the reliability of health data. It also contributes to the efficacy of the health industry with cloud services in terms of response time and network resources. Furthermore, a multi-class decision tree classifier is applied for the selection of next-hop and decreases the probability of data errors with the least communication disturbance. Moreover, the low-cost securing algorithm supports secret sharing to attain data privacy and integrity, which safely stores the data of the health industry on cloud centers.

The main contributions of the EDM-ML model are highlighted below.

i. The routing algorithm is developed, which determines the greedy forwarders section based on a multi-objective function. It optimizing the weighted cost and ensures self-reliance to access patients' data for health centers.
ii. Threshold data is utilized by a multi-class decision tree classifier to train the nodes for routing the health data towards cloud storage.
iii. It also deploying secret information to secure sensitive data with lightweight overhead and offers data uncertainty management in terms of privacy, integrity, and authentication.
iv. Also, the security analysis for EDM-ML has demonstrated significant performance against anonymous threats. Moreover, simulation-based experiments significantly validate the efficacy of the proposed model than other benchmark algorithms.

The research work is structure as follows. Related work and problem background are presented in Section 2. The system model and components of the proposed model are discussed in Section 3. An extensive experimental test against benchmark algorithms is elaborated in Section 4. In the end, Section 5 concludes the research article.

## 2. RELATED WORK

In modern technology, both sensor networks and IoT are collaborated efficiently [14-16] to develop many smart applications for real systems. Due to its unique characteristics and dynamic attributes IIoT network is widely used for industrial and academic fields. In medical systems using HIIoT, the communication technologies and sensors can be divided into distinct phases. In the beginning, medical sensors are located inside or implanted on the body of the patient and measure the health data. The gathered data is transmitted to the local data collector, which performs aggregation and compression. Afterward, the aggregated medical data is transmitted towards cloud centers using intermediate edge devices based on multi-hop paradigm and medical experts can access the data for appropriate needful and treatment. However, the patients' data is very sensitive and can be compromised in terms of privacy, and integrity over the uncontrolled channels, therefore securing such a communication model is an interesting and challenging task [17-19]. Authors in [20], briefly reviewed the basic models of machine learning and explain the uses in IoT-based systems. Also, they proposed Q-learning (QL) based reinforcement learning paradigms for IoT-based eHealth systems. Also, the goal of the proposed work is to contribute and refining the motivation, problem formulation, and methodology of machine learning algorithms for MAC layer channel access. Based on the results, it optimizes the performance for densely deployed devices environment. In [21], the authors proposed a sensor/sensor-tag based smart healthcare environment. It makes use of S-USI and offering data security in terms of privacy. Also, to increase the authentication mechanism, a robust secure-based S-USI mechanism for pervasive services in the cloud is proposed using a well-formed coexistence protocol proof. Also, using the formal security analysis, the importance of the proposed work is demonstrated for security efficiency. Authors in [22] proposed a non-linear mathematical model-based routing protocol for WBAN. In the proposed protocol, two non-linear mathematical models Model 1 and Model 2 for WBANs are used. In Model 1, the authors improved the rate of data transmission, while the aim of Model 2 is to decrease the ratio of energy consumption. The proposed protocol is evaluated using simulation and results depict the significant performance of the proposed work than other solutions in terms of energy consumption, transmission rate, and path loss. Priority-based energy-efficient routing algorithm (PERA) is presented in [23]. It generates the priority using the nature of the data. High priority is given to emergency data, second priority is given to on-demand data, and third priority is assigned to periodic data among nodes. Also, two nonlinear optimization models are proposed for enhancing the network lifetime and decreasing energy consumption. In[24], authors developed a new routing algorithm, which makes use of a fuzzy-based Dijkstra algorithm. It adopts the architecture of a software-defined network (SDN) that changes the existing routing path in data transmission and balancing the network resources. The simulated results demonostrate that proposed solution outperforms than traditional approaches and impoved the performance in terms of network lifetime and energy consumption.

Authors in [25], proposed an intelligent security system called Intelligent Framework for Healthcare Data Security (IFHDS). It offers a secured approach to process big data using a column-based approach. The sensitive data is split into several parts based on the level of its sensitivity and each part is stored separately on distributed cloud storage. Splitting data provide a lower cost on data encryption and decreases the computing resources of the medical devices. The experimental results illustrated the proposed framework protecting the patient data with an acceptable computation time as compared to other security approaches. In [26], the authors presented a novel architecture and its implementation for data sharing between inter-organizational, which increases the

security level and privacy for patients' information. It makes use of semi-trusted cloud computing environments and reducing the complication of the network. The proposed architecture offers attribute-based encryption and cryptographic secret sharing to distribute the data across multiple clouds. Also, its implementation and verified results illustrate practical and feasible performance than other schemes. In [27], the authors proposed a privacy-preserving health data aggregation scheme, which securely gathers the patients' data from multiple sources and ensures a fair incentive for contributing patients. Also, it utilized signature techniques and retain reasonable incentives for patients' data. Moreover, the proposed solution integrates the Boneh-Goh-Nissim cryptosystem with Shamir's secret sharing to keep fault tolerance and data security. The results discussion demonstrate that the proposed scheme can cope with differential attacks, tolerate the failure of healthcare centers failures, and keep fair incentives for patients. Authors in [28], proposed the architecture for secure communication and allows the transferring of information, computing, network services, sensors data, and storage resources among the mHealth clouds. It comprises two main layers, and the routing algorithm is based on the shortest path first (SPF) to increase the connectivity and stability between the connected nodes. Based on the experiments, it is more secure, and highly scalable whenever new nodes are added. In [29], the authors proposed a secure framework that restricts insider attacks and improves security levels. It is comprised of different processes such as data uploading, slicing, indexing, encryption, distribution, decryption, retrieval, and merging. Also, before storing the big data on multi-cloud it performs a hybrid encryption algorithm and protects the communication against threats. The Simulation analysis is done with the realistic cloud storage scenario, and results demonstrated better outcomes than benchmark algorithms.

