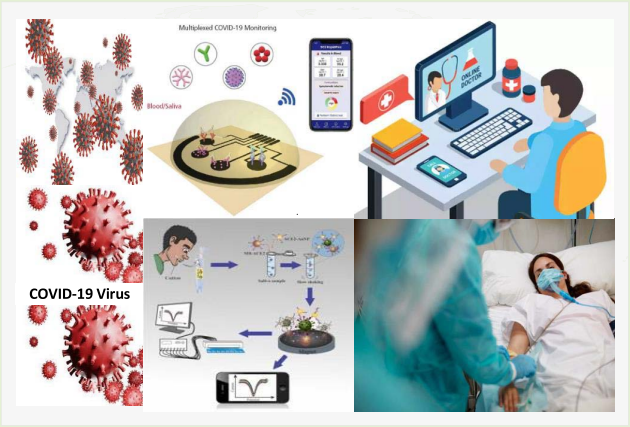
QoS Review: Smart Sensing in Wake of COVID-19, Current Trends and Specifications With Future Research Directions

Muhammad Adil, *Graduate Student Member, IEEE*, Hani Alshahrani, *Member, IEEE*, Adel Rajab, *Member, IEEE*, Asadullah Shaikh, *Member, IEEE*, Houbing Song, *Senior Member, IEEE*, and Ahmed Farouk, *Member, IEEE*

***Abstract*—Smart Sensing has shown notable contributions in the healthcare industry and revamps immense advancement. With this, the present smart sensing applications such as the Internet of Medical Things (IoMT) applications are elongated in the COVID-19 outbreak to facilitate the victims and alleviate the extensive contamination frequency of this pathogenic virus. Although, the existing IoMT applications are utilized productively in this pandemic, but somehow, the Quality of Service (QoS) metrics are overlooked, which is the basic need of these applications followed by patients, physicians, nursing staff, etc. In this review article, we will give a comprehensive assessment of the QoS of IoMT applications used in this pandemic from 2019 to 2021 to identify their requirements and current challenges by taking into account various network components and communication metrics. To claim the contribution of this work, we explored layer-wise QoS challenges in the existing literature to identify particular requirements, and set the footprint for future research. Finally, we compared each section with the existing review articles to acknowledge the uniqueness of this work followed by the answer of a question why this survey paper is needed in the presence of current state-of-the-art review papers.**



***Index Terms*— Smart sensing, QoS of IoMT, IoMT applications in COVID-19, QoS requirements, QoS challenges, routing protocols.**

I. Introduction

COVID-19 is an infectious and transmittable virus that can provoke penetrating respiratory syndrome in humans [1]. This virus has been spread all over the globe and infected 437,792,328 individuals, followed by 5,978,217 fatalities and 369,500,307 recovered cases by March 1, 2022 [2]. The research community believes that COVID-19 infection rates can be reduced with the help of efficient use of technology such as the Internet of Medical Things (IoMT). In recent years, this technology has attained coercing research ground in the healthcare sector to detect different diseases followed by the assessment, monitoring, and prescription of patients [3]. The literature contains, various kinds of artificial intelligence-based algorithms or machine learning algorithms, and deep learning (DL) algorithms that had revealed incredible results in terms of accuracy to detect and assess patient health related issues [4]. Utilizing machine learning and artificial techniques, the current contemporaries of IoT devices can be extended freely at the client-side to evaluate, accumulate and process data in the network. Following this discussion, IoT applications have been used in many healthcare domains, such as seizure detection [5], physical therapy [6], social distancing monitoring [7], and pandemic management [8], etc.

Patient wearable IoT devices revealed remarkable results in the healthcare domain and the research community relentlessly working to extend their applicability in different healthcare applications. Recently, the existing healthcare IoT applications have been utilized in the COVID-19 pandemic to addressed various problems associated with patients, but the urgent

Manuscript received 4 March 2022; accepted 21 April 2022. Date of publication 25 April 2022; date of current version 12 January 2023. This work was supported in part by the National Science Foundation under Grant 2150213. The associate editor coordinating the review of this article and approving it for publication was Dr. Uttam Ghosh. *(Corresponding author: Muhammad Adil.)*

Muhammad Adil is with the Global Foundation for Cyber Studies and Research, Washington, DC 20015 USA (e-mail: muhammad.adil@ieee.org).

Hani Alshahrani, Adel Rajab, and Asadullah Shaikh are with the College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia (e-mail: hmalshahrani@nu.edu.sa; adrajab@nu.edu.sa; asshaikh@nu.edu.sa).

Houbing Song is with the Department of Electrical Engineering and Computer Science, Embry–Riddle Aeronautical University, Daytona Beach, FL 32114 USA (e-mail: h.song@ieee.org).

Ahmed Farouk is with the Department of Computer Science, Faculty of Computers and Artificial Intelligence, South Valley University, Hurghada 84511, Egypt (e-mail: ahmed.farouk@sci.svu.edu.eg).

Digital Object Identifier 10.1109/JSEN.2022.3170055

expansion of these applications ignored various things such as QoS, load balancing, and security, etc., which is the basic needs of these applications. Following this, it has been noted that the existing healthcare IoT applications are extended and utilized from the perspective of the COVID-19 pandemic without considering the QoS challenges and requirements. Therefore, in this paper, we have emphasized to attract the attention of the research community and healthcare stakeholders toward this valuable issue to identify the present problems in these applications to improve the QoS metrics.

To explore the role of IoT technology utilization in the healthcare domain particularly in the context of COVID-19 infectious tracking and control. Firstly, we will review the existing state-of-the-art schemes concerning the architectures, protocols, platforms, and applications in the context of QoS metrics to identify the present challenges and requirements of these applications. In the next phase, we will follow-up these challenges and requirements to pave the future research directions that could be useful for them to maintain high QoS metrics in the operational network. To this point, we inaugurate the following contributions in this review paper:

1) In the first step, we will go through the current review articles related to the QoS of IoMT, and particularly those used in the COVID-19 pandemic. Furthermore, we will examine the current QoS techniques used in these networks to determine the present intricacies and obligations of present literature.
2) Next, we will confront every section with competing review articles in terms of recognized challenges accompanied by distinct demands to confess the uniqueness of this work.
3) Thereafter, we will follow the highlighted dares and calls to circumscribe a potential research direction in this domain. After that, we will compare our future work section with comparative articles to guarantee the superiority, novelty and uniqueness of this paper.
4) Considering the highlighted requirements, challenges, and future research opportunities, we have added table III, IV, and V in the paper for comparative analysis to certify the originality of this work and answer the question why this survey paper is needed in the presence of existing review articles.

The rest of the paper is partitioned as below: Introduction to QoS in IoT applications and particularly in the healthcare domain is over-viewed in Section II, whereas Section III highlights the open challenges associated with these networks. Future research opportunities are enlisted and explained in Section IV, while Section V compiles and concludes the paper.

