IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 22, 2020, accepted June 24, 2020, date of publication July 6, 2020, date of current version July 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007405

A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in Wireless Body Area Networks

GULZAR MEHMOOD[1], MUHAMMAD ZAHID KHAN[1], ABDUL WAHEED[2,3], MAHDI ZAREEI[4], (Member, IEEE), AND EHAB MAHMOUD MOHAMED[5,6], (Member, IEEE)

[1]Department of Computer Science and Information Technology, University of Malakand, Pakhtunkhwa 23021, Pakistan
[2]Department of Information Technology, Hazara University Mansehra, Mansehra 21120, Pakistan
[3]School of Electrical and Computer Engineering, Seoul National University, Seoul 08826, South Korea
[4]Tecnologico de Monterrey, School of Engineering and Science, Zapopan 45201, Mexico
[5]Electrical Engineering Department, College of Engineering, Prince Sattam Bin Abdulaziz University, Wadi Addwasir 11991, Saudi Arabia
[6]Electrical Engineering Department, Faculty of Engineering, Aswan University, Aswan 81542, Egypt

Corresponding author: Gulzar Mehmood (gulzar.mahmood@uom.edu.pk)

ABSTRACT Wireless Body Area Network is an emerging technology that is used primarily in the area of healthcare applications. It is a low-cost network having the capability of transportability and adaptability. It can be used in location independent and long-term remote monitoring of people without disturbing their daily activities. In a typical WBAN system, sensing devices are either implanted or etched into the human body that continuously monitors his physiological parameters or vital signs. In such a network, trusts among the stakeholders (healthcare providers, users, and medical staff, etc.) are found of high importance and regarded as the critical success factor for the reliability of information exchange among them. In remote patient monitoring, the implementation of trust and privacy preservation is crucial, as vital parameters are being communicated to remote locations. Nonetheless, its widespread use, WBAN, has severe trust and privacy risks, limiting its adaptation in healthcare applications. To address trust and privacy-related issues, reliable communication solutions are widely used in WBANs. Given the motivation, in this paper, we have proposed a trust-based communication scheme to ensure the reliability and privacy of WBAN. To ensure reliability, a cooperative communication approach is used, while for privacy preservation, a cryptography mechanism is used. The performance of the proposed scheme is evaluated using MATLAB simulator. The output results demonstrated that the proposed scheme increases service delivery ratio, reliability, and trust with reduced average delay. Furthermore, a fuzzy-logic method used for ranking benchmark schemes, that has been concluded that the proposed scheme has on top using comparative performance ranking.

INDEX TERMS Wireless body area networks, body-to-body-networks, energy-efficiency, trust-based communication, reliability, fuzzy logic.

I. INTRODUCTION

Trust may be defined as the kind of belief that something is reliable enough that will not harm or interrupt the smooth services of real-time applications. It has great importance in real life as well as in the use of dealing with sensitive data. WBAN healthcare applications are mostly concerned with entity sensitive data. Hence trust has great importance and influence on the quality and credibility in healthcare applications and provisions. Trust-based provision has an explicit relationship with a healthcare professional because it guarantees an accurate and timely diagnosis of the patient [1]. Wireless Body Area Networks (WBAN) is the particular type of Wireless Sensor Network (WSN) made

The associate editor coordinating the review of this manuscript and approving it for publication was Wei-Chang Yeh.

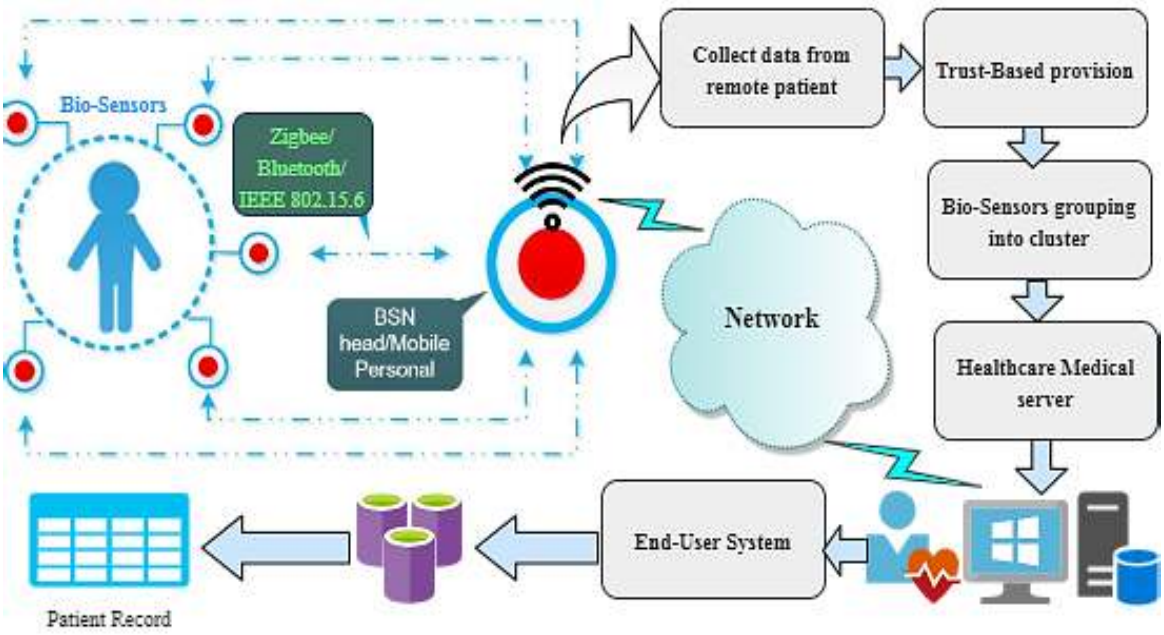


FIGURE 1. Trust based architecture of WBAN.

from small bio-sensors, which are fitted on, or implanted inside entity-body for recognizing vital parameters [2]. The implanted bio-sensors monitor the biological changes insides the body and then sent through control nodes to the gateway and then further to the remote Medical Server (MS) [3]. WBAN usually assumes star topology because there are limited bio-sensors associated with the entity-body, and all are mostly controlled by a central controller [4]. These central controllers are resource-full devices; however, due to the recourse-constrained nature of bio-sensor devices, issues arise at the node level.

Moreover, energy-efficiency is also of equal importance in terms of reliability in WBAN. The replacement of battery at remote patient monitoring in WBAN is avoided, especially in the case of implanted bio-sensors [5]. Figure 1 depicts the general description of a trust-based scheme for the remote patient monitoring system in WBAN. In which, data are collected from the remote patient through the Body Control Unit (BCU). Then pass the data from the trust engine. After the necessary action and trust, provision saves the reliable data in the database of medical server. The trust provision is accomplished whenever data are collected from bio-sensors. The detailed scenario is presented in section 3 of the paper. According to research statistics, more than 80% of WBAN applications are in the field of the health side [6]. Therefore, most authors considered healthcare applications as a test case for evaluating WBAN solutions [7].

In remote patient monitoring, trusted information has great importance for healthcare providers due to the sensitivity of data. Therefore, trust and reliability provision is essential for healthcare services in WBAN [8], [9]. Trust can further ensure the reliability in WBAN, which is essential in the healthcare service of WBAN [10]. In the literature, we will give a detailed review of relevant schemes to address the research gaps. Furthermore, the cryptography-based solution is provided in the last section of the proposed solution for privacy preservation and improved reliability in WBAN.

A. HIGH-LEVEL DESCRIPTION

In healthcare applications, the preservation of trust among bio-sensors and other devices, e.g., control nodes and gateways, is essential for the reliability of WBAN [11]. Since the information sensed by bio-sensors is sent further to be considered for the diagnosing process of entity-body in the WBAN environment. Many authors have highlighted various kinds of challenges in their research works. Therefore, in WBAN, trust must be ensured to send reliable data to the medical server. If un-trusted and unreliable data is transmitted to the medical server/medical database, healthcare providers (doctors and technicians) will ultimately make a wrong diagnosis, which can severely threaten the lives of patients. In this context, trust and reliability in WBANs applications are highly valuable.

B. LIMITATIONS OF EXISTING SOLUTIONS

WBAN faced many trust, privacy, and reliability challenges due to critical data. In remote patient monitoring dealing with healthcare users, the provision of trust of entity and reliability of data are key challenges. Apart from this, some other key challenges are related to security, interoperability, mobility, heterogeneity, reliability, privacy, biocompatibility, and, most importantly, power consumption. The reliability level of WBAN is increased by using key management techniques,

which also provides trust in the network. Although, security mechanism such as cryptography has been used previously for trust management [12]. However, previously proposed trust management schemes consume many resources of resource-constrained WBANs due to the massive operations involved [8], [13], [14].

C. MOTIVATION

The paper attempts to address trust management in WBAN while considering the necessary resources requirement. Trust management in WBAN is an essential aspect used to improve the reliability of healthcare services. Some researchers have demonstrated their trust management models or schemes used in WSN and WBAN using different approaches. Some of these approaches are fuzzy logic, machine learning approaches, bio-inspired, deterministic, and probabilistic based approaches [8], [14]–[16]. Cooperative communication is a useful networking approach for trust management and to increase reliability inside the network. Although, some authors used a cooperative communication approach for improving the reliability of inside the network. However, the detailed performance evaluation has not performed. Therefore, we have been motivated to address the issue of trust using the trust engine along with cooperative communication collectedly in the WBAN environment.

D. NOVEL CONTRIBUTION

The novel contribution of the proposed scheme is a trust-based ERCS (Energy-Efficient and Reliable Communication scheme) to ensure trust using cooperative communication. The cooperative strategy has been adopted to create trust among bio-sensors to make the network reliable. Furthermore, the trust has generated at the remote medical server by applying the trust certificate. To the best of our knowledge, the cooperative sensing approach, along with the trust engine for trust management has not been used previously in WBAN. Using this approach, the service delivery ratio is increased while the average delay is minimized significantly.

