Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5665408, 12 pages
https://doi.org/10.1155/2022/5665408

Research Article

Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications

Eshrag Refaee,[1] **Shabana Parveen**,[2] **Khan Mohamed Jarina Begum**,[1] **Fatima Parveen**,[3] **M. Chithik Raja**,[4] **Shashi Kant Gupta**,[5] **and Santhosh Krishnan**[6]

[1]*Information Technology & Security, College of Computer Science and Information Technology, Jazan University, Saudi Arabia*
[2]*Computer Science, Jazan University, Jazan, Saudi Arabia*
[3]*Tech Mahindra, India*
[4]*Information Technology, University of Technology and Applied Sciences-Salalah, Salalah, Oman*
[5]*Computer Science and Engineering, Integral University, Lucknow, India*
[6]*Department of Mechatronics Engineering, Wollo University, Kombolcha Institute of Technology, Kombolcha, Ethiopia Post Box No: 208*

Correspondence should be addressed to Santhosh Krishnan; santhosh@kiot.edu.et

Received 13 April 2022; Accepted 26 May 2022; Published 6 June 2022

Academic Editor: Kuruva Lakshmanna

The Internet of Things (IoT) has impacted various aspects of life, but its profound effects on the health sector are particularly striking because of its cutting-edge nature. Mobile computing characteristics enable IoT to play a more important role when used with mobile computing. A significant part of the benefits of IoT in healthcare can be attributed to mobile health, which is greatly enhanced by mobile computing. Wearables transmit large amounts of data to IoT devices through sensors, actuators, and transceivers. Threats, attacks, and vulnerabilities abound for data on the Internet of Things. Therefore, addressing IoT-related security, privacy, and vulnerability issues call for a robust security solution. This paper proposes a secure and scalable healthcare data transmission framework in IoT based on an optimized routing protocol. Initially, the health data is collected from various IoT devices like wearable devices and sensors. The raw data is preprocessed via data cleaning and data reduction techniques. K-nearest neighbor (KNN) imputation is performed and principal component analysis (PCA) is employed for dimension reduction of the data. Utilizing modified local binary patterns (MLBP), the features are extracted from the preprocessed data. By combining the fuzzy dynamic trust-based RPL algorithm with the butter ant optimization (BAO) algorithm for low-power and lossy networks, the proposed fuzzy dynamic trust-based RPL (FDT-RPL) protocol improves the overall security of data transmission. The algorithm has been implemented for a smart healthcare system, and the performance is analyzed by comparing it with traditional approaches. The proposed routing protocol provided a secure and scalable healthcare data transmission.

1. Introduction

Currently, mobile edge computing (MEC) and the Internet of Things (IoT) face several challenges in meeting the demands of the future. The development of technology is focused on reducing the amount of data that must be transmitted and the amount of network traffic that must be handled. Wireless sensor networks (WSNs) are one of the most significant sources of big data in the IoT. In smart cyberphysical systems (SCPS), wireless sensor networks are used for many different applications [1]. As wireless sensor technologies continue to evolve, we are witnessing the dawn of a new age of pervasive and intelligent Internet of Things (IoT) applications. Numerous breakthroughs have been made possible by the Internet of Things, allowing it to provide connectivity to devices everywhere, all the time. Many IoT

applications rely on a sensor node to send data to a base station, where it is used for various purposes. WSNs' data transfer, scalability, and energy efficiency may all be improved through the use of efficient routing protocols. IoT communication protocols have many challenges due to instability in low-power wireless connections and restricted resources that often do not match quality of service standards [2].

Healthcare applications increasingly use wearable devices and ambient sensors. Considering that each application is unique, routing protocols should be determined according to their outline. The patient's body and surroundings are filled with wireless sensor nodes that need a specialized routing protocol to safely and effectively transfer all of the necessary data to and from each node [3]. The low-power and lossy networks (LLN) are a class of networks characterized by high loss rates, low data rates, and unstable communication links due to the associated devices' resource constraints (i.e., limited power, memory, and computation). There are point-to-point, multipoint, and point-to-multipoint patterns in which LLN-based IoT devices can be used. Such traffic patterns, however, cannot be dealt with adequately by current routing methods on the market. Consequently, the RPL routing protocol, an IPv6 network protocol that is proactive and lightweight, is the best answer for these situations [4]. Figure 1 shows the IoT healthcare architecture.

With the proliferation of wireless sensor networks, low-end gadgets with limited resources can now connect to the Internet and provide potentially life-changing services. RPL and RPL-based protocols have never been investigated in the context of IoT, though their significance as IoT routing algorithms is acknowledged here [5].

Hence, in this article, we have proposed a secured and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications. When it comes to IoT for mobile computing, the proposed method was aimed at meeting multiple goals including a low latency and energy usage in the IoT while still providing maximum security, throughput, and data rate. The further portion of the paper is structured as shown: Section 2 provides the associated literature and the problem statement. The flow of the proposed work is explained in Section 3. Section 4 examines and compares the proposed method's behavior to that of traditional approaches. Finally, Section 5 brings the paper's overarching theme to a close.

2. Related Work

In Qu et al., a basic overview of wireless body area networks (WBAN) is provided, which then moves on to analyze and evaluate various routing protocols to determine their relative merits and drawbacks [6]. Finally, they have outlined several issues and suggestions that can be used to guide the design of future routing systems. Studying energy-efficient WBAN routing strategies in medical systems may gain from this research.

In Patel and Jinwala, an RPL protocol that incorporates a reputation-based technique to protect against selective forwarding attacks has been proposed [7]. An IoT node's reputation is determined by looking at how it forwards data. For an IoT node, its data transmission performance is evaluated by comparing observed real packet loss with an expected normal loss.

In Marietta and Chandra Mohan, it is stated that to satisfy the demands of the Internet of Things, current routing protocols must address many significant research questions. Router protocols are examined in terms of their design, as well as their classifications [8]. Dynamic topology, scalability, mobility of nodes, and restricted bandwidth are among the most pressing issues in the IoT. The objective of the current protocol evaluation is to determine the shortest path and the minimum amount of data required to be sent.

Specifically, a secure routing protocol for low-power and lossy network (RPL) routing protocols is explored as well as future research directions in [9]. For IoT applications, they are focusing mostly on rank and version number assaults. As a result of the literature review, the authors suggest that a new, secure RPL protocol will also help to address the security challenges associated with IoT applications for smart cities. (1) They do not address numerous attacks and particularly rank-based attacks and version numbers simultaneously in RPL-based IoT for smart urban. (2) They do not enable both detection and prevention for both attacks. (3) Several of them provide just one form of network architecture for evaluating the efficacy of their solution, although assaults might be impacted by the forms of network architecture. On the whole, they all have inferior system performance and prediction accuracy. Smart cities require the RPL nodes to be mobile so that their rank and topology can change dynamically.

In Pujianto et al., the authors proposed a butter ant optimization technique to evaluate imputation methods for handling missing data. KNN imputation can achieve the same level of accuracy as complete information in each scenario, with just a little variation in accuracy [10]. Additionally, the proposed system has improved mobility uniformity for several frames of expression copying while also maintaining reduced servo displacement variances for single frame instant similarities.