II. Related Work

Quality of Service (QoS) is assumed to be the ultimate requirement of healthcare IoT networks, because, without maintaining the high standard of QoS metrics during communication these networks are trivial. For this, multiple research groups, patient wearable IoT producers, and healthcare enterprise market stakeholders are working concomitantly to depreciate the complexity of these gadgets during

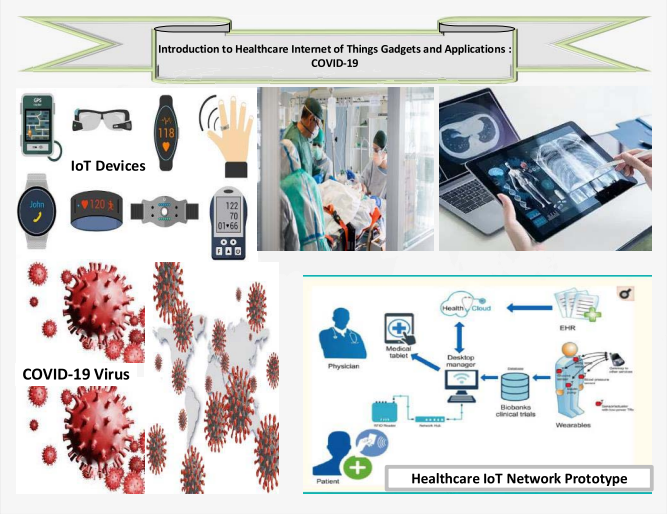


Fig. 1. COVID-19 pandemic healthcare IoT architecture diagram.

the manufacturing, deployment, and interconnecting stages to enhance QoS metrics [9]. In addition, the concerned research societies also investigated techniques that are useful to desegregate the three essential functions of patient wearable IoT devices such as collecting, processing, and communicating information in these networks with enhanced QoS metrics [10], [11]. To continue, the recent investigation focuses on innovative strategies such as network coding, collaborative and multilayer or cross-layer communication amongst coupled devices to promote communication attributes with better QoS results [12], [13]. As the demand for healthcare IoT applications increases the QoS obligation of these networks is also progressing, therefore, patient wearable devices need proper utilization with an accurate link evaluation to warrant efficient data compilation and exchange in the network [14]. To enhance the QoS in these applications, cross-layer, multilayer protocols, and a proper link estimation had played a remarkable role in the literature [15]–[19]. Figure 1, provides a visual illustration of IoT applications in the healthcare sector while taking into account the COVID-19 pandemic.

Cai *et al.* [20] presented a hierarchical structure-based modulation technique for healthcare IoT networks to enrich the QoS standard among communicating devices followed by the other network components. In this model, the authors incorporated additional transmission mechanisms to deal with buffer overflow and multi-relay implant concerns. Jaiswal *et al.* [21] presented a three-factor-based QoS improvement approach that takes into account traffic demand, healthcare IoT device lifetime, and best path for hop count communication infrastructure for these networks. Bhanumathi and Sangeetha [22] present a detailed survey on different routing protocols for body area networks to identify the hindrance factors such as human posture, node temperature, and transmission range, etc., that can affect the QoS of employed networks. To enhance the QoS standards in healthcare IoT applications, Khan *et al.* [23] proposed a hybrid protocol known as ZE-QoS by utilizing MAC/physical/data link layer and network layer infrastructure. ZE-QoS protocol considers three crucial features of the

TABLE I
COMPARATIVE SURVEY PAPERS SUMMARIZATION

Name of the Scheme	Descriptive Evaluation
Al-Humairi et al. [27]	Reference [27] highlights the use of tardiest technologies in the healthcare sector to mitigate the COVID-19 viral infection rates through patient implanted devices. However, the authors did not recommend anything congenial to the QoS of these applications, which is the prime demand of these networks.
Aman et al. [28]	In [27], the authors highlighted the prevailing trials associated with Internet of Medical Things (IoMT) design, applications, and security that have been ignored during the expansion of these applications in the COVID-19 pandemic. Alternatively, the writers did not specify the probable barriers related to the QoS that could be tackled, while extending the existing technology.
Malliga et al. [29]	Different healthcare IoT applications adopted in the COVID-19 pandemic to counter the widespread infectious rate of coronavirus are summarized as pre-screening, victim patient monitoring, infected people tracking, and quarantined people evaluation.
Agarwal et al. [30]	To handle a catastrophic pandemic like COVID-19 in the future, reference [29], ventures to scrutinize emerging applications of healthcare IoT. In order, to build background insights about this envisioning technology to fight against such a disastrous situation by highlighting the weak aspects to strengthen them in the future.
Siriwardhana et al. [31]	In this review article, the utilization of 5G and Internet of Things (IoT) are collectively evaluated to develop a rigid technology against a mortifying disease like COVID-19. The authors present different uses cases on the collective deployment of 5G and IoTby considering telehealthcare, education, supply chains, e-government, and smart manufacturing to ensure the operation, but they disregarded the QoS metrics while highlighting these scenarios.
Alsamhi et al. [32]	In this survey article, the utilization of blockchain-based healthcare IoT applications is considered to promote interaction attributes, while stretching the contemporary IoT technology in the COVID-19 pandemic. Furthermore, they assumed various uses case e.g. patient monitoring, social distancing, medical supply, sanitization, detecting and assessment of the patient to tackle the devastating circumstance.

TABLE II
OPERATIONAL PECULIARITIES EVALUATION OF ORDINARY IOT AND HEALTHCARE-IOT

peculiarities of ordinary IoT	peculiarities of ordinary IoT
Have several applications	Particularly employed in the health care sector.
Adjustable according to the application requirement	Work in the context of assigned task
Does not required accurate and precise results	Required extremely specific and explicit results according to the prescribed task.
Deployment does not need any special skills or requirement	Only be employed at a specific location in order to achieve accurate results.
During failure, does not have critical impact on the system	During failure, effect the reliable results of the system.
Traffic high intermittent with immense volume	Traffic is extremely careful with event-based communication.
Normal battery for ordinary operation	Special battery requirement for a longspun

network traffic while deciding the next-hop count device for forwarding data, which includes optimal path, congestions, and communication cost.

An Optimized Energy Efficient and Quality-of-Service aware Routing Protocol (OEEQR) was proposed by Kaur *et al.* [24] to overwhelm the QoS culmination in the IoT applications used in the healthcare domain. Different features and communication attributes are considered while checking the trustworthiness of this scheme. Kaur and Kumar [25] suggested an event-based load balancing scheme utilizing a multi-objective ant colony optimization algorithm with the help of a cross-layer routing paradigm to enrich the QoS attributes in healthcare IoT applications. An advanced routing protocol known as Minimum Cost Routing Algorithm (MCRA) was proposed in reference [26], to subjugate the QoS perplexities in healthcare IoT applications. The author's used communication attributes such as queue size, link reliability, residual energy, hop count distance, and transmission channel bandwidth to adequately distribute network traffic with convalescent results.