It is seen based on the related work that HIIoT is integrated with wireless technologies to provide a significant contribution to the health industry. Medical devices perform a vital role to further enhance the monitoring of health conditions using IoT networks. The IoT-based medical things capture the health data from the patient body and forwarded it either to medical centers or multi-clouds. It is observed that due to the lack of resources, on-time delivery of patients' data with the least latency disturbance for real-time health centers is a challenging task. It is also noticed that most of the solutions only offer consistent routing services to increase the performance of medical applications, however, most of them ignored the significance of privacy-aware solutions. Although, some solutions are proposed to cope with security issues of health applications but with additional computing cost and frequent data damages. Therefore, lightweight gathering algorithms along with privacy and integrity should be given high priority to avoid data breaches and potential threats [30, 31]. By keeping such factors, the proposed work presents an efficient model for HIIoT using a machine learning approach along with the security of health data. The proposed work utilizes a machine-learning algorithm to supports energy management, reliable delivery with the nominal communication delay for health data. Also, it securing health data from malicious threats and ensures privacy using a lightweight cryptographic secret sharing scheme.

## 3. PROPOSED EDM-ML MODEL

In this section, we present the discussion on the EDM-ML model in detail.

### *3.1 System Model*

This section elaborates the system model for the proposed EDM-ML model along with network assumptions. In the proposed work, we consider different HIIoT sensors with limited constraints and computing machines. All the HIIoT sensors have a preset transmission range with communication frequencies. The Global Positioning System (GPS) is deployed inside each sensor to determine position coordinates. Unlike continuously data sensing, we assumed that distributed sensors only collect the health data at a predefined time interval. A local table is maintained by each node to identify the neighbors' information and provide updated data for routing decisions by exploiting certain conditions. The proposed model operates in the multi-hop communication system and facilitates the forwarding of huge medical data with limited transmission power. The malicious nodes reproduce false messages to blockage or deny the network traffic. We assumed that HIIoT sensors are structure in an undirected graph $G$ with a set of edges $E$. Each edge only connects sequential nodes with a particular bandwidth. Before discussing the proposed model, the following network assumptions are considered.

i. All the nodes have the same properties with data sensing intervals.
ii. Each sensor node chooses the next hop using the optimization function.
iii. The transmission links are dual directional
iv. Edge and cloud devices are more controlling for storage and processing.
v. Each node only maintains the information of its nearest neighbors.

### *3.2 Architecture of EDM-ML model*

This section discussed the developed components of the proposed EDM-ML model. The architecture of the EDM-ML model for the healthcare industry is illustrated in Figure 1. In the beginning, using the multi-objective optimization method, a weighted cost is computed and supports to decision process. It utilizes the multi-class classifier for predicting the status of the nodes and leads to optimal health services. The weighted cost is determined using the multi-factors and it should be minimized among the neighbors.

It distributed the energy resource uniformly and estimate the channel performance by considering the fault degree in packet reception ratio. Secondly, unlike most of the existing solutions that greedily compute routing decisions with an additional overhead on medical devices, the proposed EDM-ML model exploits the decision tree as a multi-class classifier and performs the learning process using updated external data. Accordingly, it supports optimizing the routing performance in terms of reliable health services with network intelligence. Also, the proposed EDM-ML model offers an efficient collaboration of local coordinators to cloud systems using trustworthy intermediate links. In the end, it supports securing e-health service with robust transmission analysis against anonymous attacks and increasing the integrity of the health industry. The overview and flow of the EDM-ML model are depicted in Figure 2.