A technique for predicting and imputing missing data in IoT gateways is proposed by França et al. to attain greater autonomy at the edge of the network. It is not uncommon for these gateways to have minimal computational power. It is therefore important to have simple and effective imputation procedures for missing data. As a result, two neural network-based regression models are presented here to fill in data gaps in IoT gateways [11]. Isolated losses were studied in this study by inserting missing data using a uniform distribution. There may be alternative ways to insert missing data as possible.

In Wu et al., the authors proposed a distributed principal component analysis (PCA) for performing PCA on a variety of datasets, as well as their performance and their applicability in the context of distributed data collection systems. The conceptual and empirical analyses provide that these strategies can fully exploit the computational and storage capabilities of the dispersed agents [12].

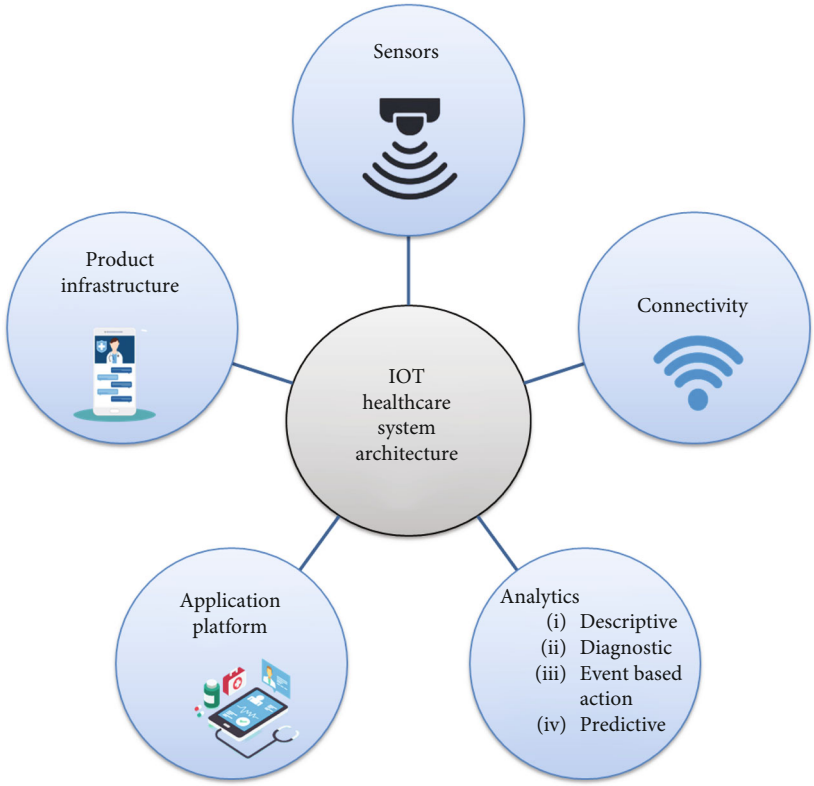

Figure 1: IoT healthcare architecture.

According to the complexity of mobile apps and the environment in which they run, the research by Manukumar and Muthuswamy provides unique multiobjective effective offloading decision frameworks for enabling this practice. Mobile devices that do heavy computational tasks that require a lot of battery power and CPU utilization are the primary focus here [13]. When it comes to mobile cloud computing, they want to expand the MoEOD framework. In addition, they want to reduce the amount of energy needed to offload the job by considering multiple users and the movement of the phone user via edge devices.

IoT health devices' privacy and security are also provided through mobile computing, a topic that is discussed in Nazir et al., as well as how mobile computing has an impact on IoT in healthcare. The authors conducted a comprehensive literature review to determine if mobile computing and IoT have any positive effects on healthcare settings and smart hospitals [14]. IoT-based healthcare systems involve heterogeneous gadgets; thus, building a topological arrangement, safety framework for multidevices, multiprotocol network, and cryptographic algorithms to suit the needs of all in the IoT-based medical organization may be a problem.

In Somula et al., the authors proposed a novel cloudlet model to handle healthcare applications that can reduce processing time while still maintaining enough security for the user's data. An initial connection is established with an available local cloudlet; if the cloudlet is unable to supply the required resources or services, a remote cloud will be accessed instead [15].

A comprehensive literature review is used to identify the security difficulties and challenges of IoT devices. When these issues are taken into consideration, mobile computing has been employed to offer possible answers. Mobile computing has developed hardware and software solutions to the IoT security concern [16].

In Jegadeesan et al. for smart city applications, the authors have developed an effective mutual authentication technique that is anonymous and secure. An investigation of the security and performance of the proposed anonymously mutual authentication methodology demonstrates that the proposed technique is more secure than current schemes and that the suggested method is more efficient than current methods [17]. This scheme does not guarantee confidentiality, but it is viewed as a potential future project for safeguarding the transmission of communication signals. A key management mechanism will also be developed in the future to ensure secure communication between numerous groups of users.

In Peng et al., the authors reviewed mobile cloud computing (MCC) from the standpoints of service uptake and provision is presented. To begin, they went over the basics of MCC, such as what it is and how it works. Offloading is then reviewed as an example of an existing mobile user (MU) service acceptance by MCC [18].

In Muheidat and Tawalbeh, some of the problems, concerns, and challenges related to mobile devices, cloud computing, and big data cyber security were addressed [19]. Although cloud applications keep offering enormous data security solutions, key issues limit their expansion and use.

Cloud data maintaining the security require more strong solutions and practice guidelines in research consideration.

As a result of Lin et al., the authors lay the foundation for a better service system, taking privacy, security, and resilience into account. Based on the case study of mobile healthcare applications, the proposed concepts are proven to be effective [20]. The current study has a few drawbacks. For starters, it may be lacking in the literature. Future works on data protection and resilience development will be reviewed using a systematic evaluation process that has proven useful in the literature. Another requirement is confirmation that the design concepts are effective.

In Politou et al., the authors suggested that several privacy concerns arise from mobile computing and sensing applications, particularly from big data algorithm processing that deduces sensitive personal facts, such as social behavior or emotional state, from this data [21].

In Gezahagn et al., several common healthcare uses and pertinent issues and solutions are discussed. The authors presented and explained an integrated wireless structure design that takes advantage of existing and developing wireless networks, as well as mobile networks, to provide location control and patient monitoring, intelligent disaster response systems, and mobile medical applications [22].

A study on the IoT routing protocols is presented in Zrelli. An overview of both hardware platforms and software platforms for the IoT is presented here. According to researchers, a routing protocol for low-power and lossy networks (RPL) is energy-efficient when it comes to IoT applications [23]. Whenever the amount of sensor nodes deployed in an IoT system increases, they experience a rise in energy usage. Relative to other measures, the energy usage should be lower when using the routing indicator "energy."