A. Existing Survey Papers

In this section, we will concentrate on the existing review papers associated with the QoS of healthcare IoT applications applied in the episode of COVID-19 to explore this topic from multiple perspectives. Despite that, we will take into account these papers for comparative analysis based on distinctive factors to evaluate, and affirm the innovation of this work. In table I, we have compiled the current review papers associated with the QoS of healthcare IoT applications published in the propinquity of the COVID-19 pandemic.

B. Structural and Functional Distinctions Within IoT and Medical IoT

Before delving into the analysis of the QoS of healthcare IoT applications, we will relish to clarify the fundamental demarcation between IoT and MoIT gadgets [33]. Table II outlines the most typical distinctions between these devices.

C. Healthcare Internet of Things Requirements

In the recent past, it has been perceived that the evolution of healthcare IoT technologies allows pervasive communication among intelligent gadgets, sensors, machines, and actuators on the client-side to handle various health-related problems [34]. Owing to the explicit condition of implementation, operation, and scalability, healthcare-IoT technologies confront many difficulties, which leaves the door open to academics, entrepreneurs, and healthcare experts to develop new ideas in terms of

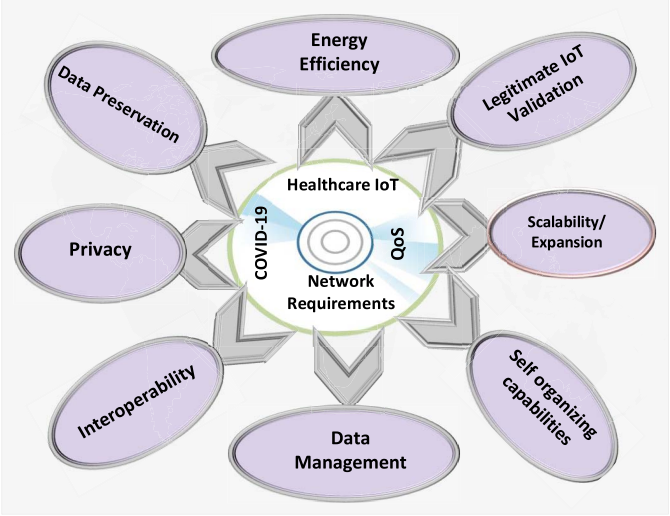


Fig. 2. Healthcare IoT applications fundamental requirements.

a productive network. Figure 2, summarizes the fundamental obligations of the existing healthcare IoT networks extended in the COVID-19 pandemic.

1) Healthcare IoT Scalability Requirements: Owing to the productive results of Healthcare IoT, its implementation, applications, and operational requirements are much higher than wireless body area networks or other traditional IoT applications. In these applications, scalability issues emerge at many levels, as the number of patient wearable devices interconnections grows up. Undermentioned are some important problems, which need concentration for all stakeholders working directly or indirectly in this domain.

a) Data communication requirements: Healthcare IoT applications used in the catastrophic situation of COVID-19 are stretched without peculiar deliberation of communication attributes. As we know, these applications are comprised on a huge number of patient wearable devices, which interact and share information with each other by following hop count communication for the sake of dispatch of data from the origin to the destination. Without decent scalability planning, numerous volumes of data interchange in these applications create network overhead, which arises the QoS concern and affects the credibility of an employed network.

b) IoT devices naming & addressing: As the healthcare IoT network expands, the number of patient wearable devices connected in the network also increases, which demands prim address and spacing to communicate effectively, therefore, scalability also arises the issues of addressing and space in these networks.

c) Data management: Healthcare IoT applications that are used in the COVID-19 pandemic also face data management challenges, as the number of patient wearable intelligent devices grew up in the network without appropriate consideration of QoS.

d) Service management: Efficient service superintendence also promotes the QoS in employed healthcare IoT, however, this issue is also neglected during the augmentation phase of existing healthcare IoT applications, therefore. at present, it needs the awareness of the research community to tackle it for better results.

e) Interoperability requirements: In healthcare IoT applications, different patient wearable devices have different tasks to collect and transmit data from patients to a remote physician. To promote reliable communication in the network, cooperation among different devices is disparately needed. Therefore, this argument also entails the researcher's attention to manipulate it accurately in the protracted applications of healthcare IoT.

f) Self-organizing capability: In contrast to computer networks, which need experts or technicians to configure it according to their requirement from time to time, healthcare IoT contains intelligent gadgets with self-organizing and configuring capabilities to adjust with the situations without requiring human intervention. Although, these devices adjust themselves with the circumstances without mortal intervention, but still scalability awakes the issue of traffic over head and QoS, which is the fundamental obligation of these networks.

g) Energy efficiency: Intelligent patient wearable gadgets comprised embedded batteries, which need provident utilization for continued operation. During scalability, energy consumption demands special attention for long terms operation of the network, because of unnecessary communication or long hop communication, the onboard battery power of these devices exhausts before their expected time period.

h) Data preservation requirements: QoS management during data preservation is another notable feature of healthcare IoT applications, which is ignored during the extendability of extant applications in the connection of the COVID-19 pandemic. Therefore, the research community followed by healthcare enterprises are acknowledged to take care of this prominent issue in the coordination of data protection.

i) Authentication of legal devices: Authentication of legal patient wearable devices with an improved QoS communication infrastructure is the ultimate requirement of healthcare IoT applications, which is omitted during the extendability of present applications in the COVID-19 pandemic. To enhance the QoS of standards in extend applications, academia and healthcare expert need to work synchronically and devise a convalescent authentication model by taking into account this important issue.

j) Particular hardware requirements: H-IoT gadgets require unique hardware for handling different tasks to accumulate and partake data in the network, which is ignored during the expansion phase of existing applications in the COVID-19 pandemic, therefore, the QoS is affected up to a great extent in these applications which need the considerable awareness of concerned parties to promote its standard in the present applications.

k) Particular software requirements: In healthcare IoT, software tools and applications have a huge influence on the network performance, which is overlooked during the extendability of the present applications in the calamitous situation of the COVID-19 pandemic. In order to achieve better results, this requirement must be considered, while contriving these kinds of applications in the future.

TABLE III
OPERATIONAL PECULIARITIES EVALUATION OF ORDINARY IoT AND HEALTHCARE-IoT

Description of requirement	Data Communication	Naming & addressing	Data management	Service Management	Inter operability	Self organization	Energy Efficiency	Data Preservation	Authentication of Legal Devices
Al-Humairi et al. [27]	⊗	⊗	⊗	⊗	√	⊗	√	⊗	⊗
Aman et al. [28]	⊗	√	⊗	⊗	⊗	⊗	⊗	⊗	⊗
Malliga et al. [29]	⊗	⊗	√	⊗	⊗	⊗	⊗	⊗	√
Agarwal et al. [30]	√	⊗	√	⊗	⊗	⊗	⊗	⊗	⊗
Siriwardhana et al. [31]	⊗	⊗	⊗	√	⊗	√	⊗	√	⊗
Alsamhi et al. [32]	⊗	⊗	√	⊗	√	⊗	⊗	⊗	√
Our Survey Paper	√	√	√	√	√	√	√	√	√

Table III, illustrate the comparative analysis with existing survey papers, they have ignored this important issue.