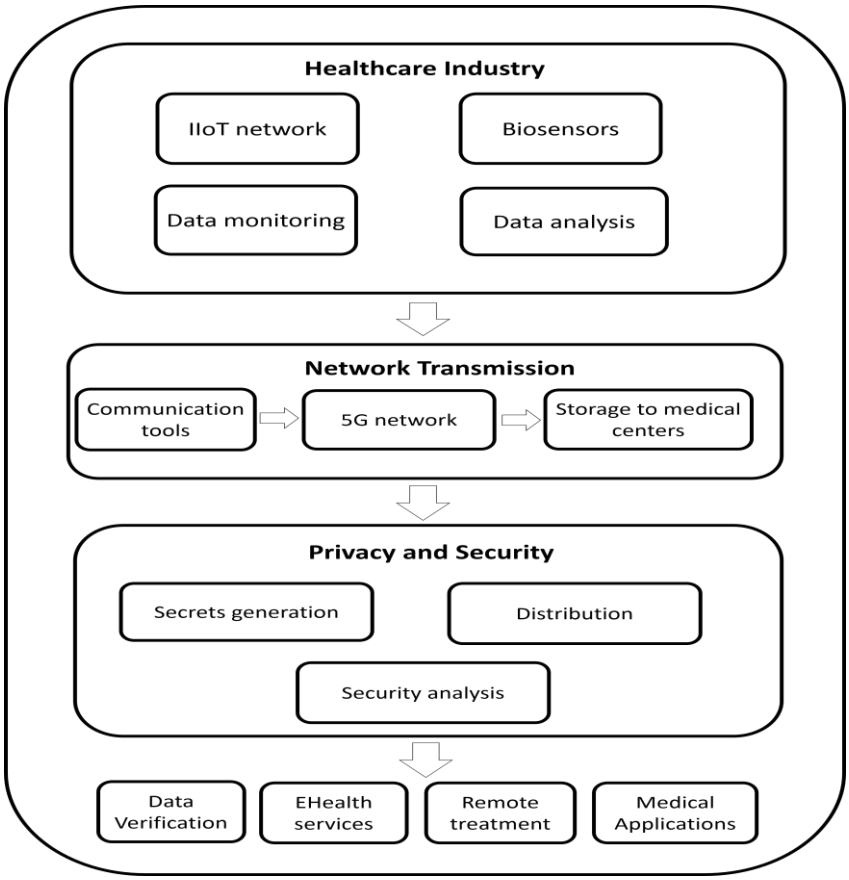



**FIGURE 1** Architecture of EDM-ML model for HIIoT

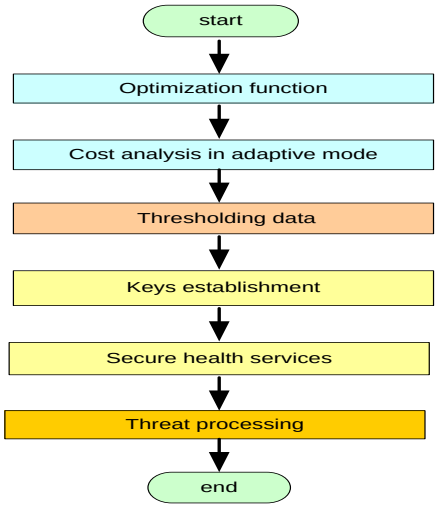


**FIGURE 2** Overview of the EDM-ML model

The EDM-ML model utilizes the optimization function and measures network performance at a regular time interval. Using weighted cost, the EDM-ML model updated the selection criteria of next-hop by incorporating the node trust $\boldsymbol{Tr_n}$, which is computed based on the three factors i.e. transmission cost, bandwidth availability, and the fault degree in packet reception rate $\boldsymbol{Ft_{PRR}}$. Also, each metrics performs a uniform contribution for evaluating the trust value using weighted metrics. During the data transmission, each node determines the values of the nodes from the neighbor table and computes weighted cost $\boldsymbol{f(n)}$, as defined in Equation (1).

$$\boldsymbol{min\ f(n)} = \alpha\ (\frac{\mathbf{1}}{\boldsymbol{P_c}}) + \boldsymbol{\beta Tr_n} \tag{1}$$

In Equation (1), $\boldsymbol{Tr_n}$ is the integration of $\boldsymbol{k}$ multiple factors using $\boldsymbol{F(x_n)}$ as given in Equation (2). Also, the summation of $\alpha+ \boldsymbol{\beta}$ must be equal to 1. It offers a balanced contribution to each factor and optimizes the decision of $\boldsymbol{f(n)}$.

$$\boldsymbol{Tr_n(i,j)} = \sum_{n=1}^{k} \boldsymbol{F(x_n)} \tag{2}$$

The power consumption $\boldsymbol{P_c}$ of the node $\boldsymbol{i}$ is directly proportional to the distance $\boldsymbol{d_{i,j}}$, and indicates if node $\boldsymbol{i}$ cover a longer distance to destination node $\boldsymbol{j}$, then it consumes high power consumption. The transmission distance of node $\boldsymbol{i}$ is denoted by $\boldsymbol{d(i)}$ and can be computed using an absolute value between nodes $\boldsymbol{n_i}$ and $\boldsymbol{n_j}$ as given in Equation (3).

$$\boldsymbol{d(i)} = \mathbf{1}/|\boldsymbol{n_i - n_j}| \tag{3}$$

The bandwidth availability $\boldsymbol{b_{wd}(i)}$ filters the residual space among nodes $\boldsymbol{n_i}$ and $\boldsymbol{n_j}$ as defined in Equation (4).

$$\boldsymbol{b_{wd}(i)} = |\boldsymbol{b_i - b_c}| + \boldsymbol{P_l} \tag{4}$$

where $\boldsymbol{b_i}$ is the initially available space, $\boldsymbol{b_c}$ is the consumed space and $\boldsymbol{P_l}$ is the probability of packet loss

The EDM-ML model integrates the fault degree of PRR and measures the symmetry of the particular link among source and neighbor nodes. It floods the beacon messages over the link at a particular time interval and records back the received acknowledgment packets $ack$. Accordingly, lower the $ack$ packets indicates the least strength of the link for node $i$ and $j$ and assumed as not appropriate for the data transmission at time $t$. Let's consider that $P_\alpha$ denotes the send data packets $ack_\mathrm{p}$ denotes the received acknowledgments, then $Ft_{\mathrm{PRR}}$ is defined in Equation (5).

$$\boldsymbol{Ft_{PRR}(i,j)} = \boldsymbol{P_\alpha}\ .\ \boldsymbol{ack} \tag{5}$$

Afterward, the EDM-ML model utilizes a multi-class classifier and divides the HIIoT sensors into three groups. The updated and computed information $\boldsymbol{f(n)}$ is collected to adjust the decision. It splits the HIIoT sensors into three groups $\sum_{i=1}^{n} \boldsymbol{G_n}$, where n denotes the number of groups. The nodes in $\boldsymbol{G_1}$ cannot take part in data transmission, while the situation of nodes in $\boldsymbol{G_2}$ and $\boldsymbol{G_3}$ is variable and based on the $\boldsymbol{f(n)}$ value. The values of $\boldsymbol{f(n)}$ specify the lower and higher probabilities in the range of (0, 1). If values of $\boldsymbol{f(n)}$ near or equal to 1, then nodes are structure in $\boldsymbol{G_2}$. On the other side, the nodes are arranged in $\boldsymbol{G_3}$ if their $\boldsymbol{f(n)}$ value is near or equal to 0 and indicates the lower priority for the contribution of data transmission. Accordingly, the nodes are arranged in the form of decision trees and split into multiple levels. Table 1 depicts the format of the multi-class decision classifier.