In Kareem and Tayeb, research trends, limitations, and possibilities will be identified and discussed, as it compares and evaluates various mitigation methods and strategies. Consequently, current research is compared concerning the experimental environment, attack focus, attack method, and performance metrics applicable to attacks on lossy networks and low-power networks [24].

2.1. Problem Statement. Recent interest in the Internet of Things had grown among academics, governments, and technologists from a wide range of fields. Security, scalability, and big data analytics are just a few of the pressing concerns in the Internet of Things. The characteristics of IoT networks vary greatly in terms of network size, traffic patterns, and mobility. A variety of factors, including traffic conditions, energy consumption, scalability, portability, bidirectionality, and transmitter range, must be taken into account when determining the need for a routing protocol in a given scenario. As a result of the unique characteristics of IoT devices, new routing protocols have been developed.

3. Proposed Work

A healthcare system developed for remotely patient data diagnosis and analysis must enable safe and continuous data flow. Because of these benefits and because it reduces patient and doctor visits, it is becoming increasingly popular. Real-time data, such as audio and video calls, should also be available in case the doctor wants to talk to or get more information about an individual patient. Using the web portal, patients should be able to access their personal health information and follow their doctor's orders no matter where they are. The remote center, doctors, and online portal all benefit from secure data transfer. Smart mobile phones, rather than computers or other devices, are the primary means through which Internet access is available in India. In addition, computers and other computing equipment may not always have the right power source, but smartphones are much more efficient because of their smaller power consumption and simplicity of use. To link the portable unit to a mobile device via Bluetooth, the systems must have the ability to connect. One of the most essential features of offline data aggregation is that it ensures that data is collected in remote areas where there are no networks. The system should be able to withstand the elements, be portable, and be simple to operate.

In this part, we describe the flow of the suggested methodology. Presented here is a schematic representation of the suggested technique, which involves analyzing the dataset for IoT sensors, preprocessing the data with data cleaning and data reduction, feature extraction with fuzzy dynamic trust-based RPL routing protocol, and a butter ant optimization algorithm based on secure and scalable healthcare data transmission in IoT for mobile computing applications. A schematic representation of the proposed technique is shown in Figure 2.

3.1. Data Collection. The M-HEALTH dataset comprises recordings of 10 participants' vital signs and body movements while they do various physical tasks. Ankle, wrist, and chest sensors are employed to monitor the subject's trained movements. Walking, running, jogging, cycling, jogging, and jumping forward and backward are among the twelve options: standing still, resting in a chair, or laying down. Other options include sitting or lying down. mHealthDroid's potential has been demonstrated through the development of an example application. The mHealth Framework's core features and components have been incorporated into this application.

3.2. Preprocessing. Network traffic is transformed into a sequence of observations, with each data expressed as a feature vector, through preprocessing. The class of observation, like "ordinary" or "unusual," is an optional term. It is possible to use such feature vectors as feed toward machine learning techniques.

3.2.1. Data Cleaning. The primary objective of this stage is to analyze data and learn about its various characteristics. Identifying mistakes, missing values, and corrupted records is part of this stage. The accuracy of a machine learning (ML) model can be severely impacted by training it on data that contains missing values. Data mistakes should be adequately addressed to provide a trustworthy dataset, which will improve the quality of training data and allows for

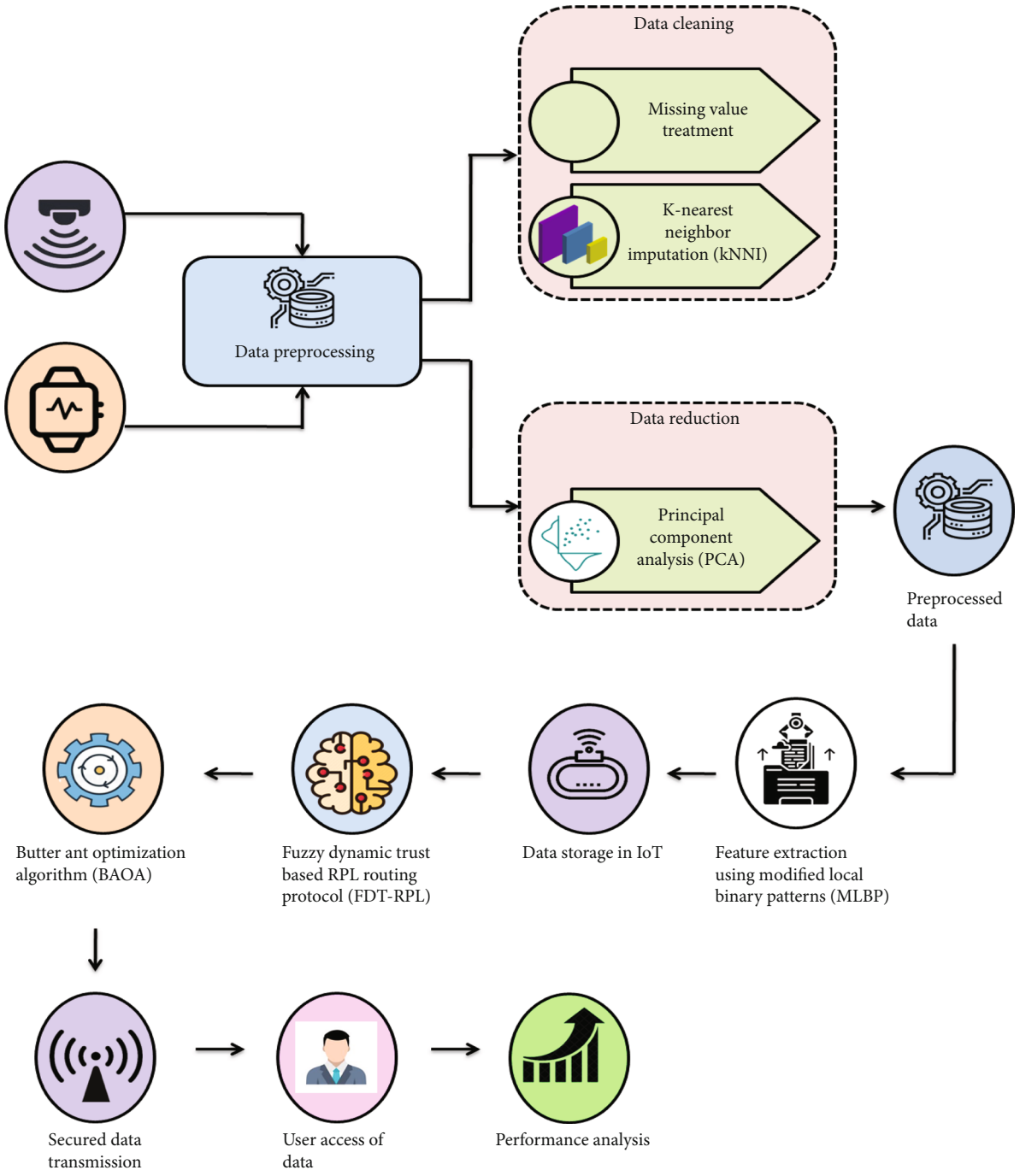

Figure 2: Schematic representation of the proposed work.

accurate decision-making to be carried out. Missing data were replaced by a method that calculates the mean/median of nonmissing values and substitutes them for those that are missing.