III. EXISTING APPLICATIONS AND CHALLENGES

Most healthcare IoT applications extended and deployed in the COVID-19 pandemic intends to combat the contamination of virus, monitoring of patients, and evaluation of people. Intelligent IoT devices are fastened with patients or placed in a specified location such as airports, supermarkets, and hospital entrances, etc., to monitor and assess people for COVID-19 virus infection and share the acquired data with the remote destination.

A. Challenges With Data Monitoring

Data collected by healthcare IoT devices deployed in the COVID-19 pandemic are extremely vast and need a strait-laced structure to achieve the forecasted results. Based on application requirements, these ingenious devices are needed to assess and control the extensive frequency of viral virus (corona) during pandemics like COVID-19.

Rashid *et al.* [35] recommended a CovidSens named intelligent framework for COVID-19 infected people assessment to alert the risk of coronavirus by spontaneously evaluating the victim people to analyze infectious data and acknowledge the propagation of coronavirus in suspected locations. The suggested model is very helpful to distill invaluable erudition for the exhibition of concerned agencies, government, and public to cordon the speculated area. However, the scheme spreads information concerning COVID-19 via social media, which unlocks the doorway for bogus reports circulating, therefore, this challenging issue obliges to be resolve for better results to preserve the confidence of customers and enterprises. In [36], the present multilevel safe management system for evaluation of people associated with different sectors utilizing the Swiss cheese risk management model. This scheme is very productive for the motionless organization to identify and mitigate the contamination of the COVID-19 virus for safe resumption of work. In contrast to static workplaces, the proposed model is not practical for a conspicuous area.

In [36], a drone-based framework for COVID-19 pandemic monitoring is suggested with specialized network architecture to use real-time data and scenarios for detection and mitigation of novel coronavirus. The challenges associated with digital surveillance system applications used in the COVID-19 pandemic are highlighted in reference [37]. In [38], various interactive means of communication are presented to monitor and assess the progress of different businesses from a remote location by inducting virtual conferences. The challenges associated with this include good internet connection, reliable equipment, and availability of concerned staff to manage the network. In [39], it is highlighted that patient wearable intelligent devices collect information about their assigned task followed location tracking of victims to stop the widespread of virus in a pandemic situation like COVID-19. However, the ethical and personal matters of an individual are ignored, which is the major challenge to be addressed. In [39], real-time data dashboards simulating system was proposed by Dong *et al.* utilizing AI and interactive web-based interface for minimization of coronavirus contamination. The system uses various things such as social media feeds, victim location, and concerned agencies' information in coordination to produce accurate results.

B. Architecture Challenges

The standard of QoS in the extended/expended healthcare IoT applications (COVID-19 pandemic) cannot be achieved without the deliberation of proper network architecture. Therefore, in this section, we will concentrate on the layerwise complications amalgamated with healthcare IoT networks to build a groundwork for improving the QoS standards of certain healthcare IoT applications. Figure 2, visualizes the different components of these challenges.

Reference [40] describes the notion of patient wearable intelligent machines to share data in the network employing the transmission protocols 802.15.4. Healthcare IoT networks are made up of tiny resource-constrained devices that are installed at the physical layer and focus on their assigned duties. Efficient usage allows them to enhance network productivity; therefore, specific configuration, deployment, and

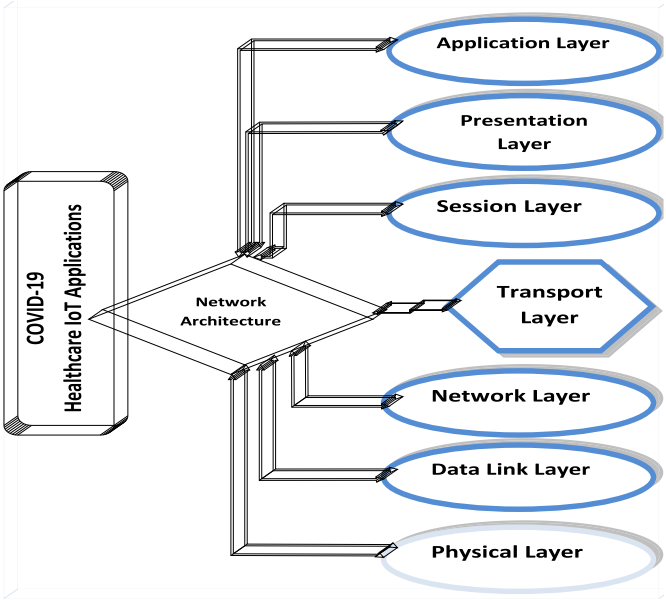


Fig. 3. Healthcare IoT network layer-wise architecture.

job direction are the most meaningful challenges to them, which were neglected throughout the COVID-19 pandemic, when the existing applications are extended for different tasks management [41]–[43].

To ensure the QoS standard and reliable operation of the employed healthcare IoT network, layer two and three devices adjustment, configuration, and traffic management play a significant role, which is ignored in the recent past under one umbrella [44], [45]. With the help of efficient routing protocols, the network traffic should be manipulated energetically in the employed healthcare IoT network, which is also ignored during the expansion phase of these networks. In fact, the research community utilized the existing routing protocols during this phase, which itself degrades the QoS because they were designed for a specific application, environment, and operation [46]. Similarly, interoperability is another issue that may be handled through routing protocols, but it is also neglected in these applications while extending the present application and now causing QoS problems in the form of inferior results [47], [48]. In an improved QoS infrastructure network, the role of the session, presentation, and application layer cannot be ignored, because effective session initiation minimizes traffic overhead in the deployed network. Similarly, reliable authentication, data compression, and recording also enhance the output of a network, but these important attributes did not give any attention during the expansion phase of the existing applications, which is now a challenging task for the research community to address [49]–[52].

C. QoS Challenges With Improved Security

Undoubtedly, a huge quantity of data manipulating in healthcare IoT applications demands a protected indoor and outdoor/open-air communication environment to preserve the confidence of patients, family members, service providers, and healthcare stakeholders [53]. By utilizing patient wearable intelligent IoT devices to accumulate, record and assist healthcare experts electronically in term of patient conditions, disease diagnoses, and prescribed medicine, etc. The authentication and data preservations should be given profound importance to maintain the trust of all stakeholders. [54]. To achieve better results, security with scalability of these applications can not be overlooked. At present, healthcare IoT apps played a critical part in coronavirus contamination prevention measures by performing various assessments such as virus mutiny prognostication, viral tracking, victims therapy or diagnosis, and medication prescription. Different types of security concerns equated with these applications are reviewed in more detail in the following subsections.

l) QoS Challenges with trust management: QoS along with trust management is an imperative constituent of healthcare IoT applications expended in the catastrophic situation of COVID-19. Patient wearable devices are organized in a peer-to-peer or ad hoc networks paradigm, which needs proper trust management infrastructure to enable secure data sharing among participating entities in the network [55], [56]. Trust management and QoS with high mobility of the patients is stimulating issues to address and maintain reliable communication among these gadgets. Despite that, patient wearable devices are usually self administrative and do not have a distributive authentication model, which also arises QoS issues during validation and communication [57].