Moreover, for privacy preservation, a new cryptographic solution is proposed at last to further preserve the privacy of data during remote patient monitoring in WBAN. The performance of the proposed scheme is evaluated using extensive simulations using various metrics using MATLAB simulator. The detailed performance evaluation demonstrated that the proposed scheme outperforms the state-of-the-art previously proposed schemes in terms of trust, energy-efficiency, and reliability. In the last section of the paper, a fuzzy logic rank-based evaluation is given. This ranking-based evaluation further attested that the proposed scheme gives an improved performance compared to previously proposed schemes.

In section II, we summarize the most relevant state of the art schemes related to the problem domain, especially in the area of WBAN and WSN. In section III, the proposed scheme is presented for remote patient monitoring using the WBAN scenario. In section IV, the performance result of the proposed scheme is demonstrated. And finally, in section V, the conclusion and future direction are elicited.

II. BACKGROUND AND LITERATURE SURVEY

In this section, we review state-of-the-art trust-based and reliability related schemes in WBAN. In WBAN healthcare applications, reliability is a crucial concern since remote patient monitoring deals with critical data. In remote patient monitoring, the data is only accepted from a trusted entity-body. Furthermore, remote patient monitoring involves several entities when forwarding sensed data to the medical server. This communication is sometimes based on a Body-to-Body Network (BBN), which supports several innovative applications, including remote patient monitoring, interactive games, and military applications [17]–[19].

He *et al.* [20] proposed ReTrust (Attack-Resistant and light-weighted trust management), a two-tier architecture for medical body sensor networks. In the first tier, the trust model is defined, and then the trust calculations of Re-Trust are accomplished. In trust calculation, a different attack management system is analyzed for different categories of trust. Moreover, security analysis, efficiency analysis, and functionality evolution of the proposed ReTrust are accomplished. From the critical study, it has been concluded that the proposed approach prolongs network lifetime capacity and ensures privacy. However, it lacks the detail of basic network parameters. Additionally, the explanation is missing that in what way the proposed trust management approach improves reliability. Furthermore, the proposed approach needs to test on the recent WBAN environment. Similarly, a Dynamic Trust Evaluation Model (DTEM) is proposed by Ye *et al.* [9] for WSNs. In the proposed model, the direct trust approach is combined with a recommendation-based trust approach to dynamic weight. Furthermore, direct trust is calculated based on the number of trust factors consisting of previous communication history. While the recommendation trust is calculated and evaluated by the third party. The author performed trust evaluation at the end and stated that a normal node will always cooperate during communication while a malicious node will not. From the critical review of the proposed scheme, we concluded that the trust model is an efficient alternative to traditional security mechanisms. It can evaluate and solve the node inside misbehavior attack, which provides security services to the upper layers. However, it may be a challenging task to deploy and manage the trust authority is restricted WBAN due to a restricted environment.

Ganeriwal *et al.* [21] proposed a module to check the actions of its neighbor nodes. Apart from this, the author also analyzed to know that their activities are cooperative or non-cooperative. Furthermore, the reputation of neighbor sensor nodes is also checked. It has been concluded that enough processing and interaction with sensors are required to reach a stable point. However, if the bio-sensor has a quick movement inside the network, the proposed framework will not be performing accordingly. Feng *et al.* [16] proposed a method in which trust is calculated using and analyzing the

neighbor node's data forwarding behavior. In the proposed method, NBBTE (Node Behavioural Strategies Banding Belief Theory into Trust Evaluation method) is used to establish trust factors between neighbor nodes. Furthermore, to get integrated trust values, the Dempster–Shafer (D–S) evidence theory method was assumed instead of a simple weighted-average. However, this scheme is not energy-efficient due to excessive message communication among neighbor sensor nodes [9]. Gemoz *et al.* [22] proposed a model where the data is being classified into three types, *raw data*, *routed data*, and *process data*. A bio-sensor vital sign is a raw data as long as other nodes sense it without any additional processing or routing. Whenever the sensed data is sent to other nodes, it becomes routed data. Processing means data interpretation, such as data fusion, data aggregation, or data classification. In the proposed mechanism, they are associated with energy. If an action by a node consumes the usual power, then the effect is coincided as normal. Otherwise, if the effect of a node consumes more energy, then it is considering as an abnormal action, and the node is considering as a malicious node. However, sometimes a critical event consumes more energy, which is essential for the system to consider, and the proposed mechanism fails to distinguish it. In [23], [24], trust is calculated based on three factors. The 1st criteria are cooperative communication, 2nd criteria are the level of energy, and the 3rd criteria are data consistency that the resistance against denial of service attacks. However, the main limitation of the proposed schemes is that it is not clear how the trust value will be updated [9].

In [25], Rathore *et al.* proposed a trust model for Wireless Sensor Networks in which the trust factor is based on the consistency and consensus of the data. The paper introduces a novel model for the trusted computing of a node. The proposed model proves itself to be more effective compared to other methods that adopt machine learning and neural network-based approaches. However, the main drawback of the proposed model is that if the percentage of malicious nodes is more than 50%, then the model does not work well [26]. In [14], Anguraj and Smys proposed a malicious node detection scheme named "BAN-Trust," which identifies the malicious attacked on WBAN. BAN-Trust can conceive common behaviors among the bio-sensor nodes, i.e., data, energy, and communication. Besides, the proposed scheme used a clustering approach to minimize delay, increase throughput, and energy-efficiency. The proposed scheme can be adopted in an optimized manner for a remote patient monitoring system in WBAN, where it gives marvelous results. Fault aware trust determination algorithm (FATD) is proposed for Wireless Body Sensor Network (WBSN) in [27] by Chitra and Kanagachidambaresan Where the trust of the node is identified using the voltage of the battery, receiver signal strength (RSSI), and mobility of the nodes. A unique value between -1 and 1 is assigned to each node represent a trust value. The proposed algorithm is a better solution for trust issues and increases the network lifetime. The author claimed to test the proposed work in a real healthcare environment. However, dependency on battery voltage is not a realistic approach to trust management. Moreover, real-time testing of the proposed algorithm with diverse parameters is needed.

Similarly, in [28], Bhangwar *et al.* tried to solve the issue of trust by restricting the misbehaving nodes with increased network lifetime and maintained a trusted and balanced environment. The author stated that the traditional cryptographic schemes consume much of the network's resources and are also complicated for trust evaluation. Therefore, trust and thermal-aware routing protocol are proposed for trust among nodes to isolate the misbehaving nodes. However, with the increasing traffic load, the temperature of some nodes rises, which degrades the performance of WBAN. Jayasinghe *et al.* [13] proposed a privacy preservation blockchain method for edge computing know as Trust Chain. In which a mechanism for IoT devices trust can be evaluated incorporating their physical properties and identity. This future eliminates physical attacks on IoT devices. The main limitation of the proposed mechanism is that the centralized server is used for storage. Moreover, excessive exchange of messages between the device and server overload the network.

In this research study, state-of-the-art trust-based research contributions for WBAN application are reviewed. We have concluded from the literature survey that a novel scheme to enhance the trust and reliability level of WBAN applications is needed. The new scheme should increase the trust level for remote patient monitoring in WBAN. Moreover, with the increase in trust level, the reliability level is also increased in WBAN.

III. PROPOSED SYSTEM MODEL

In this section, the proposed model is discussed in detail. In WBAN remote patient monitoring applications, numerous body vital signs are sensed by bio-sensor nodes. These vital parameters are then sent to the remote medical server or cloud-based server for further processing, where necessary treatment and action have been carried out on it. In the system model, all the components from simple bio-sensor up to the medical server are mentioned. To maintain trust and reliability, it is necessary to ensure it from tier one at zero level of WBAN, where we need trust and cooperation at the first stage. At the second tier of WBAN, i.e., at the gateway level, trust provision is essential. Then, there is a stable and secure network at the medical server where trust provision is not an issue. However, the trust provision is initialized from the medical server. Moreover, relay nodes may also involve in the routing process in the most cause in WBAN [29]. Therefore, relay nodes' extra responsibility is to discover and maintain a trusted route in the network.

The maintenance of the trusted routes is also the responsibility of the relay nodes or control node. The proposed scheme has been elaborated and demonstrated in the following ways. First, a trust-based remote patient monitoring system architecture is developed. The basis of

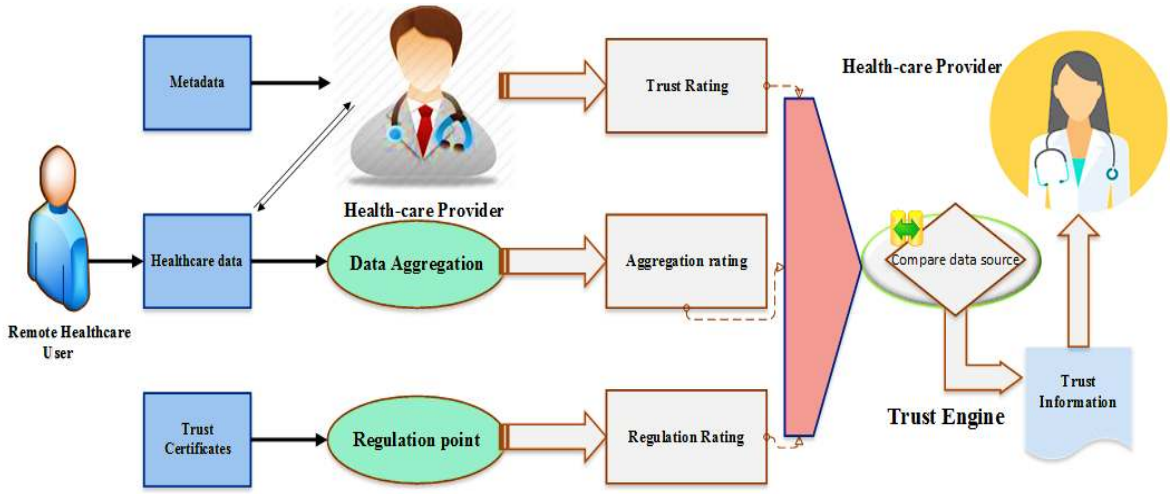


FIGURE 2. Trust-based and reliable model.

the trust-based architecture, trust-based cooperative system is designed. And lastly, the cryptography Solution for privacy preservation is discussed in section 3.3.