The K-nearest neighbor approach is a basic yet efficient machine learning algorithm for classifying and recognizing patterns. In the training tuples, each attribute has N values. In an N-dimensional feature space, each tuple is represented by a single point. Analogy helps the algorithm learn to categorize. It is possible to create patterns by grouping like-tuples into a single cluster. In the pattern space, the technique finds the K-nearest neighbor training tuples closest to an unknown tuple.

Low-quality data in the initial training sets may not be identified as KNNs or may even be hazardous when picked. This means that KNNs must not be selected solely based on a single training sample's ability to classify KNNs. Cleaning away low-quality training data is also a good idea if KNN algorithms are going to be used on huge training data in the real world. Finally, we modify the original data without duplicate or repetitive data and incomplete data. Then, this modified data or cleaned data is further processed for

lessening the maximum quantity of the cleaned data into minimal quantity through applying the PCA technique in the data reduction stage.

3.2.2. Data Reduction. When dealing with high-dimensional data, the employment of data reduction methods is necessary since many dimensions are unnecessary and can obscure existent clusters in noisy data, as well as because the increased complexity of processing might jeopardize real-time requirements. The model makes use of principal component analysis (PCA). As a data reduction technique, PCA may be used to construct a subset of new data by projecting existing characteristics onto new data.

It might be tough to discover all the connections between attributes during data analysis. Principle comparative analysis (PCA) is a powerful tool for discovering hidden associations, enhancing data visualization, detecting outliers, and classifying within the newly specified dimensions. When unsupervised learning is required on a dataset, PCA may be big assistance since it will help to efficiently initialize centroids for clustering.

As a prerequisite for the best performance of several machine learning techniques, we first normalise the datasets onto a unit scale (mean = 0 and variance = 1) in order to optimize the PCA result.

$$y = SE(z). \tag{1}$$

We proceed as follows:

(i) Organize our dataset

With Y having a set of m vectors $(y_1, y_2, \cdots, y_m) \cdots n$, each x_i element is an instance of our dataset, z_i is the value of one element, and $\bar{x}$ is the mean value of all elements.

(ii) Find the mean using the equation

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n}. \tag{2}$$

(iii) Calculate variance

$$S^2 = \frac{\sum_{i=1}^{n} (z_i - \bar{x})^2}{(n-1)}. \tag{3}$$

(iv) Calculate covariance

$$X^{n\times n} = \left(z_{j,i}, y_{j,i} = \operatorname{cov}\left(\mathrm{Dim}_i, \mathrm{Dim}_j\right)\right), \tag{4}$$

where $X^{n\times n}$ is our data matrix with n rows and n columns and Dim_j is the jth dimension.

(v) Calculate eigenvalues and eigenvectors

The eigenvalues and eigenvectors of the covariance form the basis of a PCA. It is the eigenvectors and eigenvalues that will determine the new feature space's direction and magnitude.

If C is an $n \times n$ matrix and if B is a scalar multiple of y, that is,

$$CX = \lambda x \tag{5}$$

for some scalar λ. Equivalently, the value is known as A's eigenvector, which corresponds to A's eigenvalue. Since the nonzero vectors that meet the equation are the eigenvectors that correspond to an eigenvalue of a matrix B,

$$(\lambda J - C)x = 0. \tag{6}$$

G is the set of all vector z that meet our eigenspace equation.

$$G = \{z : (C - \lambda J)z\} = 0. \tag{7}$$

(vi) The next step is to sort the eigenvectors according to their eigenvalues, from highest to lowest. A decent approximation of the original data can be achieved by removing the less important components from the dataset. In the following stage of our algorithm design, we will feed the reduced data into feature extraction phase for retrieving the significant texture features

3.2.3. Feature Extraction Using Modified Local Binary Patterns. Since its processing technique takes the grey value as the starting point and arbitrarily selects one pixel as the center point to set the threshold, LBP is also known as a local binary mode. If the pixel value is greater or equal to the threshold, it will be marked as 1; if it is less than the threshold, it will be marked as 0. It is a binary description of an image's grey value performed by an operator.

According to the basic idea of MLBP grey pixel binarization interpolation, we can write the P function as

$$P = p(h_d, h_0, -h_d, h_1 - h_d, \cdots, h_{t-1} - h_d). \tag{8}$$

Assume that the variables $(h_t - h_d)$ and h_d are independent of each other; then, the above formula can be rewritten as

$$p \approx p(h_d, h_0, -h_d, h_1 - h_d, \cdots, h_{t-1} - h_d), \tag{9}$$

$$P \approx p(r(h_0 - h_d), r(h_1 - h_d), \cdots, r(h_{t-1} - h_d). \tag{10}$$

Any local differential transform may be eliminated as a result of the MLBP operator's linear invariant property for grey values in any local differential transform. That is to say, as long as the image's grey values remain in the same

sequence, the output of MLBP remains constant under uniform illumination.

Formally, given a pixel at (y_d, z_d), the resulting MLBP can be expressed in decimal form as follows:

$$\mathrm{MLBP}_{Q,S}(y_d, z_d) = \sum_{Q=0}^{Q-1} t\left(j_Q - j_d\right)2^Q, \tag{11}$$

wherej_d,$j_Q$are used, respectively, values of the center pixel's greyscale;Ppixels are encircling pixels in a sphere with a sphere radius of$R$, and the function$t(y)$has the following definition:

$$t(y) = \begin{cases} 1, \text{if } y \geq 0, \\ 0, \text{if } y < 0. \end{cases} \tag{12}$$

Invariant to monotonic greyscale modifications that retain the local neighborhood pixel intensity order, the fundamental MLBP operator is defined above. We can use a texture description based on the histogram of MLBP labels generated across a certain area. Mobile computing makes use of IoT large data storage technologies, which are examined in this relevant article. Lastly, MLBP was performed for extracting texture characteristics from the volume-reduced data. Followed by, this extracted data are kept into the IoT to transmit the data across IoT nodes through the proposed routing protocol with reduced energy usage and delay.

3.2.4. Fuzzy Dynamic Trust-Based RPL Routing Protocol

(1) Model of IoT Dynamic Fuzzy Trust. Uncertainty was already incorporated into trust choices using fuzzy logic. The trust is calculated using a fuzzy multistep component. Fuzzy logic is employed in the first stage to estimate trust on an individual basis for every trust dimension. The maximum degree of trust is determined using fuzzy logic in the next stage. The complete, dynamical, and fuzzy logic-based concept is incorporated into RPL, and also, an enhanced OF is given in the suggested technique. A multilevel fuzzy model for assessing the trustworthiness of IoT objects is the FDTM-IoT. An FDTM-IoT initial fuzzy stage uses three dimensions to determine trustworthiness. QoS, quality of P2P communication (QPC), and contextual information are all taken into account. The model is dynamic and complete because of the careful consideration of dimensions and assessment techniques. The FDTM-IoT project has been structured hierarchically. Thus, each dimension has its subdimensions, as seen below. A dynamic model may be created using this framework. Other dimensions and subdimensions can easily be added or removed from this dynamic model. Fuzzy inference systems are proposed for each dimension separately. In the second stage of fuzzy inference, the fuzzy inference system is fed into the final fuzzy system in all dimensions. As a result of this inference process, a final degree of confidence may be calculated.