m) QoS Challenges with data preservation: In the literature, most patient wearable IoT devices did not use symmetric and asymmetric key-based authentication algorithms because of the high computation cost and limited resources of these gadgets, which arises the QoS issues in these networks, because the researcher's designed lightweight validation schemes [58]–[60] to address the security concern, but they overlooked the QoS concerns [61], [62]. In the turn of dependable operation, these devices demand certain routing protocols in the coordination of lightweight authentication models to enhances their productivity. High standard QoS cannot be achieved without consideration of routing protocols in correlation with authentication schemes that involve public and private key matching e.g., PKI, RSA or digital signature-based authentication [63].

n) QoS challenges with privacy: Healthcare IoT applications utilized in the COVID-19 pandemic are highly effective in terms of outcomes, but they also offer numerous privacy risks to the medical information of patients [64]. For example, reference [65] revealed these applications can infer patient daily and private activities such as showers monitoring, cooking monitoring, eating monitoring, and leaving or incoming home. Keeping in view, there is a tradeoff between QoS and privacy, since increased privacy demand has an impact on the QoS of the employed network, as shown in reference [66]. Considering the correlation factors of these networks, authentication, and communication need a cooperative mechanism for better results. Therefore, the researchers, stakeholders, and healthcare experts are acknowledged to devise cooperative protocols to fix this issue.

D. QoS Challenges With Interoperability

Heterogeneous IoT networks intended in the healthcare domain produces an immense piece of real-time information that follows layer-wise open system interconnection (OSI) to share this data in the network [67]. Patient wearable devices connected heterogeneity can arise QoS issues in terms of their features, size, vendor, operation, and application-specific requirements etc., [68]. Despite patient wearable devices heterogeneity, the perspectives like complex technologies interconnection, data formats, routing protocols, authentication schemes, hardware and software compatibility, data semantics, transmission frequencies, followed by processing strategies are the most indispensable challenges associated with any healthcare IoT network that could improve QoS standard in collaboration [48], [69]. To highlight the provocations of QoS that are interlinked with healthcare IoT networks in terms of the aforementioned attributes are broadly summarized in figure 4 and consequent subsections.

o) QoS challenges technical interoperability: As the healthcare IoT is rising and expanding without a proper established plan, it arises many problems in terms of technical interoperability. Most commonly this is seen in the expansion phase of existing healthcare IoT applications in the COVID-19 and will be anticipated to recapitulate in the coming years [48]. As a result, it knocks the door of technical interoperable challenges, which could be detrimental for the QoS of these applications. In literature, several technical interoperable solutions are presented to fix this problem [69]–[72], but most of them are circumstantial to the system, conditions, or ostracize the flag of QoS, which is the central interest of these applications.

p) QoS challenges syntactic interoperability: In healthcare IoT applications, the term "syntactic interoperability" pertains to the data edifice, configuration, and formats that could be utilized for transmission in the network across various platforms [73]. Syntactic interoperability intends to smooth the transformation of messages amidst patient wearable IoT gadgets in an operational network. Despite that, syntactic interoperability would be accomplished through pre-defined interconnectivity, data structure, format, and encoding, which is overlooked during the extendibility phase of existing applications in the COVID-19 pandemic [74]. To tackle this problem, the middle-ware like interface could be effective such as discussed in reference [75], whereas the author's used a software-defined gateway to dynamically control patient wearable devices to maintain a high standard of QoS in the network. The major problem with current solutions is that they focus only on data consistency rather than a dependable interface structure, which is the most important aspect of these problems to be grasped for successful results.

q) QoS challenges semantic interoperability: Semantic interoperability is linked with web technologies to query and answer the things in the employed network as a potential method to maintain coherent relations across diverse experimental infrastructures [76]. However, the majority of existing techniques use the top-down approach by stipulating only framework and meta-directory service, which is not a concrete solution for emerging applications [77]–[79]. Therefore, the involved parties need to set down around a single table and decisive more productive framework by considering all challenges correlated with semantic interoperability.

E. Comparative Analysis of the QoS Challenges

Section 3 cannot be concluded without comparative analysis with rival review papers, because to the best of our knowledge most of them present survey papers present only one aspect of these challenges, which is far beyond the true picture of fundamental obstacles incorporated with these applications to be considered to improve the standard of QoS. In addition, the challenges highlighted in this review are collectively the prerequisites of any IoT application, they demand a high standard of QoS requirements. Therefore, the research community is acknowledged to assume all of them, while devising new techniques, modifying the existing one's or expanding the networks. Table IV, exhibit the comparative analysis of our paper in the presence of existing survey papers that how our work is unique from them in term of QoS challenges.

IV. Opportunities With Future Research Direction

In this section, we will go through the research gap by assuming the highlighted requirements and challenges to set the footprint of future work in this domain with urgent or need-based scalability of existing IoT applications and particularly healthcare IoT. To do so, we have highlighted the undermentioned viable research direction in light of identified requirements and challenges to improve the standard of QoS in these applications.

A. Machine Learning Based Solutions

The performance, applicability, and reliability of machine learning techniques in IoT applications and especially in the healthcare sectors cannot be ostracized, because they are pretty handy to contrive network traffic with respect to the usable bandwidth in wired and wireless communication infrastructure [80]. In the healthcare domain, management of patient wearable devices and network traffic in the physical and transport layer via machine learning techniques could be extremely effective and productive in the context of improved QoS standards. Therefore, researchers, vendors of patient wearable devices, network administrators, and healthcare enterprises are acknowledged to utilize machine learning algorithms in different phases to take benefit of them in adaptive technologies. Consequently, it is also appropriate to specify that supervised, unsupervised, and deep learning algorithms could be extremely helpful in this regard to increase the fecundity of the employed network by following layer wise communication model.

1) **Machine Learning-based Routing Protocols:** Adequate traffic administration via routing protocols can play an animate role in the QoS of a network. Therefore, ML-based routing protocol could efficiently train network devices by predicting or analyzing the available transmission channel to transmit data from the origin to the targeted location.