A. TRUST-BASED REMOTE PATIENT MONITORING SYSTEM ARCHITECTURE

Motivation: The primary motivation for the proposed scheme is that the traditional cryptographic schemes utilized much of the resources of the resources constrain WBAN for trust management. Therefore, an alternative for these security schemes is light weighted cooperation-based trust management. In which the first trust values are generated by the trust engine, as shown in Figure 2. Based on this, a trust-based cooperative communication model is developed.

Figure 2 elaborates on the architecture, which is based on Hedaquin architecture [8], [30], but we used it for trust management. In the proposed architecture, the trust engine is the basic unit that takes inputs from trust rating, cooperative aggregation rating, and rule rating. Then the trust engine calculates the trust information based on these three kinds of ratings. On the base of trust information, healthcare providers make the necessary healthcare decisions about remote healthcare users. In trust-based details, there is an indicator to the healthcare provider about the quality and privacy of healthcare data of remote end healthcare users. Trust rating includes local/global rating; healthcare users give the local rating at the remote healthcare site. Before trust provision, a remote healthcare provider provides a global rating before trust provision. The rule ratings collected from a rule machine, which is the rating given to each node basis on degree and certificates. Furthermore, the aggregation rating is gain from the aggregation engine. In WBAN, each user is considered a cluster, and aggregative data are collected by Cluster Head (CH) [12], [31]. In the cause of received and calculated measurement data are the same, then the trust rate of data will be high. The computed trusted information has great importance for a healthcare provider to decide about a remote patient [8]. In the proposed scheme, the rating is a tuple $(P_{x,y,sc,t},\ Q_{x,y,sc,t},\ C_{x,y,sc,t})$, where P, Q, C is a real number between 0 and 1 and $P + Q = 1$. Likewise, R is a positive fraction, S is a negative fraction, and C is the predictability of the rating. Besides, in subscript x is the healthcare user who provides the rating. Bes y is the healthcare user who has been rated, and sc is defined as the scope of the data. While t is the trust type for healthcare data. The scope in the tuple is the vital sign measurement, e.g., heart rate and device ECG machine.

A Trust engine is a tuple $(R_{x,y,sc,t},\ S_{x,y,sc,t}) \in T$, where T is a trust of end-user healthcare data. The trust engine calculates the trust of healthcare data provided by remote healthcare users. The trust derived in the trust engine is depended on trust rating, aggregation rating, and rule rating. Furthermore, trust ratings from high recommendation will be given preference on relatively low recommendation data. The re-communication includes information about the critical of data and their privacy level. The trust-based rate recommendation is considered as follows:

$$R_{x,z,sc,F,t} = R_{y,z,sc,F,t} \tag{1}$$

$$S_{x,z,sc,F,t} = S_{y,z,sc,F,t} \tag{2}$$

$$C_{x,y,sc,F,t} = \frac{R_{x,y,sc,R,t}}{R_{x,y,sc,R,t} + R_{x,y,sc,R,t}} \times C_{y,z,sc,F,t} \tag{3}$$

$C_{x,y,sc,F,t}$ is the trust rating at the local level at the remote side. Certainty 'C', high degree value, obtains excellent rating and attention as compared to low certainty. After calculating the rating for healthcare data (local/global, aggregation ratings and rule rating), the healthcare data will be in the form of a tuple $(RT_{x,y,sc,F,t}, ST_{x,y,sc,F,t})$ and $(RR_{x,y,sc,F,t}, SR_{x,y,sc,F,t})$. Furthermore, trust can be calculated at the global level by the trusted party at the health care unit

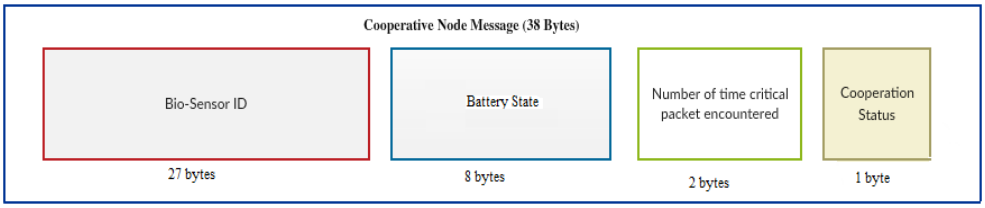


FIGURE 3. Structure of CNM (cooperative node message).

in the trust engine as follow:

$$TR_{x,y,sc,F,t} = \omega_T \cdot RT_{x,y,sc,F,t} + \omega_T \cdot RR_{y,sc,F,t} \quad (4)$$

$$TS_{x,y,sc,F,t} = \omega_T \cdot ST_{x,y,sc,F,t} + \omega_T \cdot SR_{y,sc,F,t} \quad (5)$$

In equations 4 and 5, ω_T is the weight of trust given to the vital sign of different entity parameters and $\omega_T \in \mathbb{R}^+$ positive fraction.

Most importantly, this measurement automatically calculated the trust of remote healthcare user data and gave a weight according to their rating [30]. The trust evaluation improves the reliability of communication and isolates the malicious nodes interference [32].

B. TRUST-BASED COOPERATIVE COMMUNICATION SYSTEM

In this section of the paper, we describe in detail the cooperative communication strategy for remote patient monitoring in WBAN, according to [33], [34]. In cooperative communication scenarios, cooperative sensed values collected from different bio-sensors deployed on entity-body. The cooperative communication strategy is based on Cooperative Node Message (CNM) and Cooperative Communication Trust Model (CCTM).

1) COOPERATIVE NODE MESSAGE (CNM)

Cooperative Node Message is sent from Cluster Head (CH) through Gateway (GW) to requested a remote Medical Server (MS). In MS healthcare providers, check their trust and cooperation status updating the trust information and awareness in the network. The structure of CNM is presented in Figure 3. CNM contains four sub-sections bi-sensor node id, battery status, number of critical packets encountered, and cooperation status (i.e., either cooperative or non-cooperative node).

In healthcare site healthcare provider validates all the requirements of cooperative nodes. And cooperative information is communicated back through *GW* to control nodes or *CH*.

2) COOPERATIVE COMMUNICATION TRUST MODEL (CCTM)

CNM is initially sent to the requested WBAN and compares the initial parameters, the requester ID, Bio-sensor unique identifier and neighbor list, etc. The proposed scheme will be further elaborated by explaining its steps and requirements. The trust level can be directly calculated between the acquisition and collaboration among neighboring nodes in WBAN. In the cause of relay nodes (*R*), cooperative behavior is maintained in Trust Lists (*TLs*). The trust list record is updated on a regular interval on interaction with intermediate nodes. The TLs value is calculated using a correlation on the base of the information received from the intermediated node in CNM. The TLs table and trust value calculation table are demonstrated in Table 1.

The bio-sensor node's status is based on node storage capacity and remaining energy. A bio-sensor node has four primary status: critical poor, normal, and unusual. The critical node needs direct attention to communication. A node with a poor state, i.e., the storage capacity of 95% of its remaining energy is below 15%, a normal node has status storage capacity below 95%, and its residual energy is between 15 to 80%. And similarly, a node having status unusual has storage capacity under 95%, and the remaining energy is over 80%. This classification of bio-sensors helps us in creating a cooperative trust model in WBAN in remote patient monitoring.

We focus on creating trust among the bio-sensors related to an entity-body based on the above information in Table 1. Which usually derived from the bio-sensors node associated with WBAN. The scenario of Trust-Based ERCS is illustrated in Figure 4, where we consider two bio-sensor nodes A and B are related to a single WBAN. Moreover, A and B can easily decode their values send by others using a cooperative network coding approach. A relay node may involve a bio-sensor node not directly linked to the gateway node. In this case, a node from WBAN is used as a relay node (*R*). Similarly, trust is built among all bio-sensors devices using a cooperative network coding approach. The cooperation among sensor devices A and B are explained with the help of the below algorithm.

In figure 4, two sensor nodes A and B are considered to be cooperating and sharing their initial value to provide trust among bio-sensor nodes. Therefore, A and B share their value (remaining energy and storage capacity) so that trust can be generated in the WBAN. Moreover, trust value can also be generated based on their initial values and cooperation status. The node having high trust value or packet having high trust value is communicated further in WBAN remote patient monitoring system. The algorithmic steps of the proposed scheme are given below in Algo-1:

Thus, the trust level can be achieved using a cooperative network coding approach, which provides reliability in

TABLE 1. Correlation between battery status, cooperation status, and trust value.

Battery Status Classification (0-100%)		Cooperation Status	Trust Value (TV)
Critical	<13	-	-
Poor	≥ 13 & < 33	0	0
Poor	≥ 13 & < 33	1	+3
Poor	≥ 13 & < 33	0	-2
Poor	≥ 13 & < 33	1	+2
Normal	≥ 33 & < 70	0	-2
Normal	≥ 33 & < 70	1	+2
Normal	≥ 33 & < 70	0	-3
Normal	≥ 33 & < 70	1	+4
Unusual	≥ 70	0	-3
Unusual	≥ 70	1	+2
Unusual	≥ 70	0	+1
Unusual	≥ 70	1	-4

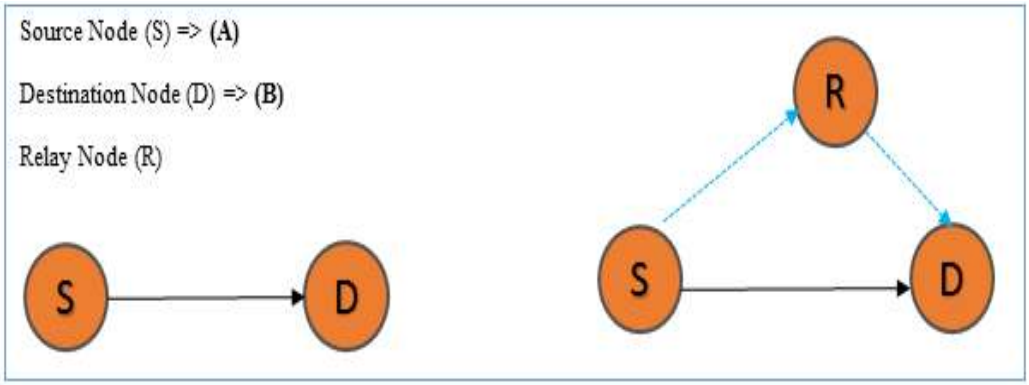


FIGURE 4. Bio-sensor A and B cooperation.