**Table 1.** Multi-class Classifier Features

| $f(n)$ | | | | Group |
|---|---|---|---|---|
| $E(i)$ | $d(i)$ | $b_{\mathrm{wd}}(i)$ | $Ft_{\mathrm{PRR}}(i,j)$ | $G_\mathrm{n}$ |

Afterward, the EDM-ML model provides management of e-health services with the consideration of data privacy and integrity against unidentified threats. It consists of two phases. Firstly, the chosen next-hop accomplished the generation and dispersal of secret keys over the secure channel. Secondly, it provides a lightweight securing algorithm for health data and utilizes the management of secret keys to perform iterative encryption functions. Initially, the local coordinator generates a secret key using a Lagged Fibonacci generator (LFG) [32, 33], which is the class of pseudorandom generator and operates on recurrence relation. It is a significant factor related to the security model and collaborated with the exclusive-OR $\oplus$ operator. It generates a truly random number of lengths $\boldsymbol{k}$ and can be used efficiently in a parallel manner without imposing overhead when the number of IoT sensors

is increasing. Moreover, the secret information is kept secure from the claim of authorized generation using the encryption of the private key. The local coordinator encrypts each generated secret key using a private key and proves its authenticity. LFG is utilized by the local coordinator and generated series of secret keys as defined in Equation (6).

$$\boldsymbol{K_n \equiv K_{n-i} \oplus K_{n-j}\ (mod\ m)} \quad (6)$$

where $\boldsymbol{< i < j}$ , $\boldsymbol{K_n}$ is the generated key, $\boldsymbol{K_{n-i}}$ and $\boldsymbol{K_{n-j}}$ are previous keys, $\boldsymbol{m}$ is the power of 2. The EDM-ML model performs a lightweight encryption function using $\oplus$ operation between data $\boldsymbol{D_n}$ and secret key $\boldsymbol{K_n}$. Finally, the outcome of encryption $\boldsymbol{E}$ is digitally signed using a private key of the source node $\boldsymbol{S_{pr}}$ as defined in Equation (7).

$$\boldsymbol{E: S_{pr} + (D_n \oplus K_n)} \quad (7)$$

On the opposite side, the encrypted data is decrypted first by utilizing the public key of the source node $S_{pu}$ and point out the authentication of incoming data. Secondly, it gives encrypted information using an aggregation function that performs the bitwise $\oplus$ operation as defined in Equation (7). Afterward, the encrypted data is transmitted using the paradigm of multi-hop until it reached to cloud level. During multi-hop, the encryption function $E$ is applied iteratively and securing the heath blocks of data. Also, the pair of private-public keys increases the data verification and privacy of medical data in the presence of malicious actions and established a chain of verification on each iteration. On getting the secret data, the cloud servers perform a reverse operation on each block using the secret keys and recover the health data. To maintain integrity, the EDM-ML model utilizes a lightweight pseudorandom number generator and obtained secret fields called keys that are provided as input to the encryption algorithm. They are maintained in the form of a chain such that the newly generated key $K_q$ is connected with the previous one $K_r$, which make it very difficult and offers high processing time for attacker to break its pattern as defined in Equation (8). Also, the keys are encrypted using the private information of the source node based on the RSA cryptosystem [34] to verify their authenticity on remote sites.

$$K_n: K_{n-q} \oplus K_{n-r} \quad (8)$$

Also, the health data is divided into blocks $x_i$ with the integration of the initialization vector. The encryption function is applied on each block with the integration of the $\oplus$ operation. Accordingly, the unique secrets are generated and make use of cascading hash function $h_i$ to interconnect them as given in Equation (9). The interconnected hashes increase the computational and recovery time for the attackers to compromise the data privacy and integrity. Algorithm 1illusrates the flow of the proposed model.

$$h_n: h_i \oplus h_{i+1} \quad (9)$$

**Algorithm 1**: *Efficient Data Uncertainty Management using HIIoT*

1. Procedure Uncertainty management
2. Initialization
3. Input: medical sensors, sink node, data blocks
4. Output: multi-class classifier with securing health services
5. for sensor $S_i \in G(N, \epsilon)$ do
6. optimized cost ( )
7. $min\ f(n) = \alpha\ (\frac{1}{P_c}) + \beta T r_n$
8. end for
9. for node $n_i \in$ Neighbors (N)
10. evaluate nodes metrics $d(i)$, $b_{wd}(i)$, $Ft_{PRR}(i,j)$
11. $T_n(i,j) = \sum_{n=1}^{k} F(x_n)$
12. $DT.learning\ process(next\_hop)$
13. end for
14. for interative_security do
15. $K_n: K_{n-q} \oplus K_{n-r}$
16. $E: S_{pr} + (D_n \oplus K_n)$
17. $h_n: h_i \oplus h_{i+1}$
18. end for
19. end procedure

## 4. PERFORMANCE EVALUATION

### *4.1 Sensitivity Analysis*

The weighted factors α and β support a significant role in computing the multi-objective cost function. The weighting factors are applied to identify the ratio for power consumption and trust parameters while optimizing the cost value. In the EDM-ML model, the count of α and β must be equal to 1. To accomplish sensitivity analysis, two configurations are considered to evaluate the significance of weighted factors α and β i.e EDM_ML (0.6,0.4) and EDM_ML (0.4,0.6). In Figure 3, the effects for delay metrics are depicted for α > β. Moreover, Figure 4 depicts the effect of the delivery metrics for β > α.