(2) FDT-IoT-Based RPL (FDT-RPL). The FDT-RPL is made up of four basic processes; FDT-RPL ensures safe interoperability. IoT devices may rely on this collaborative approach to supply them with safe and reliable routing information. The FDT-RPL procedure is detailed in-depth in the following sections.

A fuzzy trust model called FDT-RPL can determine trust between entities in a low-power, lossy network using fuzzy logic. There are two phases to FDT-RPL. First, three dimensions are taken into account. Contextual information, QoS, and QPC all play a role. There is a fuzzy system for each of the four dimensions. In the second phase of the fuzzy system, the results of the first stage's fuzzy stage are employed as inputs. The second fuzzy phase determines the final level of trust between A and B. FDT-RPL is a dynamic and complete model because it considers dimensions and calculation techniques. The ability to get dynamic and ongoing advice also aids in the modeling of dynamism. The ability to adapt one's behavior to the current environment depends on considering both direct and indirect information. The model's applicability is aided by the use of contextual information (CI), and linkage stability and item mobility are a few examples. As an example, the fuzzy location region may be expressed by the radius t_{18}.

$$t_{18} = u_{18} * w_{\max}. \tag{13}$$

The fuzzifier is a frequent component in fuzzy inference systems that evaluate the degree of membership of fuzzy sets. A membership function can be used to compute each fuzzy set in the fuzzifier. Because of this, a fuzzy set with three separate membership functions were designed.

$$f_\mu(y) = \frac{1}{\sqrt{2\pi\sigma}} g^{-\left((y-\mu)^2/2\sigma^2\right)}, \tag{14}$$

$$\begin{cases} f_{\text{low}}(y) = \dfrac{1}{\sqrt{2\pi} \times 0.3} g^{-\left((y-0.2)^2/\left(2\times(0.3)^2\right)\right)}, \\ f_{\text{medium}}(y) = \dfrac{1}{\sqrt{2\pi} \times 0.3} g^{-\left((y-0.5)^2/\left(2\times(0.3)^2\right)\right)}, \\ f_{\text{high}}(y) = \dfrac{1}{\sqrt{2\pi} \times 0.3} g^{-\left((y-0.8)^2/\left(2\times(0.3)^2\right)\right)}. \end{cases} \tag{15}$$

Every node in the RPL topology connects with its neighbors and transmits data at a power level that corresponds to its communication range. Therefore, the communication range is*e*.

$$E_i^{mt} = l * \left(E_{\text{elec}} + E_{\text{amp}} * e^2\right), \tag{16}$$

$$E_i^{mr} = l * E_{\text{elec}}. \tag{17}$$

The RPL protocol can be improved by using trust-based RPL routing protocols. The RPL protocol's security is enhanced during routing choices by a variety of trust metrics that have been created and included in the protocol. RPL trust-based routing protocols, along with the threats they

1. Initiate the population size of butter-ants (p), mode of perception (m) Power exponent (e) and probability switch (s).
2. Set r =0
3. for (J=1:J<=m) do
4. Create a small beginning colony of butter-ants
5. Determine all butter-ants' fitness levels.
6. Apply the equation to determine the butter-ant's fragrance (21).
7. Decide which butter-ant will provide the greatest overall solution (h^*)
8. end for
9. Despite not meeting, the stopping criteria (r<n) do
10. Set r=r+1.
11. for (J=1:J<=m) do
12. Create a random number d, dϵ(0,1
13. if (t<s) then,
14. Ensure that butter-ant is at its best (h^*) as in equation (22).
15. Otherwise
16. As in equation (23), move butter-ant randomly
17. When end-if
18. Each butter-ant is evaluated based on its fitness function
19. end for
20. Select the best solution for the overall situation (h^*)
21. Calculate the value of sensory modality according to equation (24).
22. end
23. Create the best possible solution (h^*)

Algorithm 1: BAO algorithm pseudocode.

address, the trust-based strategy they utilize, the flaws they have, and the validation mechanism they use. By far, the most extensively used routing protocol is the routing protocols for low-power and lossy network. To avoid network loops, RPL utilizes a distance vectors routing protocol (dvrp). Point-to-point traffic is not supported by RPL, even if it performs well in P2MP and MPP communication modes. Using the appropriate routing metrics, RPL may be customized to fit any application. Due to a lack of fine-tuning of RPL's general features, many applications may experience poor performance. To optimize the proposed FDT-RPL's performance, the BAO algorithm is utilized.

3.2.5. Butter Ant Optimization Algorithm. Each BAO algorithm is a search agent whose fitness changes depending on the butter ant. To further aid in the optimization process, each butter ant contributes to the process by emitting its unique scent based on the intensity of its fitness. Butterflies may communicate with each other by releasing a scent that is detected by the surrounding surroundings. Because it can detect the scent of other butter ant optimizations (global search), a butter ant optimization goes in the direction of other optimizations (local search). However, if one butter ant optimization has a stronger scent than the rest, it will draw attention to itself. As a result, each butter ant goes randomly toward the most fragrant butter ant. The geography of the goal function affects or determines the stimulus intensity of a butter ant optimization. There are three key steps to the BAO algorithm: start-up, iteration, and finalization. Each time BAO algorithm starts up, the start-up procedure is carried out as usual. The search is iterated until the best answer is identified, and then, the process is ended. The objective

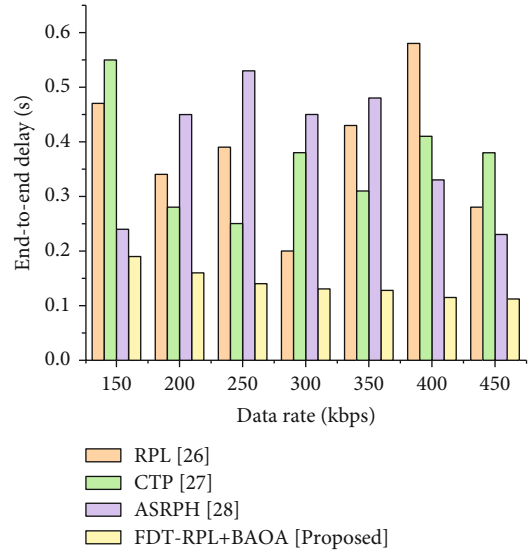

Figure 3: End-to-end delay results of the proposed methodology.

function and solution space are established at this step of algorithmic development.