Algorithm 1 Proposed Trust-Based ERCS Scheme

START

Requirement: S_A, S_B, S_{GW} communicate their initial values for each session T **do**

1) **If** Bio-sensor A generate $\rightarrow S_A$
2) Bio-sensor B generates $\rightarrow S_B$
   Then
3) Both Broadcast S_A and $S_B$values
4) Bio-sensors A, B & GW Received Broadcast values S_A & S_B, $S_B \bigoplus S_A$, $S_A \bigoplus S_B$ **else**,
5) Bio-sensors A transmit $\rightarrow S_{AB} = S_A \bigoplus S_B$
6) Bio-sensors B transmit $\rightarrow S_{BA} = S_B \bigoplus S_A$
7) Gateway get $S_{AB} \rightarrow = S_A \bigoplus GW_{\text{value}}$
8) Gateway get $S_{BA} \rightarrow = S_B \bigoplus GW_{\text{value}}$
9) Thus, Gateway GW get $\rightarrow S_{AB} \approx S_{BA}$
   end if
10) Gateway GW Update their table
11) Gateway $GW \rightarrow S_A$ & S_B, $S_B \bigoplus S_A$, $S_A \bigoplus S_B$
12) For the trust, provision check the calculated and received values.
    End for

the network. Furthermore, using a cooperative approach, the energy consumption will be minimized significantly. Moreover, trust can be calculated using the formula in equation 6;

$$Tr = Wc\ Tc + We\ Te + Wd\ Td \tag{6}$$

In the above equation, Tr represents trust level, Wc, We, *and* Wd is the wait associated with trust interaction. Tc represents communication trust, Te represents energy trust, and Td represents data trust. Furthermore, W_c is weight is correlated with the interaction trust, W_e is the energy trust, and W_d is the weight associated to data trust. While $W_c + W_e + W_d = 1$ are all are non-negative numbers, Tc of a bio-sensor node is calculated according to successful (S) and unsuccessful (U) communication among bio-sensors nodes.

$$Tc = \frac{S}{S+U} \tag{7}$$

After that step, cluster, formation, and Cluster Head (CH) selection are performed. The main aims of the clustering approach are to minimized delay and send the cooperative data to the medical server. The proposed novel cooperative approach to generate adequate trust and to reduce energy consumption in remote WBAN remote patient monitoring. Similarly, the energy trust prediction model can measure the bio-sensor node's energy level. Following is the standard equation for the measurement of energy trust.

$$Te = \begin{cases} 1, & \text{if } E_{rem} < E_{tr} \\ 0, & -E \text{ else} \end{cases} \tag{8}$$

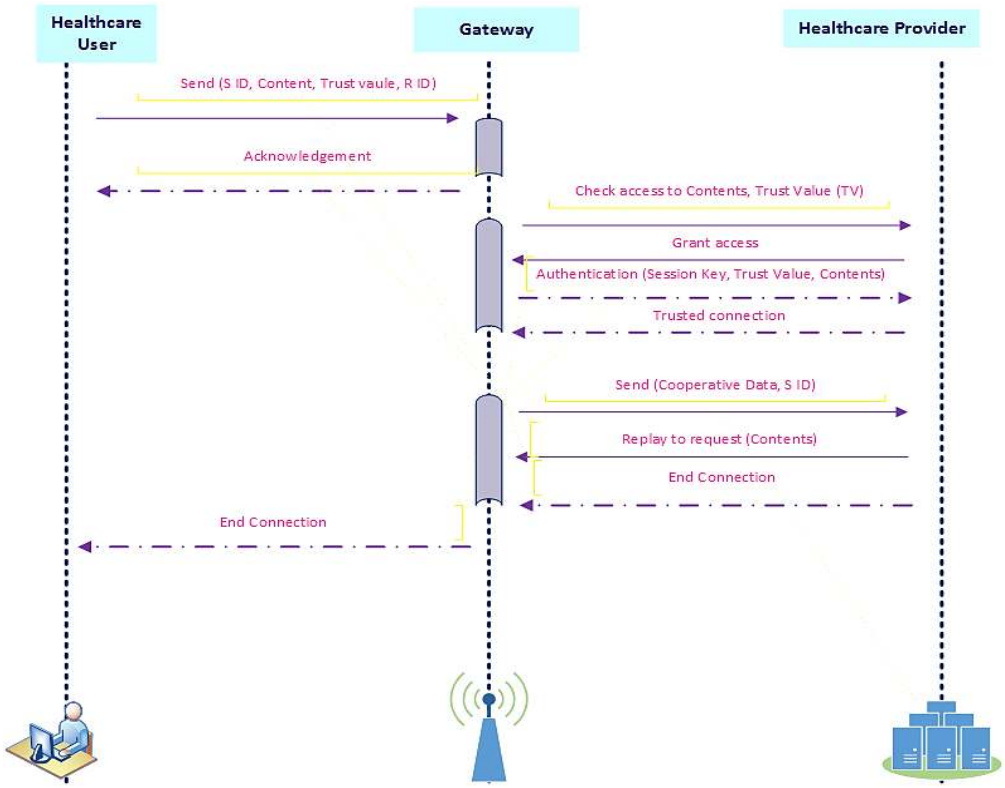


FIGURE 5. Proposed cryptographic-based privacy evaluation model.

Te is calculated for the usage rate of energy. E_{rem} is denoted as the remaining energy, and E_{tr} is the energy threshold. In case the residual energy goes down from the remaining energy, then the bio-sensor node isn't allowed to do the necessary communication.

C. CRYPTOGRAPHY SOLUTION FOR PRIVACY PRESERVATION AND RELIABILITY

In this section of the paper, a light-weighted data encryption solution is developed for remote healthcare system using WBAN. It is considered that the cryptography mechanism of our previous research work [12], is utilized here for privacy-preservation. This hybrid approach uses the session key with the trust value generated during the last section to ensure privacy. The privacy issue is a significant challenge in remote healthcare monitoring WBAN. Privacy preservation of healthcare sensitive is to maintain a trust base on creating a reliable session for critical data. Therefore, the proposed cryptographic solution tries to guarantee privacy at its best level. The privacy preservation solution for remote-Healthcare WBAN assured secure and trust-based transactions among nodes using session key size (128 *bits*). A packet is sent to the healthcare user, which contains the content of vital signs, node ID, and trust value. The gateway also appends its secret value with the packet. Then the encoded message is communicated to the medical server, where the healthcare provider checks their integrity and grant access based on trust value. Then in the secure session, the cooperative data are communicated. The trust-based link is ended at the server-side after a specific time whenever there is no need for connection for data transfer.

Figure 5 describes the cryptographic solution for healthcare users in remote patient monitoring in WBAN. Healthcare user sends a request based cooperative trust value through the gateway to the medical server. Where healthcare provider authenticates their identity and the secure session is established for remote healthcare users. Then session has been active for the time of a specific time frame. After accomplishing the data transfer between healthcare users and healthcare providers, the secure session made ended whenever needed. This process is again initiated whenever a new request is made for communication.

IV. SIMULATION AND EXPERIMENTAL RESULTS

This section of the paper presents a performance evaluation of the trust-based energy-efficient remote patient monitoring scheme using a cooperative mechanism. In the simulation, the scenario of the proposed study is demonstrated to evaluate its performances. After the description of the network scenario, the system validations are performance, and the output results are examined. The experiments are carried out using MATLAB simulator to analyze the performance of the proposed mechanism. MATLAB is a simulation platform suitable for low powered wireless network scenarios, such as

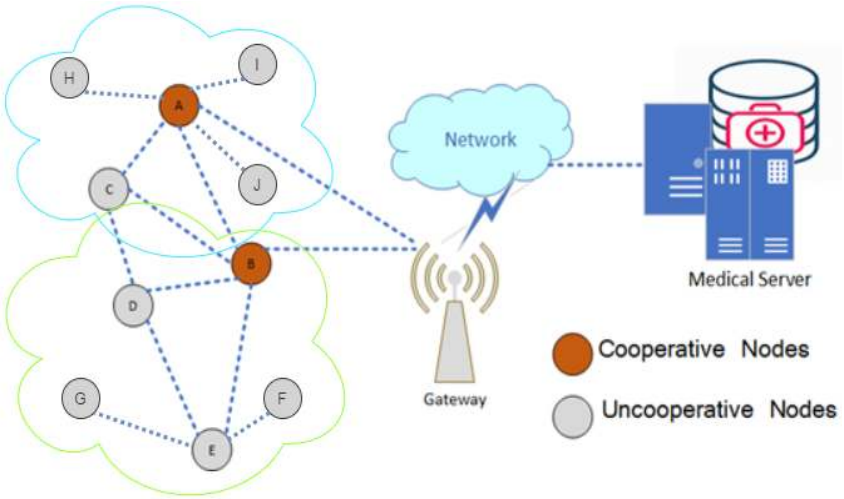


FIGURE 6. Illustration of the remote-health network scenario used for the performance evaluation.

a sensor network. For performance evaluation, the simulation result has been tested and compared with a different state of the art schemes.