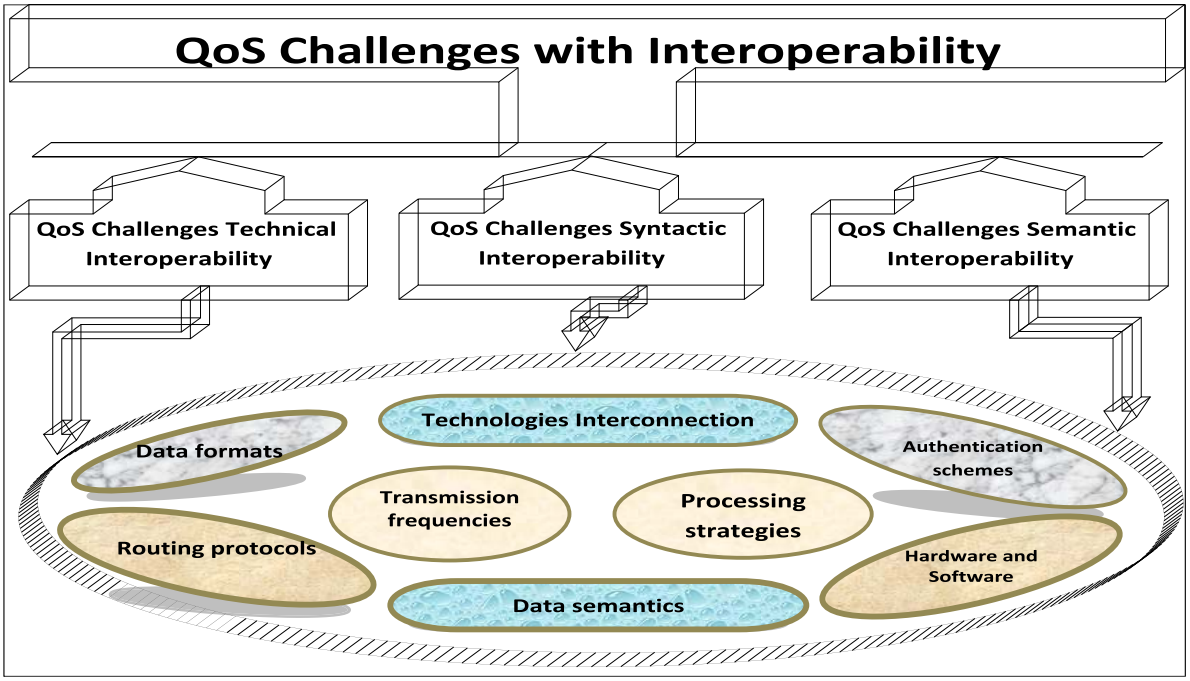


Fig. 4. Interoperable challenges in healthcare IoT.

TABLE IV
COMPARATIVE ANALYSIS OF OUR ARTICLE WITH PRESENT REVIEW STUDIES

Challenges Name	Al-Humairi et al. [27]	Aman et al. [28]	Malliga et al. [29]	Agarwal et al. [30]	Siriwardhana et al. [31]	Alsamhi et al. [32]	Our Survey
		QoS Challenges	**with data**	**monitoring**			
Drone-based monitoring	No	No	No	No	No	No	Yes
Interactive session base monitoring	No	No	No	No	No	No	Yes
Real-time data monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes
		QoS Challenges	**associated with**	**Architecture**			
Network Layer-wise challenges	Partial Yes	No	No	Partial Yes	No	No	Yes
Particular Hardware & Software	No	No	No	No	No	No	Yes
Communication Challenges	Yes	No	Yes	No	No	Yes	Yes
		QoS Challenges	**associated with**	**Improved**	**Security**		
Trust Management Challenges	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data Preservation Challenges	No	No	Partial Yes	No	No	Partial Yes	Yes
Privacy Challenges	No	No	No	No	No	No	Yes
		QoS Challenges	**associated with**	**Interoperability**			
Technical Interoperability	No	No	No	No	No	No	Yes
Syntactic Interoperability	Partial Yes	No	No	Partial Yes	No	Partial Yes	Yes
Semantic Interoperability	No	No	Partial Yes	Partial Yes	No	No	Yes

2) **Data collection and Transmission:** Machine Learning play a pivotal role to analyze collected data at the origin by following their train classifier to transmit only important information and discard unnecessary data at the origin, which improves the QoS standard because the liable devices only share important information.

B. Blockchain Based Solutions

In heterogeneous healthcare IoT applications, the role of blockchain technology can not be dumped in these applications, because they are very productive while contriving distinct assignments in the decentralized environment [81]. In literature, the QoS issue is omitted in the context of blockchain-based communication, if the research community interprets and investigates new techniques to manipulate this problem in blockchain communication infrastructure, then it could be very helpful to achieve better results.

1) **Predictable model:** QoS of employed healthcare IoT networks can be enhanced by designing predictable models with the help of ML techniques to follow and forward communication details of an individual patient to the concerned server, base station, or service provider in blockchain communication infrastructure.
2) **Data Synchronization:** Data synchronization and evaluation is another research direction utilizing blockchain

TABLE V
COMPARATIVE ANALYSIS OF OUR ARTICLE WITH PRESENT REVIEW STUDIES

Challenges Name	Al-Humairi et al. [27]	Aman et al. [28]	Malliga et al. [29]	Agarwal et al. [30]	Siriwardhana et al. [31]	Alsamhi et al. [32]	Our Survey
		Machine	**Learning based**	**Solutions**			
Machine Learning-based Routing Protocols	√	⊗	√	⊗	⊗	⊗	√
Machine algorithm in hardware and software interoperability	⊗	√	⊗	√	⊗	√	√
Different technology interoperability via ML	⊗	⊗	⊗	⊗	√	⊗	√
Role of ML algorithm in data collection & transmission	√	⊗	⊗	√	⊗	√	√
		Blockchain	**based**	**Solutions**			
Predictable model	⊗	√	⊗	⊗	⊗	√	√
Blockchain based interoperability	⊗	⊗	√	⊗	⊗	⊗	√
Data Synchronization in blockchain	√	⊗	⊗	√	⊗	√	√
		Edge	**computing**	**based**	**solutions**		
Data Management via ML techniques	⊗	⊗	⊗	⊗	⊗	⊗	√
Routing in Edge computing	√	⊗	√	√	⊗	√	√
Data management	⊗	√	⊗	√	√	⊗	√
		Fog and	**cloud computing**	**based**	**solutions**		
Data management	⊗	√	⊗	√	√	⊗	√
Interoperability	√	⊗	⊗	⊗	⊗	√	√
Routing Fog and Cloud computing	⊗	⊗	√	√	√	⊗	√
ML in Fog and Cloud computing	√	⊗	⊗	⊗	⊗	√	√
		Software	**defined network**	**based**	**solutions**		
Controller node based traffic management	⊗	⊗	⊗	⊗	√	⊗	√
Controller node based resources management	⊗	⊗	⊗	⊗	⊗	⊗	√

infrastructure to promote the QoS metrics of employed healthcare IoT applications.

C. Edge Computing Based Solutions

To intensify the QoS metrics in healthcare IoT applications practiced in the connection of the COVID-19 pandemic, the role of Edge computing cannot be overlooked, because efficient edge computing with help of ML techniques and routing protocols could be remarkably propitious for these applications [82]. At present, the literature lacks to presents such useful techniques to fix this problem. Therefore, the involved in this domain are acknowledged to utilize this emerging technology for the sake of better QoS demands.

D. Fog and Cloud Computing Based Solutions

Fog and cloud computing could be also very useful in the extended applications of healthcare IoT in the COVID-19 to enrich network performance in terms of QoS attributes [83]. Therefore, intelligent gadgets producers, researchers, network managers, and healthcare experts need to pay collective attention to-ward the utilization of these technologies, while designing hardware, protocols, or ML techniques to attain better results.