The variables used in BAO algorithm have been allocated their values. Butter ant populations are created in the algorithm once the values have been established. During the BAO algorithm simulations, a certain amount of memory is provided to hold the information of all butter ants. Butter ant's scent and fitness values are computed and saved, and their placements are produced at random in the search space. When this step is complete, the algorithm moves on to iteration, which uses the newly produced fake butter ant

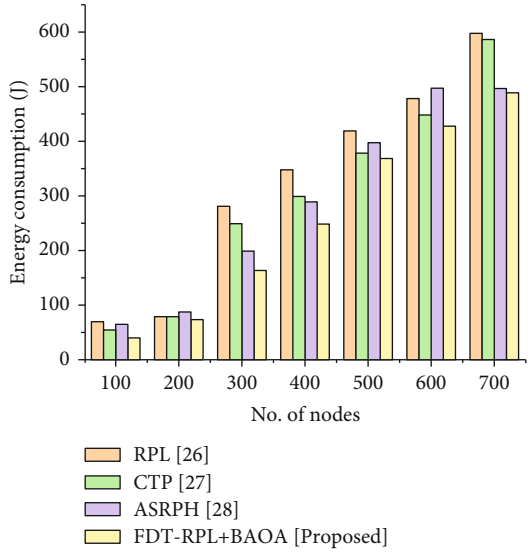

Figure 4: Energy consumption (J) results of the proposed methodology.

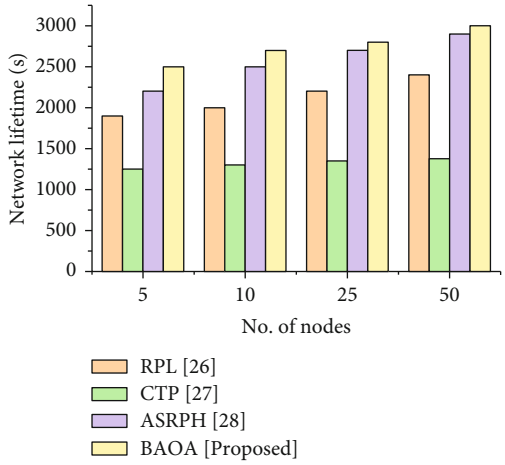

Figure 5: Network lifetime results of the proposed methodology.

to search. The fitness values of all butter ants are computed and assessed in all iterations of a second phase of the BAO algorithm. After that, the butterflies use the following equation to produce scent:

$$e = dJ^b. \tag{18}$$

When the value of ant is 0, no other butter ant can smell the aroma that a single butter ant is releasing. It is therefore possible to influence the BAO algorithm's behavior by manipulating its power exponent value. The convergence rate of the algorithm is heavily influenced by these two variables, as well as the sensory modality value. In the BAO algorithm, the value of the sensory modality (t) is adjusted as follows:

$$d(p) = \left[d(p-1) + \frac{0.025}{d(p-1) * P}\right]. \tag{19}$$

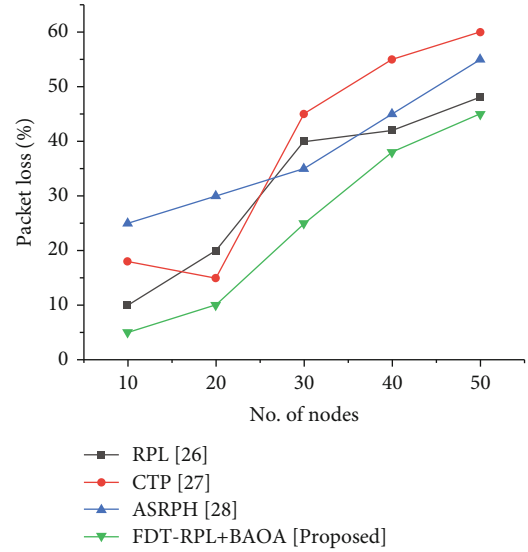

Figure 6: Packet loss results of the proposed methodology.

The fragrance value may be found in argument e, d is denoted by the sensory modality, and J is denoted by the stimulus intensity, according to the modality, which determines the power exponent; there is a wide range of absorption rates. Algorithm performance is affected by the values of parameters b and d, which are in the range of [0, 1].

$$y_j^{p+1} = y_j^p + \left(s^2 \times h^* - y_j^p\right) \times e_j, \tag{20}$$

where y_j^p represents the i^{th} iteration's butter ant. Also, h^* is the best butter ant in the current iteration, and e_j is the fragrance of i^{th} butterfly, while s is a random number between 0 and 1. It is possible to carry out the local search in this algorithm as follows:

$$y_j^{p+1} = y_j^p + \left(s^2 \times y_i^p - y_l^p\right) \times e_j, \tag{21}$$

where s a random number between 0 and 1, while y_i^p and y_l^p are i^{th} and l^{th} butter ant in the same swarm.

In this method, butter ant is used to find the best path to the desired destination using forward and backward ant operations. The computation of the maximum number of paths max MU_{xy} which can be on the network is defined by

$$\max\_MU_{xy} = \frac{KK_{xy}}{K_v + \Delta K} MK_{xy}. \tag{22}$$

The computation of density of path (C_{xy}) is defined by

$$C_{xy} = \frac{MU_{xy}}{\max\_MU_{xy}}. \tag{23}$$

Forward butter ants are employed in butter ant optimization to discover the best and fastest route to the target.

The forward ants characterize the movement of a new location as follows:

$$t_{xy}^{l}(p) = \begin{cases} \dfrac{b(\partial_{xy}) + a\left(1 - \eta_{xy}\right)}{\sum_{g \notin pbau_l} b(\partial_{xy}) + a\left(1 - \eta_{xy}\right)} \times \left(\dfrac{1}{1 + (1/M_i)}\right) \text{if } i \notin pbau_l, \\ 0 \end{cases} \tag{24}$$

where

∂_{xy}: The pheromone values of an ant at node x to travel to node y represented and computed by ants working backward,

η_{xy}: Fuzzy values on the connection from x to y estimated by the vehicle as an ant at this point,

b: Reflects the relevance of ∂_{xy} in terms of its weight,

a: Indicates the relevance of η_{xy} weight in the equation.

Upon reaching their target, advancing ants transform into backward ones and vice versa. This is why backward ants use the memories of their advanced ants to choose the best route.

4. Result and Discussions

The overall behavior of the recommended framework is discussed in this section. The MATLAB simulation tool is employed for analyzing the performance of the suggested system. Figures 3–8 compare existing and proposed approaches on parameters such as packet delivery ratio, energy consumption, throughput, network lifetime, and packet loss.

Additionally, there are routing protocols for low-power and lossy networks (RPL), connecting tree protocols (CTPs), and application-specific routing protocols for healthcare.

As shown in Figure 3, there is an end-to-end delay between the proposed and existing methods. Every millisecond a packet travels from the sender to the receiver is counted as an end-to-end delay (ms). The above figure illustrates that the proposed BAO algorithm has a low end-to-end delay compared to other existing protocols [25–28] such as the routing protocol for low-power networks (RPL), the connecting tree protocol (CTP), and the application-specific routing protocol for healthcare (ASRPH).