A. NETWORK SCENARIO

The network scenario of the proposed mechanism is given in figure 6. For simulation, 15 × 15 m^2 network area is considered. For the experiment setup, *IEEE* 802.15.6 wireless standard is being adopted. The mentioned standard provides a low power, short-range, and reliable channels for human body communication. For data communication, cooperative strategies are adopted between bio-sensors and Gateway (GW). For the proposed work, the cooperation of two nodes A and B are considered in the Figure 6.

B. SIMULATION SETTING

The initial residual energy of WABN is considered 5 Joules, and the communication range of the proposed WBAN is considered between 2 → 15 meters. For the proposed setup *IEEE* 802.15.6 wireless standard is used, and for data forwarding, star topology is used as shown in Figure 6. Bio-sensors related to WABN are considered as a group or clustered. Furthermore, the energy consumed during the simulation is formulated as;

$$E_{rem} = E_{total} - (E_t + E_r + E_l) \tag{9}$$

In equation 9, E and E_{total} is the total initial energy, while E_t and E_r are energy, consumption during transmission and receiving of data packets. Similarly, E_l is the energy consumption during body fading and interference in WBAN communication. Moreover, in the WBAN environment, two types of radio transceivers are generally used, i.e., Nordic ($nRF2401A$) and Chipcon (CC2420) [35]. But according to our proposed model, we preferred to use the Nordic ($nRF2401A$) transceiver because it is a low power transceiver.We considered the simulation time

TABLE 2. Simulation parameters.

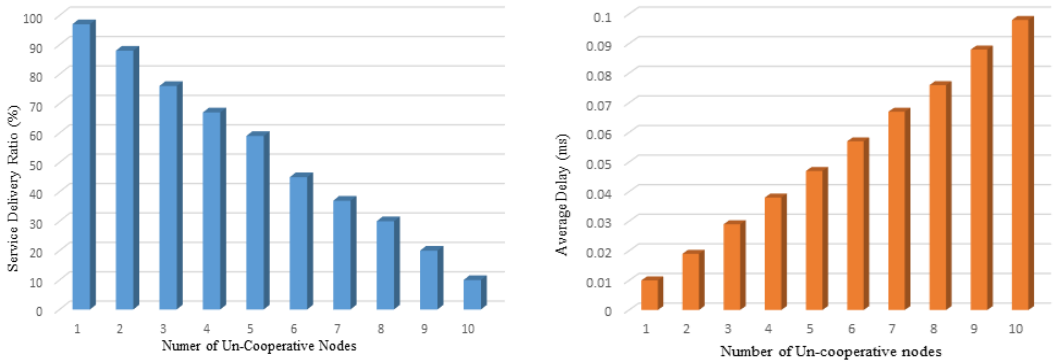
Parameters	Value
Simulation area	$15m \times 15m$
Initial residual Energy	5 J
Sensors/Devices	$11(10Bio-Sensor, 1GW)$
Transmitting Energy ETX	$16.7nJ/bit$
Receiving Energy ERX	$36.1nJ/bit$
Data Aggregation Energy (EDA)	$5nJ/bit$
Packet size (b)	Dynamic
Agent trace	On
Simulation time	$50sec$
Node Deployment	Fixed

50 seconds for the proposed scheme. Table 2 Simulation Parameters demonstrates the list of parameters used for trust-based energy-efficient cooperative communication in WBAN. Furthermore, for mobility support, we used a group-based mobility model, according to which each WBAN is considered as a group or cluster of bio-sensors.

In Figure 6, there are ten bio-sensors in which two are considered as cooperating nodes, and remaining are non-cooperating nodes. All bio-sensors are communicating their vital sign through the gateway to the medical server for remote patient monitoring. With the increase in the number of uncooperative nodes, the average service delivery decreases while the average service delay becomes increases.

C. PERFORMANCE ANALYSIS OF TRUST-BASED ERCS

This sub-section focuses on the performance analysis of the proposed trust-based cooperative strategy for remote patient monitoring in WBAN. The first and perhaps the most import analysis of the proposed scheme is when all the bio-sensor nodes are non-cooperative, which have to condense service delivery ratio. Through cooperative strategy,



(a) Service Delivery Probability (b) Average Delay

FIGURE 7. Service delivery probability and average delay vs number of uncooperative nodes.

all or some nodes perform cooperation among themselves, which maximized average service delivery. Additionally, the average service delay becomes minimized significantly. Average service delivery is measured in percentage, and average service delay is measured in millisecond (*ms*).

1) ***Experiment 1 – Average Service Delivery and Average Delay for Un-Cooperative Nodes:-*** In Figure 7, the service delivery probability and average service delay for uncooperative bio-sensors nodes are presented as shown. Two parameters average service delivery ratio and average delay are analyzed on the base of un-cooperative bio-sensors. The cooperative bio-sensors are not considered in this experiment. In the traditional non-cooperative approach, the performance is linearly increased, suitable only for a limited network.

   As can see in Figure 7a, with the increase of the number of un-cooperative nodes, the service delivery probability becomes decreases. Moreover, increasing the number of un-cooperative nodes, the average delay becomes increase, as shown in Figure 7b.

2) ***Experiment 2 - Average Service Delivery and Average Delay for Un-Cooperative VS Cooperative Nodes:-*** In this section, cooperative nodes are compared with un-cooperative nodes concerning average service delivery and average delay for the proposed Trust-Based ERCS, as shown in Figures 8a & 8b. It has clear from the results that the cooperative communication approach has improved outcomes compared to the non-cooperative method. That is due to unwanted communication is avoided.

   Figure 8a & 8b, demonstrates the average service delivery ratio and average delay encounter while increasing the number of cooperative and un-cooperative nodes in communication. It is clear from the result that cooperative communication increases the service delivery ratio as 96%, with 10% uncooperative nodes. Similarly, the average delay becomes decreases as 30% as compared to un-cooperative nodes with the presence of 10% un-cooperative nodes. The experiment is conducted on a maximum of up to 10 nodes for the more generalized result.

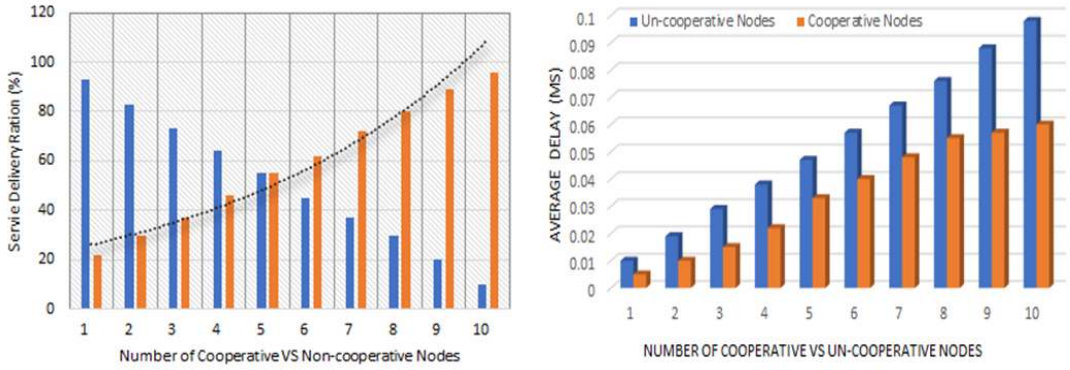
3) ***Experiment 3 - Trust value, Energy Consumption, and Reliability using Cooperative Nodes:-*** In this section, we compared the DTEM [9], Trust-Based IDCA [14], and the proposed Trust-Based ERCS scheme for trust value, reliability improvement, and consumption. Figure 9 demonstrates the trust ratio between the proposed and state of the art relevant schemes. It's clear from the graph that the trust ratio using cooperative strategy in the proposed scheme maximized the trust ratio significantly due efficient use of cooperative nodes and trust value generation at the initial stage. Using a cooperative approach, a 95% trust ratio is achieved.

   By increase the trust ratio, the improved reliability is achieved using the proposed cooperative strategy for trust-based remote patient management in WBAN, as shown in Figure 10. For a maximum of ten cooperative nodes, the reliability level is 91% due to the trust generated by cooperative bio-sensors.

   In Figure 11, the energy consumption comparison is demonstrated by using different cooperative nodes. From the yielded graph, it is concluded that the proposed scheme outperformed the benchmark schemes, i.e., IDCA [14] and DTEM [9]. A maximum ten node cooperative, the energy consumption of the proposed trust-based ERCS, is 3.7 Joule, while DTEM has energy consumption 4.7 Joule.

D. RANK BASED EVALUATION OF PERFORMANCE MATRICES

In this section, we performed the rank-based performance evaluation of the proposed scheme compared with state-of-the-art relevant schemes using fuzzy logic. Which is an efficient method and carry great results for comparisons of the performances of different schemes [36]. Moreover, the evaluation of trust management using fuzzy logic is not



(a) Service Delivery Ratio **(b)** Average delay

FIGURE 8. Service delivery ratio and average delay for cooperative vs un-cooperative nodes.