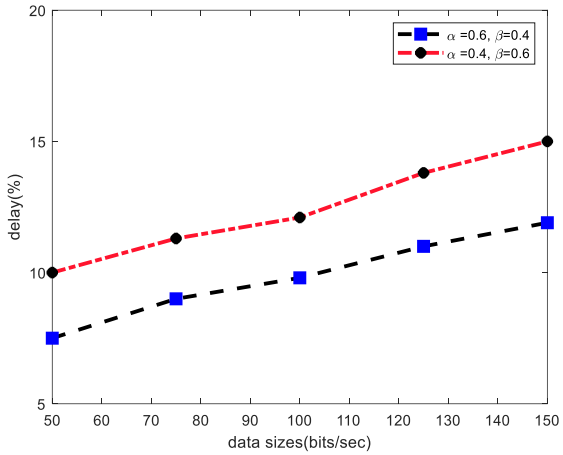



**FIGURE 3** Analysis of delay for sensitivity analysis with varying data sizes

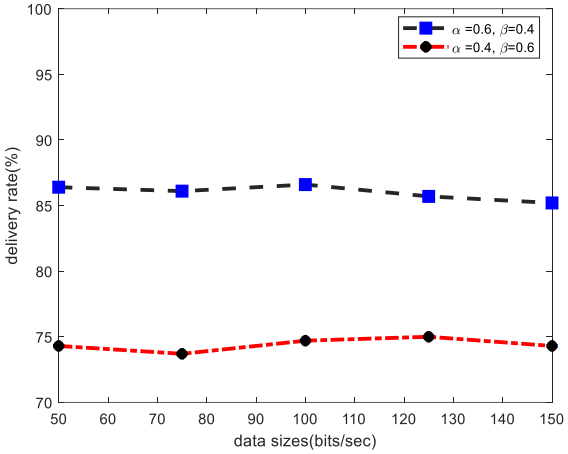



**FIGURE 4** Analysis of delivery ratio for sensitivity analysis with varying data sizes

### *4.2 Experimental Results*

The section provides the set of experiments between the proposed EDM-ML model and existing solutions. We deployed few medical sensors on the patient body to measure the health data. The packet size is fixed to 1000 bits and data is transmitted based on a constant bit rate. An IEEE-802.15.4 standard is used for media access control and the simulation is executed for 2500 sec. The transmission range of the sensors is set to 3m with an initial energy of 5j. Also, varying malicious nodes from 5 to 20 are distributed to analyze the security level of the EDM-ML model against network threats. The experiments are simulated in network simulator NS3 which is used by many researchers [35, 36]. The default parameters are listed in Table 2. The experimental analysis is done under a varying interval of rounds and malicious nodes for energy consumption, packet delivery ratio, round trip time, detection rate, and network overhead.

Table 2. Simulation parameters

| Parameters | Values |
|---|---|
| Simulation dimension | $15m^2$ |
| Channel | wireless |
| Sensors | 50 |
| Malicious nodes | 5-20 |

| | |
|---|---|
| Delivery size | 500 bits per second |
| MAC | IEEE-802.15.4 |
| Initial energy | 5j |
| Transmission power | 5(m) |
| Simulation intervals | Between 500-2500 (sec) |
| Frequency | 2.4 GHz |

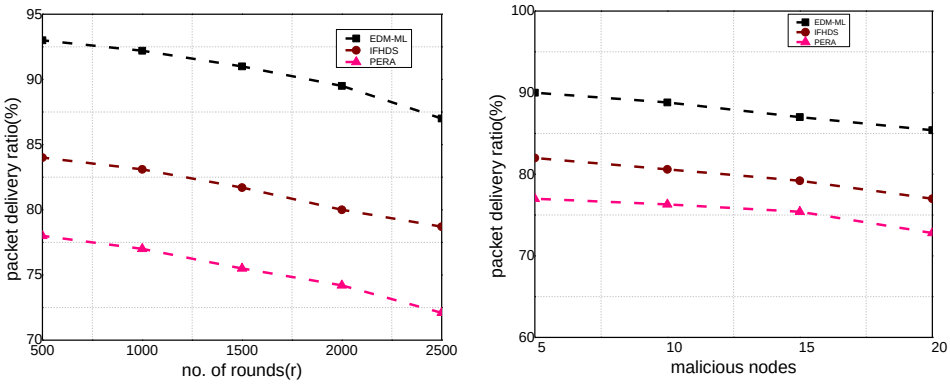
Figures 5(a) and 5(b) illustrates the performance of the EDM-ML model against the existing solution for packet delivery ratio under a varying number of rounds and malicious nodes. It is proven from the results that the EDM-ML model improves the performance by 16% and 12%. It is due to the computation of the cost function based on the multi-objective function. Furthermore, unlike most of the existing solutions that overlooked link evaluation for transmitting health data, the EDM-ML model properly analyzed the wireless channel in forwarding the sensors data towards the sink node. Moreover, the machine learning-based decision tree classifiers identified the reliable and energy-efficient data forwarders that increase the routes' stability with minor data holes and error rates. Accordingly, the EDM-ML model decreases the frequent route maintenance calls and increases the strength for reliable data delivery performance. Moreover, it uses a multi-hop paradigm for data transmission towards cloud centers and exploits multi-objective function using weighted cost. The cost function measures the performance of HIIoT from different perspectives and offers intelligent routing performance based on the node's previous behaviors. It increases the robust delivery ratio with nominal transmission power on the part of nodes

Figures 6(a) and 6(b) demonstrates the performance results in terms of energy consumption for the EDM-ML model and existing work for varying numbers of rounds and malicious nodes. It is observed that the values of the energy consumption increase with time, this is due to invalid route request packets by malicious nodes and frequency re-transmission of false packets. However, based on the results, it is seen that the EDM-ML model improves the performance of energy consumption by 21% and 14% than other solutions. It balances the data load on forwarders and classifies them using machine learning-based decision trees. Also, energy consumption with trust levels is incorporated in routing decisions, which leads to an increase in the route maintenance ratio of active routes for longer intervals. Accordingly, it decreases the breakages in the optimal routes and balances the depletion of energy resources between forwarders. Unlike existing solutions that overlooked congestion and data security factors on the active routes, the EDM-ML model has a primary focus on both factors, and therefore, it significantly increases the performance of energy efficiency. Furthermore, the communication links are securing from unknown attacks and offer trustworthy data management with the nominal rate of data re-transmissions. Such an approach decreases the consumption of energy resources and improves network stability.