Based on the proposed and existing approaches, Figure 4 shows the energy consumption results. From the above diagram, the proposed method of BAO algorithm consumes less energy than existing methods [25–28] like routing protocol for lossy networks (RPL), connecting tree protocol (CTP), and application-specific routing protocol for healthcare (ASRPH).

Figure 5 represents the network lifetime results with proposed and existing approaches. From the above figure, the proposed method of BAO algorithm has a high network lifetime. In comparison to existing methods [25–28] such as the routing protocol for lossy networks (RPL), the connecting tree protocol (CTP), and the application-specific routing protocol for healthcare (ASRPH), this protocol has the following advantages.

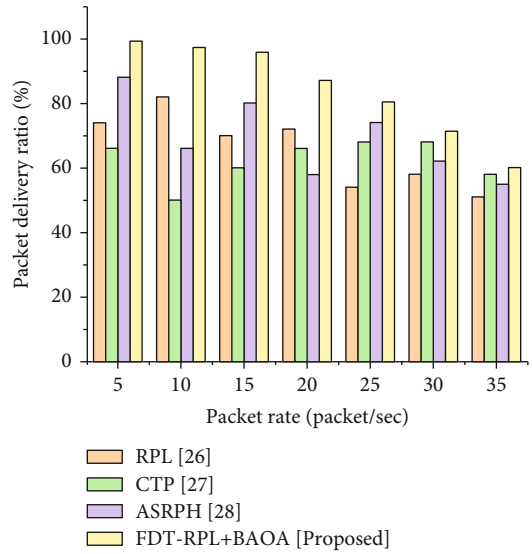

Figure 7: Packet delivery ratio results of the proposed methodology.

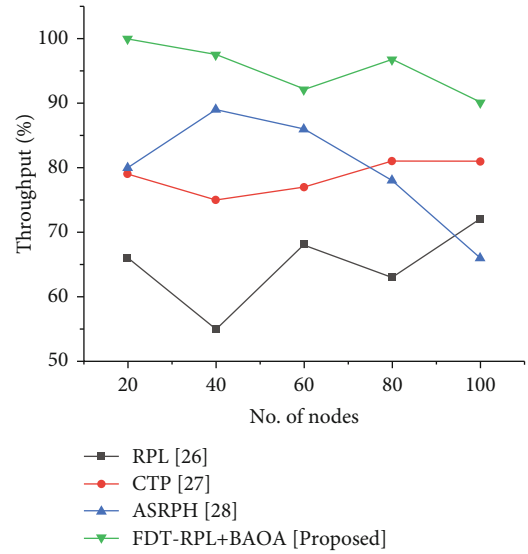

Figure 8: Throughput results of the proposed methodology.

Figure 6 represents the packet loss results with proposed and existing approaches. In comparison to existing methods [25–28] such as the routing protocol for low-power and lossy networks (RPL), connecting tree protocol (CTP), and healthcare application-specific routing protocol (ASRPH), the proposed method of BAO algorithm has relatively low packet loss.

Figure 7 represents the packet delivery ratio results with proposed and existing approaches. As can be seen in the above diagram, packet delivery ratios are measured as a function of how many packets are sent and received. With the BAO algorithm, packet delivery ratios are greatly improved over similar methods [25–28], such as routing protocol for low-power and lossy networks (RPL),

connecting tree protocol (CTP), and application-specific routing protocol for healthcare (ASRPH).

Figure 8 represents the throughput results with proposed and existing approaches. As shown above, the proposed method of BAO algorithm has a higher throughput in comparison to existing methods [25–28] like routing protocol for low-power and lossy networks (RPL), connecting tree protocol (CTP), and healthcare-specific routing protocol (ASRPH).

The overall comparison of proposed and existing methods shows that the proposed methods are high in packet delivery, throughput, and network lifetime and low in end-to-end delay, energy consumption, and packet loss.

In Figures 3–8, we compare throughput, end-to-end delay, packet delivery ratio, packet loss, network lifetime, and energy consumption for existing methods and proposed methods. There are numerous existing protocols for low-power, lossy networks, including RPL, CTP, and a healthcare-specific protocol (ASRPH). Compared to existing methods, the proposed BAO algorithm technique has a low end-to-end delay of 300 ms, while CTP, RPL, and ASRPH all have end-to-end delays of 800 ms, 1500 ms, and 500 ms, respectively. In packet delivery ratio, the proposed method of BAO algorithm has ratio 0.5 and the existing methods of RPL have 0.001, CTPhas0.3, and ASRPH has 0.003, so when compared to existing methods, the proposed techniques perform high in terms of packet delivery ratio. In the network lifetime, the proposed method of BAO algorithm has 3000 s, and the existing methods of RPL have 2400 s, CTP has 1380 s, and ASRPH has 2900 s, so when compared to existing methods, the proposed techniques perform better in terms of network lifetime [29–31]. In throughput, the proposed method of BAO algorithm has 99.7% and the existing methods of RPL have 97%, CTP has 93%, and ASRPH has 99%. Therefore, the proposed techniques outperform existing methods in terms of throughput.

The following are the demerits of the existing techniques. Considering the hop factor and energy usage into perspective will help us refine the recommended objective function (OF) in [26]. In addition, the implementation of FreeBW-OF in heterogeneous networks, where real and nonreal services can indeed be installed, will be fascinating to examine. Using practical testbed set up in actual circumstances, it is possible to further validate the suggested FreeBW-efficacy OFs by further testing. According to the results of [27], application-specific requirements cannot be met by a generic routing protocol proposal technique. They intend to do considerable research to lay the groundwork for the suggested second tier. To further improve the routing protocol, they will look at the possibility of extra routing metrics, including a computation of all performance measures. As per [28], subsequent research is needed since it will concentrate on refining the SEF-IoMT for use in situations involving human mobility, where changes in sensor position are common. Inter-WBAN data transformation in the suggested SEF-IoMT architecture has to be more energy-efficient and secure. Our suggested approach provides a proper response to the requirements of healthcare-IoT systems while maintaining acceptable performance of the network, as demonstrated by the contrast of our findings to the previous efforts.

5. Conclusion

Healthcare organizations around the world are working together to guarantee that IoT and cloud computing offers a smooth transition to the sector. The research will be of interest to users wishing to learn more about IoT and mobile computing in healthcare. As a platform for the transfer of medical data among medical device server or mobile computing app platforms, it provides a comprehensive cloud-based IoT foundation for healthcare. Many concepts and technologies are constantly being added to the IoT and mobile computing in the healthcare integration process; thus, this study also quickly categorizes and summarizes them. We have proposed the butter ant optimization algorithm for mobile computing in this study. Mobile computing is used as an intermediary layer between the Internet of Things and cloud computing, locating its resources at the perimeter of an IoT network and distributing them. As a result, greater resource management may be offered in mobile computing (MC) and cloud environments, increasing throughput and quality of service (QoS). KNN in the data cleaning stage is susceptible to artifacts, such as noise. For it to be accurate, the training data must be of high quality. When there are errors in data labeling and conflicts between distinct groups of samples, categorization becomes less reliable. Hence, it is a limitation of our research. In future days, if artificial intelligence-based techniques are used, then we will enhance the performance of this research additionally.