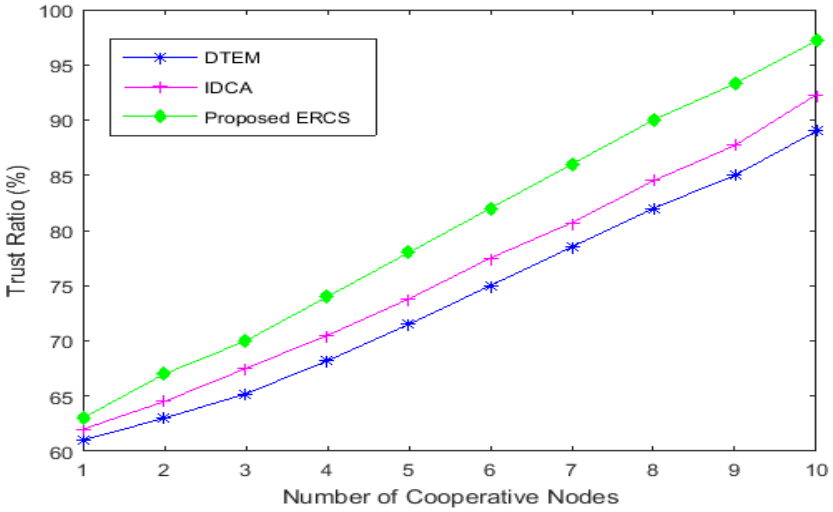


FIGURE 9. Trust ratio vs cooperative nodes.

used before. We have demonstrated performance metrics of DTEM, FATD, Trust Chain, IDCA, and the proposed Trust-Based ERCS schemes, as shown in Table 3. In this table, trust value (TV) is derived according to equation 6. Similarly, the reliability ratio also depends on the trust ratio of WBAN communication. If the trust ratio increases, the reliability ratio increase ultimately, as showed in Table 3. Accuracy of data delivery $D(M)$ is expressed in terms of expected error between the actual value of bio-sensor cooperation and average normal estimated value (M). Hence we adopt the mean square error among S and $S(M)$ for the accuracy of data delivery calculated for the given scenario as given as,

$$D_A\ (M) = 1 - \frac{D\,(M)}{E\left[(\text{S-S}\,(M))^2\right]} \tag{10}$$

Moreover, the service delivery ratio and delay are calculated in percentage according to experiment 1&2 of the experimental results, as shown in figure 7 and 8. The energy consumption is calculated according to equation 9 mentioned in the performance evaluation section IV and demonstrated in figure 11 calculated according to the formula throughput $= \frac{\text{number of bytes}}{\text{average time}}$. For the proposed scheme, the formula for throughput is given in equation 11 below.

$$Th = B \cdot log_2\left(1 + \frac{S}{N}\right) \tag{11}$$

For the proposed MIMO system WBAN, in the given equation, B represents bandwidth and $(\frac{S}{N})$ represent the signal to noise ratio. The capacity of throughput increase linearly according to the formula. Besides, confidentiality is measured between the range of values 0 to 1, as shown in the table, while privacy and scalability are measures according to and comparison with other research work.

In this research work, a fuzzy logic-based method named Evaluation Based on Distance from Average Solution (EDAS) has been used for the performance evaluation of ranking of the proposed scheme with the stat of the art relevant schemes which are mention above. The various performance metrics identified in the literature review are

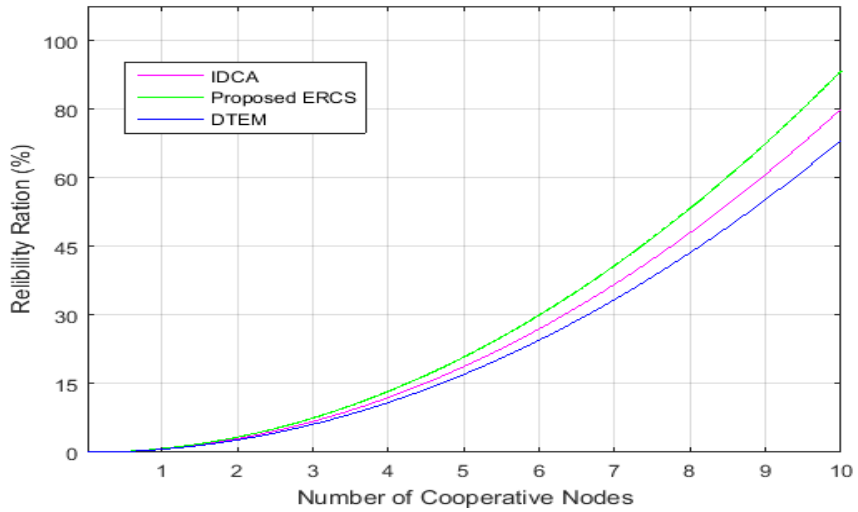


FIGURE 10. Reliability ratio vs number of cooperative nodes.

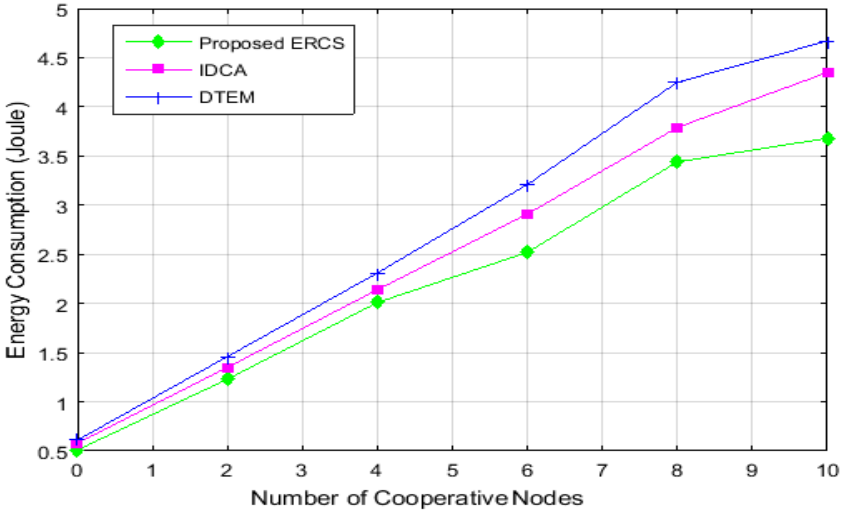


FIGURE 11. Energy consumption vs number of cooperative nodes.

compared for the proposed Trust-based ERCS with available benchmark schemes. Furthermore, in this evaluation, the cross EDAS method is used for the accumulation of cross-efficient values of various parameters, five different schemes, including the proposed one. The aggregate of Assessment Scores denoted by (λ) can be measured for ranking of proposed, and other relevant schemes for the calculation of the positive distance denoted as ($P_{\Im}$) from average solution and negative distance denoted as ($N_{\Im}$) from an ordinary solution.

In Table 3, the performance matrices of different schemes are considered.

Step 1^{st}:- Calculate the solution of the average value (ψ) of all matrices in equation 12;

$$(\psi) = \left[\psi_{\beta}\right]_{1\times\delta} \tag{12}$$

where,

$$(\psi) = \frac{\sum_{i=1}^{x} X_{\alpha\beta}}{x} \tag{13}$$

The above step defines the performance matrices as criteria of various state of the art approaches. Furthermore, the aggregate calculation values of equations 12 and 13 can be acquired as the average value (ψ) for every calculated value against each given matrices, as shown in Table 4.

Step 2^{nd}:- In this step of the EDAS based positive distances from taking the average of ($P_{\Im}$) in equations 14, 15 and 16 as given below:

$$P_{\Im} = \left[(P_{\Im})_{\alpha\beta}\right]_{\delta\times\delta} \tag{14}$$

If the case of β th criterion is more favorable then

$$(P_{\Im})_{\alpha\beta} = \frac{Maximum\left(0, \left(A_{V_{\beta}} - X_{\alpha\beta}\right)\right)}{A_{V_{\beta}}} \tag{15}$$

TABLE 3. Performance metrics of the various schemes.

Techniques	Performance metrics									
	Trust Value (TV)	Reliability (%)	Accuracy D(M)	Service Delivery ratio(%)	Throughput (bps)	Energy Cost (Joule)	Average Delay (ms)	Privacy (No/Yes)	Confidentiality (0<=CR<=1)	Scalability (No/Yes)
DTEM [9]	0.78	0.65	0.82	80	0.75	4.55	0.096	0	0.52	0
FATD [27]	0.82	0.70	0.85	84	0.81	4.40	0.084	0	0	0
Trust Chain [13]	0.86	0.74	0.87	89	0.86	4.25	0.075	1	0.54	1
IDCA [14]	0.90	0.80	0.89	94	0.91	4.17	0.066	1	0.19	0
Proposed ERCS	0.95	0.86	0.93	97	0.96	3.70	0.059	1	1	1

TABLE 4. Cross-efficient values.

Techniques	Performance metrics									
	Trust Value (TV)	Reliability (%)	Accuracy D(M)	Service Delivery ratio(%)	Throughput (bps)	Energy Cost (Joule)	Average Delay (ms)	Privacy (No/Yes)	Confidentiality (0<=CR<=1)	Scalability (No/Yes)
DTEM [9]	0.78	0.65	0.82	80	0.75	4.55	0.096	0	0.52	0
FATD [27]	0.82	0.7	0.85	84	0.81	4.4	0.084	0	0	0
Trust Chain [13]	0.86	0.74	0.87	89	0.86	4.25	0.075	1	0.54	1
IDCA [14]	0.9	0.8	0.89	94	0.91	4.17	0.066	1	0.19	0
Proposed ERCS	0.95	0.86	0.93	97	0.96	3.7	0.059	1	1	1
ψ_β	0.391	0.340	0.396	40.363	0.39	1.915	0.035	0.273	0.205	0.182

and if less favorable then the above-given equation become as:

$$(P_\Im)_{\alpha\beta} = \frac{Maximum\left(0, \left(X_{\alpha\beta} - A_{V_\beta}\right)\right)}{A_{V_\beta}} \tag{16}$$

In the above equations $(P_\Im)_{\alpha\beta}$ denoted the positive distance of βth rated algorithms from the average value concerning αth rating performance parameters, respectively. The calculated results can be reflected in the below Table 5:

Step 3^{rd}:- In this step of the EDAS calculates the negative $(N_\Im)$ distances from the average of $(N_\Im)$ using equations 17, 18 and 19 as demonstrated as below:

$$(N_\Im) = \left[(N_\Im)_{\alpha\beta}\right]_{\delta\times\delta} \tag{17}$$

If the βth criterion is the more favorable then

$$(N_\Im)_{\alpha\beta} = \frac{Maximum\left(0, \left(A_{V_\beta} - X_{\alpha\beta}\right)\right)}{A_{V_\beta}} \tag{18}$$

and if less desirable then the given above equation become:

$$(N_\Im)_{\alpha\beta} = \frac{Maximum\left(0, \left(X_{\alpha\beta} - A_{V_\beta}\right)\right)}{A_{V_\beta}} \tag{19}$$

In equations $(N_\Im)_{\alpha\beta}$ denoted the negative distance of βth rated algorithms from the average value concerning αth rating performance parameters, respectively. The results reflect in Table 6 below:

TABLE 5. Analysis results of average ($P_{\Im}$).