E. Software Defined Network Based Solutions

Software-defined (SDN) network is an alternative research direction to enhances the QoS attributes of extended healthcare IoT applications by utilizing controller nodes in the networks. Although, SDN is in use for a quite long time, but their applicability is snubbed during the COVID-19 pandemic when existing healthcare IoT applications are utilized for additional tasks. Therefore, the SDN could be an alternative choice to manage and direct network traffic with the help of controller nodes to enhances the QoS attributes.

F. Discussion With Comparative Analysis

To confirm the contribution and originality of our review article, we will again compare this section to other state-of-the-art review articles to see how our work deviates from them. As we mentioned and highlighted in the earlier sections that the present survey papers only focus on an individual aspect, and somehow they are failed to present the true picture of these attributes, and technologies to magnify the QoS norm in these applications. Indeed, we acknowledge all the potential investigation directions in this subsection to set the road map for improved QoS attributes in these applications. Apart from this, in table V, we also compare them with rival review papers to assert the innovation of this work.

V. CONCLUSION

In this review article, we have presented a thorough review of the QoS requirements and challenges regarding smart sensing in healthcare IoT applications with an objective to underline the limitations of the present literature, and highlight or set future research opportunities that could be effective in

the redressal of the identified limitations. Initially, we have had taken into account the existing IoMT applications particularly used in the connection of the COVID-19 pandemic from 2019 to 2021. In the beginning, we had a thorough evaluation of the present literature associated with the QoS of these applications to identify the most disastrous specification interconnected with them. In the consequent section, we continued our discussion to point out and highlight the challenges interlinked with these applications, that are still unresolved. In section IV, we followed the set road map of the preceding sections such as requirements and challenges to highlight the possible future research directions by considering the existing limitations of present literature to enriched QoS attributes in these applications. To claim the uniqueness of this work, we compared each section with rival review articles to certify the contribution and novelty to this work with the objective to answer the question why this article is different from them.

REFERENCES

[1] A. Fiorillo and P. Gorwood, "The consequences of the COVID-19 pandemic on mental health and implications for clinical practice," *Eur. Psychiatry*, vol. 63, no. 1, p. e32, 2020.

[2] [Online]. Available: https://www.worldometers.info/coronavirus/?utm 661 campaign=homeAdvegas1?

[3] M. S. Hossain and G. Muhammad, "Emotion-aware connected healthcare big data towards 5G," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2399–2406, Aug. 2018.

[4] M. Z. Alom *et al.*, "A state-of-the-art survey on deep learning theory and architectures," *Electronics*, vol. 8, no. 3, p. 292, Mar. 2019.

[5] M. Alhussein, G. Muhammad, M. S. Hossain, and S. U. Amin, "Cognitive IoT-cloud integration for smart healthcare: Case study for epileptic seizure detection and monitoring," *Mobile Netw. Appl.*, vol. 23, pp. 1624–1635, Dec. 2018.

[6] I. Ahmed, M. Ahmad, J. J. P. C. Rodrigues, G. Jeon, and S. Din, "A deep learning-based social distance monitoring framework for COVID-19," *Sustain. Cities Soc.*, vol. 65, Feb. 2021, Art. no. 102571.

[7] M. S. Hossain, G. Muhammad, and N. Guizani, "Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics," *IEEE Netw.*, vol. 34, no. 4, pp. 126–132, Jul. 2020.

[8] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced Internet of Health Things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020.

[9] A. Ahad, M. Tahir, M. A. Sheikh, K. I. Ahmed, A. Mughees, and A. Numani, "Technologies trend towards 5G network for smart healthcare using IoT: A review," *Sensors*, vol. 20, no. 14, p. 4047, Jul. 2020.

[10] M. H. Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *J. Netw. Comput. Appl.*, vol. 192, Oct. 2021, Art. no. 103164.

[11] A. A. Mutlag, M. K. A. Ghani, N. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Gener. Comput. Syst.*, vol. 90, pp. 62–78, Jan. 2019.

[12] K. Kumar, S. Kumar, O. Kaiwartya, Y. Cao, J. Lloret, and N. Aslam, "Cross-layer energy optimization for IoT environments: Technical advances and opportunities," *Energies*, vol. 10, no. 12, p. 2073, Dec. 2017.

[13] M. Adil, "Congestion free opportunistic multipath routing load balancing scheme for Internet of Things (IoT)," *Comput. Netw.*, vol. 184, Jan. 2021, Art. no. 107707.

[14] L. Hughes, X. Wang, and T. Chen, "A review of protocol implementations and energy efficient cross-layer design for wireless body area networks," *Sensors*, vol. 12, no. 11, pp. 14730–14773, 2012.

[15] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021.

[16] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog computing in healthcare—A review and discussion," *IEEE Access*, vol. 5, pp. 9206–9222, 2017.

[17] G. Marques, R. Pitarma, N. M. Garcia, and N. Pombo, "Internet of Things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: A review," *Electronics*, vol. 8, no. 10, p. 1081, Sep. 2019.

[18] M. Talal *et al.*, "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review," *J. Med. Syst.*, vol. 43, no. 3, p. 42, Mar. 2019.

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

[20] G. Cai, Y. Fang, J. Wen, G. Han, and X. Yang, "QoS-aware buffer-aided relaying implant WBAN for healthcare IoT: Opportunities and challenges," *IEEE Netw.*, vol. 33, no. 4, pp. 96–103, Jul. 2019.

[21] 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 Pers. Commun.*, vol. 111, no. 4, pp. 2493–2515, Apr. 2020.

[22] V. Bhanumathi and C. P. Sangeetha, "A guide for the selection of routing protocols in WBAN for healthcare applications," *Hum.-Centric Comput. Inf. Sci.*, vol. 7, no. 1, pp. 1–19, Dec. 2017.

[23] Z. A. Khan, S. Sivakumar, W. Phillips, and B. Robertson, "ZEQoS: A new energy and QoS-aware routing protocol for communication of sensor devices in healthcare system," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 6, Jun. 2014, Art. no. 627689.

[24] T. Kaur, N. Kaur, and G. Sidhu, "Optimized energy efficient and QoS aware routing protocol for WBAN," *Recent Patents Eng.*, vol. 14, no. 3, pp. 286–293, Jan. 2021.

[25] T. Kaur and D. Kumar, "MACO-QCR: Multi-objective ACO-based QoS-aware cross-layer routing protocols in WSN," *IEEE Sensors J.*, vol. 21, no. 5, pp. 6775–6783, Mar. 2021.

[26] V. Bhanumathi and C. P. Sangeetha, "QoS-aware minimum cost routing algorithm for wireless body area networks," *Adhoc Sensor Wireless Netw.*, vol. 47, nos. 1–4, pp. 1–18, 2020.

[27] S. N. S. Al-Humairi and A. A. A. Kamal, "Opportunities and challenges for the building monitoring systems in the age-pandemic of COVID-19: Review and prospects," *Innov. Infrastruct. Solutions*, vol. 6, no. 2, pp. 1–10, Jun. 2021.