Data Availability

There are no relevant data to be made available.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] T. Vaiyapuri, V. S. Parvathy, V. Manikandan, N. Krishnaraj, D. Gupta, and K. Shankar, "A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing," *Wireless Personal Communications*, Article ID 234037751, pp. 1–24, 2021.

[2] K. Jaiswal and V. Anand, "EOMR: an energy-efficient optimal multi-path routing protocol to improve QoS in wireless sensor network for IoT applications," *Wireless Personal Communications*, vol. 111, no. 4, pp. 2493–2515, 2020.

[3] M. R. Rahman, M. M. Islam, A. I. Pritom, and Y. Alsaawy, "ASRPH: application specific routing protocol for health care," *Computer Networks*, vol. 197, p. 108273, 2021.

[4] T. Ul Hassan, M. Asim, T. Baker, J. Hassan, and N. Tariq, "CTrust-RPL: a control layer-based trust mechanism for supporting secure routing in routing protocol for low power and

lossy networks-based Internet of Things applications," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 3, p. e4224, 2021.

[5] H. Kharrufa, H. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications: a review," *IEEE Sensors Journal*, vol. 19, no. 15, pp. 5952–5967, 2019.

[6] Y. Qu, G. Zheng, H. Ma, X. Wang, B. Ji, and H. Wu, "A survey of routing protocols in WBAN for healthcare applications," *Sensors*, vol. 19, no. 7, p. 1638, 2019.

[7] A. Patel and D. Jinwala, "A reputation-based RPL protocol to detect selective forwarding attack in Internet of Things," *International Journal of Communication Systems*, vol. 35, no. 1, article e5007, 2022.

[8] J. Marietta and B. Chandra Mohan, "A review on routing in internet of things," *Wireless Personal Communications*, vol. 111, no. 1, pp. 209–233, 2020.

[9] Z. A. Almusaylim, A. Alhumam, and N. Z. Jhanjhi, "Proposing a secure RPL based internet of things routing protocol: a review," *Ad Hoc Networks*, vol. 101, p. 102096, 2020.

[10] U. Pujianto, A. P. Wibawa, and M. I. Akbar, "K-nearest neighbor (k-NN) based missing data imputation," in *In 2019 5th International Conference on Science in Information Technology (ICSITech)*, Yogyakarta, Indonesia, Oct 2019.

[11] C. M França, R. S Couto, and P. B Velloso, "Missing data imputation in Internet of Things gateways," *Information*, vol. 12, no. 10, p. 425, 2021.

[12] S. X. Wu, H. T. Wai, L. Li, and A. Scaglione, "A review of distributed algorithms for principal component analysis," *Proceedings of the IEEE*, vol. 106, no. 8, pp. 1321–1340, 2018.

[13] S. T. Manukumar and V. Muthuswamy, "A novel multi-objective efficient offloading decision framework in cloud computing for mobile computing applications," *Wireless Personal Communications*, vol. 107, no. 4, pp. 1625–1642, 2019.

[14] S. Nazir, Y. Ali, N. Ullah, and I. García-Magariño, "Internet of Things for healthcare using effects of mobile computing: a systematic literature review," *Wireless Communications and Mobile Computing*, vol. 2019, 20 pages, 2019.

[15] R. Somula, C. Anilkumar, B. Venkatesh, A. Karrothu, P. Kumar, and R. Sasikala, "Cloudlet services for healthcare applications in mobile cloud computing," in *Proceedings of the 2nd International Conference on Data Engineering and Communication Technology*, pp. 535–543, Singapore, 2019.

[16] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[17] S. Jegadeesan, M. Azees, P. M. Kumar et al., "An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications," *Sustainable Cities and Society*, vol. 49, p. 101522, 2019.

[18] K. Peng, V. Leung, X. Xu, L. Zheng, J. Wang, and Q. Huang, "A survey on mobile edge computing: focusing on service adoption and provision," *Wireless Communications and Mobile Computing*, vol. 2018, 16 pages, 2018.

[19] F. Muheidat and L. A. Tawalbeh, "Mobile and cloud computing security," in *Machine Intelligence and Big Data Analytics for Cyber Security Applications*, pp. 461–483, Springer, Cham, 2021.

[20] W. Lin, M. Xu, J. He, and W. Zhang, "Privacy, security and resilience in mobile healthcare applications," *Enterprise Information Systems*, pp. 1–15, 2021.

[21] E. Politou, E. Alepis, M. Virvou et al., "An introductory survey on attention mechanisms in NLP problems," in *Intelligent Systems and Applications*, pp. 93–131, Springer, Cham, 2022.

[22] G. H. Gezahagn, T. Teklu, H. Yirgaw, and M. Huda, "Pervasive healthcare computing: applications, challenges and solutions," in *Pervasive Healthcare*, pp. 31–45, Springer, Cham, 2022.

[23] A. Zrelli, "Hardware, software platforms, operating systems and routing protocols for Internet of Things applications," *Wireless Personal Communications*, vol. 122, no. 4, pp. 3889–3912, 2022.

[24] M. A. Kareem and S. Tayeb, "Securing routing in low power and lossy networks," in *Proceedings of the Future Technologies Conference*, pp. 330–344, Cham, 2021.

[25] A. Musaddiq, Z. Nain, Y. Ahmad Qadri, R. Ali, and S. W. Kim, "Reinforcement learning-enabled cross-layer optimization for low-power and lossy networks under heterogeneous traffic patterns," *Sensors*, vol. 20, no. 15, p. 4158, 2020.

[26] H. Bouzebiba and M. Lehsaini, "Freebw-rpl: a new rpl protocol objective function for internet of multimedia things," *Wireless Personal Communications*, vol. 112, no. 2, pp. 1003–1023, 2020.

[27] A. H. Lenin, S. M. Vasanthi, and T. Jayasree, "Automated Recognition of Hand Grasps Using Electromyography Signal Based on LWT and DTCWT of Wavelet Energy," *International Journal of Computational Intelligence Systems*, vol. 13, no. 1, pp. 1027–1035, 2020.

[28] T. Saba, 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*, vol. 13, no. 10, pp. 1567–1575, 2020.

[29] M. Alazab, K. Lakshmanna, T. Reddy, Q. V. Pham, and P. K. R. Maddikunta, "Multi-objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities," *Sustainable Energy Technologies and Assessments*, vol. 43, p. 100973, 2021.

[30] D. S. Rajput, S. M. Basha, Q. Xin et al., "Providing diagnosis on diabetes using cloud computing environment to the people living in rural areas of India," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, pp. 2829–2840, 2022.

[31] C. Zhu, C. U. Idemudia, and W. Feng, "Improved logistic regression model for diabetes prediction by integrating PCA and K-means techniques," *Informatics in Medicine Unlocked*, vol. 17, p. 100179, 2019.