Techniques	Performance metrics									
	Trust Value (TV)	Reliability (%)	Accuracy D(M)	Service Delivery ratio(%)	Throughput (bps)	Energy Cost (Joule)	Average Delay (ms)	Privacy (No/Yes)	Confidentiality (0<=CR<=1)	Scalability (No/Yes)
DTEM [9]	0	0	0	0	0	0	0	1	1.542222	0
FATD [27]	0	0	0	0	0	0	0	1	0	0
Trust Chain [13]	0	0	0	0	0	0	0	0	1.64	4.5
IDCA [14]	0	0	0	0	0	0	0	0	0	0
Proposed ERCS	0	0	0	0	0	0	0	0	3.888889	4.5

TABLE 6. Analysis results of average ($N_{\Im}$).

Techniques	Performance metrices									
	Trust Value (TV)	Reliability (%)	Accuracy D(M)	Service Delivery ratio(%)	Throughput (bps)	Energy Cost (Joule)	Average Delay (ms)	Privacy (No/Yes)	Confidentiality (0<=CR<=1)	Scalability (No/Yes)
DTEM [9]	0.9907	0.9066	1.0688	0.9819	0.9230	1.3754	1.7789	0	0	1
FATD [27]	1.0928	1.0533	1.1444	1.0810	1.0769	1.2971	1.4315	0	1	1
Trust Chain [13]	1.1948	1.1706	1.1949	1.2049	1.2051	1.2187	1.1710	2.6666	0	0
IDCA [14]	1.2969	1.3466	1.2454	1.3288	1.3333	1.1770	0.9105	2.666	0.0711	1
Proposed ERCS	1.4245	1.5226	1.3463	1.4031	1.4615	0.9316	0.7078	2.6666	0	0

Step 4^{th}:- In this step weighted sum of positive ($P_{\Im}$) for the Rated Algorithms, as shown in Table 7 below:

$$(SP_{\Im})_{\alpha} = \sum_{\beta=1}^{x} y_{\beta}(P_{\Im})_{\alpha\beta} \tag{20}$$

Step 5^{th}:- In this step weighted sum of $(N_{\Im})_{\alpha\beta}$ for the Rated Algorithms is shown in Table 8 as below in equation 21:

$$(SN_{\Im})_{\alpha} = \sum_{\beta=1}^{x} y_{\beta}\,(N_{\Im})_{\alpha\beta} \tag{21}$$

The result reflected in the table 8 below:

Step 6^{th}:- In this step, the calculated scores based on of $(SP_{\Im})_{\alpha}$ and $(SN_{\Im})_{\alpha}$ values which are based on a given rated method are stated in the following equations 22 and 23:

$$N\,(SP_{\Im})_{\alpha} = \frac{(SP_{\Im})_{\alpha}}{\text{maximum}_{\alpha}\,((SP_{\Im})_{\alpha})} \tag{22}$$

$$N\,(SN_{\Im})_{\alpha} = 1 - \frac{(SN_{\Im})_{\alpha}}{\text{maximum}_{\alpha}\,((SN_{\Im})_{\alpha})} \tag{23}$$

Step 7^{th}:- In this step, calculates the scores based on $N(SP_{\Im})_{\alpha}$ and $N(SN_{\Im})_{\alpha}$ values which are based on the appraisal score *(AS)*which is equal to (λ) for the Rated method given in equation 24:

$$\lambda_{\alpha} = \frac{1}{2}\,(N\,(SP_{\Im})_{\alpha} - N\,(SN_{\Im})_{\alpha}) \tag{24}$$

where $0 \leq \lambda_{\alpha} \leq 1$.

The outcome of (λ) is determined by the aggregate score of $NSP_{\Im}$ and $NSN_{\Im}$ values.

TABLE 7. Analysis results of the aggregate $(SP_{\Im})_{\alpha}$.

Criteria (W)	0.2357	0.1814	0.1228	0.1186	0.0731	0.0429	0.0427	0.0856	0.0491	0.0476	$(SP_{\Im})_{\alpha}$
Techniques	Performance metrics										
	Trust Value (TV)	Reliability (%)	Accuracy D(M)	Service Delivery ratio(%)	Throughput (bps)	Energy Cost (Joule)	Average Delay (ms)	Privacy (No/Yes)	Confidentiality (0<=CR<=1)	Scalability (No/Yes)	
DTEM [9]	0	0	0	0	0	0	0	0.0856	0.0757	0	0.1613
FATD [27]	0	0	0	0	0	0	0	0.0856	0	0	0.0856
Trust Chain [13]	0	0	0	0	0	0	0	0	0.0805	0.2144	0.2950
IDCA [14]	0	0	0	0	0	0	0	0	0	0	0
Proposed ERCS	0	0	0	0	0	0	0	0	0.1910	0.2144	0.4055

TABLE 8. Analysis results of the aggregate $(SN_{\Im})_{\alpha}$.

Criteria(W)	0.2357	0.1814	0.1228	0.1186	0.0731	0.0429	0.0427	0.0856	0.0491	0.0476	$(SN_{\Im})_{\alpha}$
Techniques	Performance metrics										
	Trust Value (TV)	Reliability (%)	Accuracy D(M)	Service Delivery ratio(%)	Throughput (bps)	Energy Cost (Joule)	Average Delay (ms)	Privacy (No/Yes)	Confidentiality (0<=CR<=1)	Scalability (No/Yes)	
DTEM [9]	0.2335	0.1645	0.1313	0.1165	0.0674	0.0590	0.0760	0	0	0.0476	0.8962
FATD [27]	0.2575	0.1911	0.1406	0.1282	0.0787	0.0557	0.0612	0	0.0491	0.0476	1.0101
Trust Chain [13]	0.2816	0.2124	0.1468	0.1429	0.0880	0.0523	0.0500	0.2283	0	0	1.2028
IDCA [14]	0.3057	0.2443	0.1530	0.1577	0.0974	0.0505	0.0389	0.2283	0.0034	0.0476	1.3272
Proposed ERCS	0.3358	0.2763	0.1654	0.1665	0.1068	0.0400	0.0302	0.2283	0	0	1.3495

TABLE 9. Analysis result of five state of the art schemes.

Techniques	$(SP_{\Im})_{\alpha}$	$(SN_{\Im})_{\alpha}$	$N(SP_{\Im})_{\alpha}$	$N(SN_{\Im})_{\alpha}$	λ_{α}	Ranking
DTEM [9]	0.1613	0.8962	0.3979	0.3358	0.3669	**3**
FATD [27]	0.0856	1.0101	0.2111	0.2514	0.2312	**4**
Trust Chain [13]	0.2950	1.2028	0.7275	0.1087	0.4181	**2**
IDCA [14]	0	1.3272	0	0.0164	0.0082	**5**
Proposed ERCS	0.4055	1.3495	1	0	0.5	**1**

Step 8^{th}:- In this step activity related to the measurement of the appraisal scores (λ) in terms of decreasing order and then determine the ranking of Rated methods is stated. From the output result, it is clear that best ranking schemes have a higher (λ) compare to other related schemes. So, in the below Table 9, the proposed algorithm has the highest (λ) as shown. Therefore, the final calculated ranked result is demonstrated in the table 9 below.

From the output fuzzy logic EDAS-based ranking, we concluded that the proposed scheme outperforms the available state of the art schemes available in the research domain. From the output table, the proposed scheme is on top based on the performance metrics. While Trust Chain [13] and DTEM [9] are on 2^{nd} and 3^{rd} ranked and so forth.

V. CONCLUSION AND FUTURE WORK

In a fast few years, WBAN-based technologies open a new way for remote healthcare treatment. WBAN is a very interesting technology consists of a constrained network formed from bio-sensors devices. Bio-sensors sensed vital signs and sent them to the medical server for principal medical analysis. The data manipulation is very critical and needs trust-based provision in WBAN remote healthcare applications. Therefore, trust-based remote patient monitoring and the energy-efficient scheme have been proposed in this research work to increase trust and reliability. Focus is on trust-based medical services to perform healthcare activities at the remote side to healthcare users at the doorstep. The proposed work is a novel healthcare idea in WABNs. First, a trust-based model for creating trust values is proposed. Then based on the trust value, a trust-based cooperative communication system is developed. And finally, for reliability and privacy insurance, a cryptographic based solution has been proposed. The proposed solution tried to improve the error-free reliable service to healthcare users. Furthermore, the proposed scheme improved trust level and reliability with minimum energy consumption. Moreover, the average service delay of communication done for critical data communication is minimized. A fuzzy logic EDAS-based ranking indicates that the proposed scheme outperforms the available benchmark schemes.

In the future, the proposed scheme will be implemented on the software testbed. Furthermore, a more generalized healthcare architecture will be proposed using IoT Technology.