Figures 7(a) and 7(b) exhibits the data detection rate of the EDM-ML model with other existing work under the varying number of rounds and malicious nodes. Based on the experimental results, it is seen that the EDM-ML model improves the rate of detection rate of malicious actions than other solutions by 15% and 14%. It is due to that the proposed model securing the health data from unauthorized operations and verify the nodes with robust and lightweight security algorithm. It deals with both data encryption and authentication features along with system integrity. The observing health data is divided into various fixed-size blocks with a random initialization vector, which is further integrated with XoR operation to offer lightweight encryption. Accordingly, data blocks are encrypted, authenticated, and verified on intermediate points until the health data is received in medical centers. Furthermore, EDM-ML model makes use of a decision tree classifier and declare the overburden transmission routes, which explicitly improves data breaches and decreases the ratio of error detection as compared to other solution. Also, it divides the medical data in the form of blocks, and on each block, a lightweight encryption function is applied to generate the fixed-sized hashes. Thus, it offers hard and more complex computing power to malicious nodes for compromising the ehealth security.

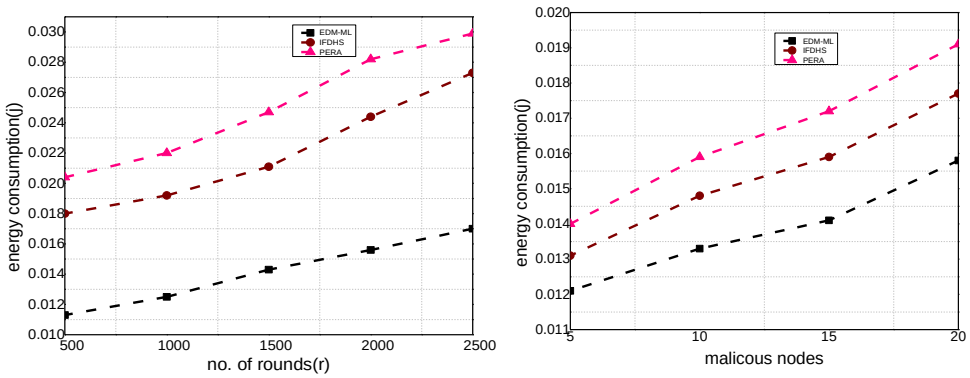
Figures 8(a) and 8(b) demonstrates the analysis of network overhead between the EDM-ML model and existing work under a varying number of rounds and malicious nodes. It is noticed from the experimental results that the EDM-ML model decreases the percentage of network overhead by 43% and 36% in the comparison of the existing solution. This is due to the that the EDM-ML model tests the performance of nodes using dynamic features and computes the weighted cost. Also, using the thresholding data decreasing the overhead in selecting the optimal routes for health data. Moreover, the EDM-ML model support low processing security algorithm by incorporating the nominal overhead on nodes level for data encryption and maintaining consistency among connected routes. Also, it balancing the transmission flow using the latest information and optimizes the performance using the decision tree. Unlike other solutions, it decreases the request packets of route maintenance and chooses more consistent forwarders without imposing overhead on the nodes.

Figures 9(a) and 9(b) show the percent of the round trip between the EDM-ML model and existing solutions time for varying number of rounds and malicious nodes. We notice that the value of round trip time is increased because due to the frequent flooding of malicious packets and uncontrolled congestion. As a result, the actual data packets have coincided with bogus packets and increases the delivery time in receiving actual data packets. However, the EDM-ML model improves the percent of the round trip time by 23% and 29% than other solutions. It happens because of balancing the load using the evaluation of network dynamics by utilizing the machine learning technique and train the forwarders to optimize the routing finding. Also, the EDM-ML model utilizes a chain of hashes to make it difficult for the malicious nodes to interrupt and delaying the actual data while transmitting on unpredictable channels. Moreover, the EDM-ML model utilizes various intermediate nodes to accomplish multi-hop routing with the computation of weighted cost function. It reducing the transmitting time among forwarders using the collected and latest nodes information and limits the HIIoT nodes for participation in routing based on multi-class decision tree classifier.



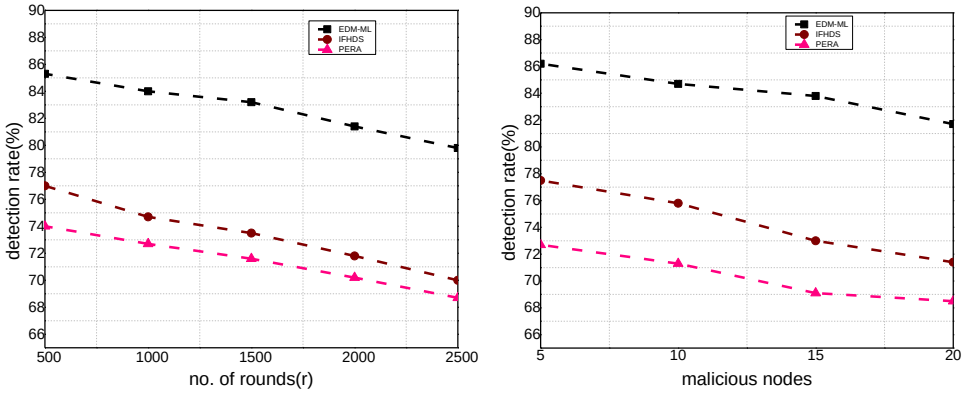

(a) (b)

Fig 5. Scenarios of: (a) analysis of packet delivery ratio under a varying number of round 500 to 2500, (b) analysis of packet delivery ratio under varying malicious nodes from 5 to 20




(a) (b)

Fig 6. Scenarios of: (a) analysis of energy consumption under a varying number of round 500 to 2500, (b) analysis of energy consumption under varying malicious nodes from 5 to 20




(a) (b)

Fig 7. Scenarios of: (a) analysis of detection rate under a varying number of round 500 to 2500, (b) analysis of detection rate under varying malicious nodes from 5 to 20

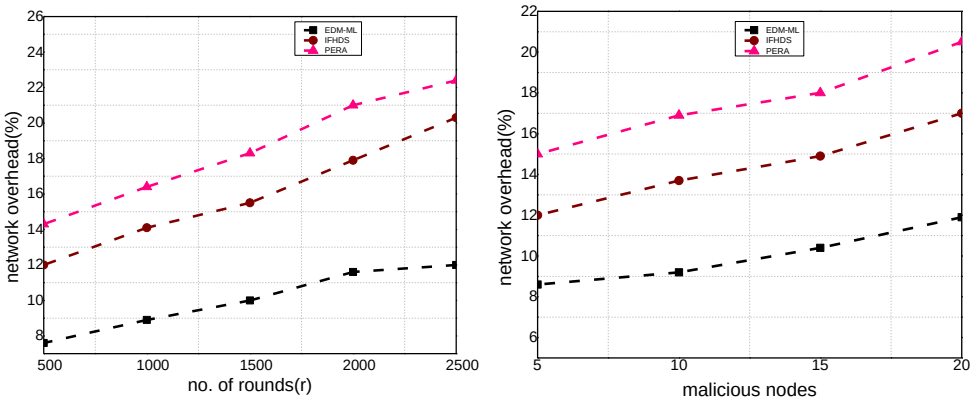



Fig 8. Scenarios of: (a) analysis of network overhead under a varying number of round 500 to 2500, (b) analysis of network overhead under varying malicious nodes from 5 to 20

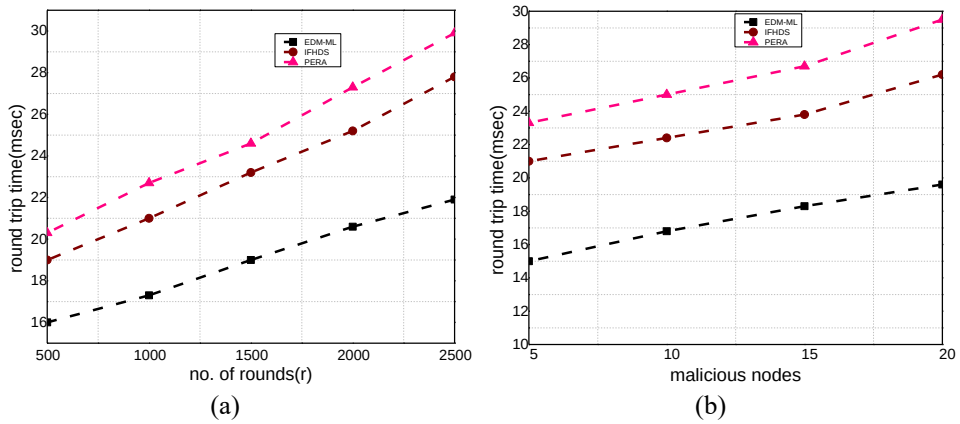



Fig 9. Scenarios of: (a) analysis of round trip time under a varying number of round 500 to 2500, (b) analysis of round trip time under varying malicious nodes from 5 to 20

## 5. CONCLUSION

This paper presents an efficient data uncertainty management model for health systems using IIoT. Its primary focus is to improve the performance of IoT-based medical systems by decreasing the complexity in data fusion and analytics. Moreover, it gives an errorless with maximum delivery with the secured real-time system in the existence of potential attacks. A multi-objective function with the optimized weighted cost is utilized to compute the distribution of various factors in a realistic environment. The proposed model makes use of a multi-class decision tree classifier and groups the nodes based on threshold features, which aims to reduce the overheads in predicting the routing decision for HIIoT network. Also, using intelligent edge devices, secret information is generated and distributed securely over the uncontrolled transmission services. The security algorithm utilizes the generated information by edge nodes and protected the health data against vulnerable attacks with the mutual validation process. It supports the trust-oriented communication system among patients and medical experts using IIoT with nominal computing overheads on involved machines. Using extensive simulation-based experiments, the EDM-ML model remarkably improved the data uncertainty using a machine learning algorithm along with confidentiality and authentication. In the future, we aim to provide a health care system using deep learning techniques and offer a trained system for further improving the EDM-ML model in terms of processing and robustness for medical services. Moreover, trusted fog-enabled architecture can be used to the trustworthy integrated system with efficient control of big data on network edges.

## REFERENCES

1. Haseeb, K., N. Islam, T. Saba, A. Rehman, and Z. Mehmood, *LSDAR: A Light-weight Structure based Data Aggregation Routing Protocol with Secure Internet of Things Integrated Next-generation Sensor Networks.* Sustainable Cities and Society, 2019: p. 101995.
2. Rahman, G.M. and K.A. Wahid, *LDAP: Lightweight Dynamic Auto-Reconfigurable Protocol in an IoT-Enabled WSN for Wide-Area Remote Monitoring.* Remote Sensing, 2020. **12**(19): p. 3131.
3. Lloret, J., L. Parra, M. Taha, and J. Tomás, *An architecture and protocol for smart continuous eHealth monitoring using 5G.* Computer Networks, 2017. **129**: p. 340-351.
4. Hossain, M.S. and G. Muhammad, *Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring.* Computer Networks, 2016. **101**: p. 192-202.