REFERENCES

[1] S. Ozawa and P. Sripad, "How do you measure trust in the health system? A systematic review of the literature," *Social Sci. Med.*, vol. 91, pp. 10–14, Aug. 2013.
[2] D. M. Barakah and M. Ammad-Uddin, "A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture," in *Proc. 3rd Int. Conf. Intell. Syst. Model. Simul.*, Feb. 2012, pp. 214–219.
[3] G. R. Kanagachidambaresan and A. Chitra, "Fail safe fault tolerant mechanism for wireless body sensor network (WBSN)," *Wireless Pers. Commun.*, vol. 80, no. 1, pp. 247–260, Jan. 2015.
[4] R. Maheswar, G. Kanagachidambaresan, R. Jayaparvathy, and S. M. Thampi, *Body Area Network Challenges and Solutions*. Cham, Switzerland: Springer, 2018.
[5] P. Abouzar, K. Shafiee, D. G. Michelson, and V. C. M. Leung, "Action-based scheduling technique for 802.15.4/ZigBee wireless body area networks," in *Proc. IEEE 22nd Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2011, pp. 2188–2192.
[6] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Netw.*, vol. 17, no. 1, pp. 1–18, Jan. 2011.
[7] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, "Wireless sensor networks for healthcare," *Proc. IEEE*, vol. 98, no. 11, pp. 1947–1960, Nov. 2010.
[8] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, "Trust and reputation management in healthcare systems: Taxonomy, requirements and open issues," *IEEE Access*, vol. 6, pp. 17246–17263, 2018.
[9] Z. Ye, T. Wen, Z. Liu, X. Song, and C. Fu, "An efficient dynamic trust evaluation model for wireless sensor networks," *J. Sensors*, vol. 2017, pp. 1–16, Oct. 2017.
[10] M. Sen and G. Mahapatra, "Secure remote patient monitoring with location-based services," in *Emerging Technologies in Data Mining and Information Security*. Springer, 2019, pp. 715–726.
[11] K. G. Mkongwa, Q. Liu, C. Zhang, and F. A. Siddiqui, "Reliability and quality of service issues in wireless body area networks: A survey," *Int. J. Signal Process. Syst.*, vol. 7, no. 1, pp. 26–31, Mar. 2019.
[12] G. Mehmood, M. Z. Khan, H. U. Rahman, and S. Abbas, "An efficient and secure session key establishment scheme for health-care applications in wireless body area networks," *J. Eng. Appl. Sci.*, vol. 37, no. 1, pp. 9–18, 2018.
[13] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee, "TrustChain: A privacy preserving blockchain with edge computing," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–17, Jul. 2019.
[14] D. K. Anguraj and S. Smys, "Trust-based intrusion detection and clustering approach for wireless body area networks," *Wireless Pers. Commun.*, vol. 104, no. 1, pp. 1–20, Jan. 2019.
[15] M. M. Alqhatani and M. G. M. Mostafa, "Trust modeling in wireless sensor networks: State of the art," *J. Inf. Secur. Cybercrimes Res.*, vol. 1, no. 1, pp. 74–90, 2018.
[16] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345–1360, Jan. 2011.
[17] A. Meharouech, J. Elias, and A. Mehaoua, "Moving towards body-to-body sensor networks for ubiquitous applications: A survey," *J. Sensor Actuator Netw.*, vol. 8, no. 2, p. 27, May 2019.
[18] H.-N. Li, L. Ren, Z.-G. Jia, T.-H. Yi, and D.-S. Li, "State-of-the-art in structural health monitoring of large and complex civil infrastructures," *J. Civil Struct. Health Monitor.*, vol. 6, no. 1, pp. 3–16, Feb. 2016.
[19] L. P. Malasinghe, N. Ramzan, and K. Dahal, "Remote patient monitoring: A comprehensive study," *J. Ambient Intell. Hum. Comput.*, vol. 10, no. 1, pp. 57–76, Jan. 2019.
[20] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 4, pp. 623–632, Jul. 2012.
[21] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 3, p. 15, May 2008.
[22] L. Gomez, A. Laube, and A. Sorniotti, "Trustworthiness assessment of wireless sensor data for business applications," in *Proc. Int. Conf. Adv. Inf. Netw. Appl.*, 2009, pp. 355–362.
[23] D. Hui-Hui, G. Ya-Jun, Y. Zhong-Qiang, and C. Hao, "A wireless sensor networks based on multi-angle trust of node," in *Proc. Int. Forum Inf. Technol. Appl.*, 2009, pp. 28–31.
[24] F. Kazmi, M. A. Khan, A. Saeed, N. A. Saqib, and M. Abbas, "Evaluation of trust management approaches in wireless sensor networks," in *Proc. 15th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Jan. 2018, pp. 870–875.
[25] H. Rathore, V. Badarla, and K. J. George, "Sociopsychological trust model for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 62, pp. 75–87, Feb. 2016.
[26] R. K. Chahal, N. Kumar, and S. Batra, "Trust management in social Internet of Things: A taxonomy, open issues, and challenges," *Comput. Commun.*, vol. 150, pp. 13–46, Jan. 2020.
[27] A. Chitra and G. Kanagachidambaresan, "Fault aware trust determination algorithm for wireless body sensor network (WBSN)," in *Proc. 1st Int. Conf. Smart Syst., Innov. Comput.*, 2018, pp. 469–476.
[28] A. R. Bhangwar, P. Kumar, A. Ahmed, and M. I. Channa, "Trust and thermal aware routing protocol (TTRP) for wireless body area networks," *Wireless Pers. Commun.*, vol. 97, no. 1, pp. 349–364, Nov. 2017.
[29] X. Liang and I. Balasingham, "A QoS-aware routing service framework for biomedical sensor networks," in *Proc. 4th Int. Symp. Wireless Commun. Syst.*, Oct. 2007, pp. 342–345.
[30] T. van Deursen, P. Koster, and M. Petković, "Hedaquin: A reputation-based health data quality indicator," *Electron. Notes Theor. Comput. Sci.*, vol. 197, no. 2, pp. 159–167, Feb. 2008.
[31] H. Zemrane, Y. Baddi, and A. Hasbi, "Ehealth smart application of WSN on WWAN," in *Proc. 2nd Int. Conf. Netw., Inf. Syst. Secur. (NISS)*, 2019, p. 26.

[32] Y. Wang, M. Zhang, and W. Shu, "An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 145, Dec. 2018.
[33] B. M. C. Silva, J. J. P. C. Rodrigues, F. Canelo, I. M. C. Lopes, and J. Lloret, "Towards a cooperative security system for mobile-health applications," *Electron. Commerce Res.*, vol. 19, no. 3, pp. 629–654, Sep. 2019.
[34] B. M. C. Silva, J. J. P. C. Rodrigues, I. M. C. Lopes, T. M. F. Machado, and L. Zhou, "A novel cooperation strategy for mobile health applications," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 28–36, Sep. 2013.
[35] G. Mehmood, M. Z. Khan, S. Abbas, M. Faisal, and H. U. Rahman, "An energy-efficient and cooperative fault-tolerant communication approach for wireless body area network," *IEEE Access*, vol. 8, pp. 69134–69147, 2020.
[36] N. A. Malik and M. Rai, "Enhanced secure and efficient key management algorithm and fuzzy with trust management for MANETs," in *Proc. Int. Conf. Innov. Comput. Commun. (ICICC)*, 2020.

GULZAR MEHMOOD received the B.S. degree in computer science from the University of Malakand, Pakistan, and the master's degree in computer science from International Islamic University, Islamabad, Pakistan. He is currently pursuing the Ph.D. degree in computer science (wireless body area networks) with the Department of Computer Science and Information Technology, University of Malakand. His research interests include wireless body area networks and wireless sensor networks with a focus on fault-tolerance, reliability, and security.

MUHAMMAD ZAHID KHAN received the B.C.S. degree in computer science from the University of Peshawar, Pakistan, in 2003, and the Ph.D. degree from the School of Computing and Mathematical Sciences, Liverpool John Moores University, U.K., in 2013. He has been an Assistant Professor with the Department of Computer and Information Technology, University of Malakand, Pakistan, since 2005, where he is currently with the Network Systems and Security Research Group. He is also a Higher Education Commission's Pakistan approved Supervisor. His current research interests include wireless sensor networks, fault management, and the Internet of Things.

ABDUL WAHEED received the master's degree in computer sciences from the Department of Information Technology, Hazara University, Mansehra, in 2014, where he is currently pursuing the Ph.D. in computer sciences. He is the member of the Crypto-Net Research Group, Hazara University. He has completed his Ph.D. Research with the NetLab-INMC under the School of Electrical and Computer Engineering (ECE), Seoul National University (SNU), South Korea, in 2019, under the HEC Research Program. He is also serving as a Lecturer with the Department of Computer Sciences, IQRA National University, Peshawar. He has numerous publications in international conferences and journals. His research interests include information security, secure and smart cryptography, heterogeneous communications within the Internet of Things (IoT), mobile ad hoc networks (MANETs), wireless sensor networks (WSNs) security, and fuzzy logic-based decision making theory.

MAHDI ZAREEI (Member, IEEE) received the M.Sc. degree in computer network from the University of Science, Malaysia, in 2011, and the Ph.D. degree from the Communication Systems and Networks Research Group, Malaysia–Japan International Institute of Technology, University of Technology, Malaysia, in 2016. In 2017, he joined the School of Engineering and Sciences, Tecnológico de Monterrey, as a Postdoctoral Fellow, where he started working as a Research Professor, in 2019. His research interests include wireless sensor and ad hoc networks, energy harvesting sensors, information security, and machine learning. He is a member of the Mexican National Researchers System (Level I). He is also serving as an Associate Editor for the IEEE Access and *Ad Hoc and Sensor Wireless Networks Journals*.

EHAB MAHMOUD MOHAMED (Member, IEEE) received the B.E. and M.E. degree in electrical engineering from South Valley University, Egypt, in 2001 and 2006, respectively, and the Ph.D. degree in information science and electrical engineering from Kyushu University, Japan, in 2012. From 2013 to 2016, he was a Specially Appointed Researcher with Osaka University, Japan. Since 2017, he has been an Associate Professor with Aswan University, Egypt. He has been an Associate Professor with Prince Sattam Bin Abdulaziz University, Saudi Arabia, since 2019. He is the General Chair of the IEEE ITEMS 2016 and the IEEE ISWC 2018. He is a Technical Committee Member in many international conferences and a Reviewer in many international conferences, journals, and transactions. His current research interests include 5G, B5G and 6G networks, cognitive radio networks, millimeter wave transmissions, Li-Fi technology, MIMO systems, and underwater communication.