5. Kumar, A., R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, *A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes.* IEEE Access, 2020. **8**: p. 118433-118471.
6. Sagar, A.K., S. Singh, and A. Kumar, *Energy-aware WBAN for health monitoring using critical data routing (CDR).* Wireless Personal Communications, 2020: p. 1-30.
7. El Atrash, M., M.A. Abdalla, and H.M. Elhennawy, *A wearable dual-band low profile high gain low SAR antenna AMC-backed for WBAN applications.* IEEE Transactions on Antennas and Propagation, 2019. **67**(10): p. 6378-6388.
8. Hayajneh, T., K. Griggs, M. Imran, and B.J. Mohd, *Secure and efficient data delivery for fog-assisted wireless body area networks.* Peer-to-Peer Networking and Applications, 2019. **12**(5): p. 1289-1307.
9. Saba, T., K. Haseeb, I. Ahmed, and A. Rehman, *Secure and energy-efficient framework using Internet of Medical Things for e-healthcare.* Journal of Infection and Public Health, 2020. **13**(10): p. 1567-1575.
10. Lloret, J., M. Garcia, J. Tomas, and J.J. Rodrigues, *Architecture and protocol for intercloud communication.* Information Sciences, 2014. **258**: p. 434-451.
11. Michalas, A. and N. Weingarten. *Healthshare: Using attribute-based encryption for secure data sharing between multiple clouds*. in *2017 IEEE 30th International Symposium on Computer-Based Medical Systems (CBMS)*. 2017. IEEE.
12. Awotunde, J.B., A.E. Adeniyi, R.O. Ogundokun, G.J. Ajamu, and P.O. Adebayo, *MIoT-Based Big Data Analytics Architecture, Opportunities and Challenges for Enhanced Telemedicine Systems.* Enhanced Telemedicine and e-Health: Advanced IoT Enabled Soft Computing Framework, 2021: p. 199-220.
13. Sun, Y., F.P.-W. Lo, and B. Lo, *Security and privacy for the internet of medical things enabled healthcare systems: A survey.* IEEE Access, 2019. **7**: p. 183339-183355.
14. Naranjo-Hernández, D., J. Reina-Tosina, and L.M. Roa, *Special Issue "Body Sensors Networks for E-Health Applications"*. 2020, Multidisciplinary Digital Publishing Institute.
15. Huang, C., D. Liu, J. Ni, R. Lu, and X. Shen, *Achieving Accountable and Efficient Data Sharing in Industrial Internet of Things.* IEEE Transactions on Industrial Informatics, 2020. **17**(2): p. 1416-1427.
16. Srivastava, A., S. Gupta, M. Quamara, P. Chaudhary, and V.J. Aski, *Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects.* International Journal of Communication Systems, 2020. **33**(12): p. e4443.
17. Yang, Q., Y. Liu, T. Chen, and Y. Tong, *Federated machine learning: Concept and applications.* ACM Transactions on Intelligent Systems and Technology (TIST), 2019. **10**(2): p. 1-19.
18. Singh, J., A. Gimekar, and S. Venkatesan, *An efficient lightweight authentication scheme for human-centered industrial Internet of Things.* International Journal of Communication Systems, 2019: p. e4189.
19. Zeadally, S. and M. Tsikerdekis, *Securing Internet of Things (IoT) with machine learning.* International Journal of Communication Systems, 2020. **33**(1): p. e4169.
20. Ali, R., Y.A. Qadri, Y. Bin Zikria, T. Umer, B.-S. Kim, and S.W. Kim, *Q-learning-enabled channel access in next-generation dense wireless networks for IoT-based eHealth systems.* EURASIP Journal on Wireless Communications and Networking, 2019. **2019**(1): p. 178.
21. Deebak, B.D. and F. Al-Turjman, *Secure-user sign-in authentication for IoT-based eHealth systems.* Complex & Intelligent Systems, 2021.
22. Rajendra Prasad, C. and P. Bojja, *A non-linear mathematical model-based routing protocol for WBAN-based health-care systems.* International Journal of Pervasive Computing and Communications, 2021.
23. Ahmed, G., Z. Jianhua, and M.M.S. Fareed, *PERA: priority-based energy-efficient routing algorithm for WBANs.* Wireless Personal Communications, 2017. **96**(3): p. 4737-4753.
24. Al-Hubaishi, M., C. Çeken, and A. Al-Shaikhli, *A novel energy-aware routing mechanism for SDN-enabled WSAN.* International Journal of Communication Systems, 2019. **32**(17): p. e3724.
25. Essa, Y.M., E.E.-D. Hemdan, A. El-Mahalawy, G. Attiya, and A. El-Sayed, *IFHDS: Intelligent Framework for Securing Healthcare BigData.* Journal of Medical Systems, 2019. **43**(5): p. 124.
26. Fabian, B., T. Ermakova, and P. Junghanns, *Collaborative and secure sharing of healthcare data in multi-clouds.* Information Systems, 2015. **48**: p. 132-150.
27. Tang, W., J. Ren, K. Deng, and Y. Zhang, *Secure data aggregation of lightweight e-healthcare iot devices with fair incentives.* IEEE Internet of Things Journal, 2019. **6**(5): p. 8714-8726.
28. Lloret, J., S. Sendra, J.M. Jimenez, and L. Parra, *Providing security and fault tolerance in P2P connections between clouds for mHealth services.* Peer-to-Peer Networking and Applications, 2016. **9**(5): p. 876-893.
29. Viswanath, G. and P.V. Krishna, *Hybrid encryption framework for securing big data storage in multi-cloud environment.* Evolutionary Intelligence, 2020: p. 1-8.
30. Ahmed, I., H. Karvonen, T. Kumpuniemi, and M. Katz, *Wireless communications for the hospital of the future: requirements, challenges and solutions.* International Journal of Wireless Information Networks, 2020. **27**(1): p. 4-17.
31. Sarkar, B.K., *Big data for secure healthcare system: a conceptual design.* Complex & Intelligent Systems, 2017. **3**(2): p. 133-151.
32. Coddington, P.D., *Random number generators for parallel computers.* 1997.
33. James, F., *A review of pseudorandom number generators.* Computer physics communications, 1990. **60**(3): p. 329-344.
34. Rivest, R.L., A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM, 1978. **21**(2): p. 120-126.
35. Alex, S., D.P. Pattathil, and D.K. Jagalchandran, *SPCOR: a secure and privacy-preserving protocol for mobile-healthcare emergency to reap computing opportunities at remote and nearby.* IET Information Security, 2020. **14**(6): p. 670-682.
36. Deebak, B.D., F. Al-Turjman, M. Aloqaily, and O. Alfandi, *An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT.* IEEE Access, 2019. **7**: p. 135632-135649.