[28] A. H. M. Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, "IoMT amid COVID-19 pandemic: Application, architecture, technology, and security," *J. Netw. Comput. Appl.*, vol. 174, Jan. 2021, Art. no. 102886.

[29] S. Malliga, S. V. Kogilavani, and P. S. Nandhini, "A comprehensive review of applications of Internet of Things for COVID-19 pandemic," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1055, no. 1, Feb. 2021, Art. no. 012083.

[30] S. Agarwal *et al.*, "Unleashing the power of disruptive and emerging technologies amid COVID-19: A detailed review," 2020, *arXiv:2005.11507*.

[31] Y. Siriwardhana, C. De Alwis, G. Gür, M. Ylianttila, and M. Liyanage, "The fight against the COVID-19 pandemic with 5G technologies," *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 72–84, Sep. 2020.

[32] S. H. Alsamhi, B. Lee, M. Guizani, N. Kumar, Y. Qiao, and X. Liu, "Blockchain for decentralized multi-drone to combat COVID-19 and future pandemics: Framework and proposed solutions," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 9, Sep. 2021, Art. no. e4255.

[33] S. Chitra and V. Jayalakshmi, "A review of healthcare applications on Internet of Things," in *Computer Networks, Big Data and IoT*. 2021, pp. 227–237.

[34] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–27, Mar. 2021.

[35] M. T. Rashid and D. Wang, "CovidSens: A vision on reliable social sensing for COVID-19," *Artif. Intell. Rev.*, vol. 54, no. 1, pp. 1–25, Jan. 2021.

[36] W. H. Gan and D. Koh, "COVID-19 and return-to-work for the construction sector: Lessons from Singapore," *Saf. Health Work*, vol. 12, no. 2, pp. 277–281, Jun. 2021.

[37] M. R. Hussein, A. B. Shams, E. H. Apu, K. A. A. Mamun, and M. S. Rahman, "Digital surveillance systems for tracing COVID-19: Privacy and security challenges with recommendations," 2020, *arXiv:2007.13182*.

[38] O. Hughes, "Zoom vs Microsoft Teams, Google Meet, Cisco WebEx and Skype: Choosing the right video-conferencing apps for you," TechRepublic, Tech. Rep., 2020. [Online]. Available: https: //www. techrepublic. com/article/zoom-vs-microsoft-teams-google-meet-cisco-webex-and-skype-choosing-the-right-video-conferencing-apps-for-you

[39] E. Dong, H. Du, and L. Gardner, "An interactive web-based dashboard to track COVID-19 in real time," *Lancet Infectious Diseases*, vol. 20, no. 5, pp. 533–534, 2020.

[40] S. Ketu and P. K. Mishra, "Cloud, fog and mist computing in IoT: An indication of emerging opportunities," *IETE Tech. Rev.*, pp. 1–12, Mar. 2021.

[41] A. Raj and S. D. Shetty, "IoT eco-system, layered architectures, security and advancing technologies: A comprehensive survey," *Wireless Pers. Commun.*, vol. 122, pp. 1481–1517, Aug. 2021.

[42] A. Kumari, R. Gupta, and S. Tanwar, "Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review," *Comput. Commun.*, vol. 172, pp. 102–118, Apr. 2021.

[43] M. Adil *et al.*, "EnhancedAODV: A robust three phase priority-based traffic load balancing scheme for Internet of Things," *IEEE Internet Things J.*, early access, Apr. 13, 2022, doi: 10.1109/JIOT.2021.3072984.

[44] A. A. Ahmed, "Lightweight digital certificate management and efficacious symmetric cryptographic mechanism over industrial Internet of Things," *Sensors*, vol. 21, no. 8, p. 2810, Apr. 2021.

[45] 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, Apr. 2019.

[46] Y. B. Zikria, M. K. Afzal, F. Ishmanov, S. W. Kim, and H. Yu, "A survey on routing protocols supported by the Contiki Internet of Things operating system," *Future Gener. Comput. Syst.*, vol. 82, pp. 200–219, May 2018.

[47] L. Soltanisehat, R. Alizadeh, H. Hao, and K.-K.-R. Choo, "Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review," *IEEE Trans. Eng. Manag.*, early access, Sep. 2, 2020, doi: 10.1109/TEM.2020.3013507.

[48] I. Yaqoob *et al.*, "Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 10–16, Jun. 2017.

[49] A. B. Pawar and S. Ghumbre, "A survey on IoT applications, security challenges and counter measures," in *Proc. Int. Conf. Comput., Anal. Secur. Trends (CAST)*, Dec. 2016, pp. 294–299.

[50] R. De Michele and M. Furini, "IoT healthcare: Benefits, issues and challenges," in *Proc. 5th EAI Int. Conf. Smart Objects Technol. Social Good*, Sep. 2019, pp. 160–164.

[51] W. Tang, K. Zhang, D. Zhang, J. Ren, Y. Zhang, and X. S. Shen, "Fog-enabled smart health: Toward cooperative and secure healthcare service provision," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 42–48, May 2019.

[52] M. Adil *et al.*, "An intelligent hybrid mutual authentication scheme for industrial Internet of Thing networks," *Comput., Mater. Continua*, vol. 68, no. 1, pp. 447–470, 2021.

[53] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," in *Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT)*, Oct. 2015, pp. 1577–1581.

[54] G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and health: Internet of Things, big data, and cloud computing for healthcare 4.0," *J. Ind. Inf. Integr.*, vol. 18, Jun. 2020, Art. no. 100129.

[55] X. Ding, J. Guo, D. Li, and W. Wu, "An incentive mechanism for building a secure blockchain-based Internet of Things," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 1, pp. 477–487, Jan. 2021.

[56] F. Naeem, G. Srivastava, and M. Tariq, "A software defined network based fuzzy normalized neural adaptive multipath congestion control for the Internet of Things," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2155–2164, Oct. 2020.

[57] M. Dai, J. Li, Z. Su, W. Chen, Q. Xu, and S. Fu, "A privacy preservation based scheme for task assignment in Internet of Things," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2323–2335, Oct. 2020.

[58] B. Cao, X. Wang, W. Zhang, H. Song, and Z. Lv, "A many-objective optimization model of industrial Internet of Things based on private blockchain," *IEEE Netw.*, vol. 34, no. 5, pp. 78–83, Sep./Oct. 2020.

[59] M. Adil *et al.*, "MAC-AODV based mutual authentication scheme for constraint oriented networks," *IEEE Access*, vol. 8, pp. 44459–44469, 2020.

[60] M. A. Jan, F. Khan, S. Mastorakis, M. Adil, A. Akbar, and N. Stergiou, "LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1202–1211, Sep. 2021.

[61] R. Somasundaram and M. Thirugnanam, "Review of security challenges in healthcare Internet of Things," *Wireless Netw.*, vol. 27, no. 8, pp. 5503–5509, 2021.

[62] R. Singh, T. Ahmed, A. K. Singh, P. Chanak, and S. K. Singh, "SeizSClas: An efficient and secure Internet-of-Things-based EEG classifier," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6214–6221, Apr. 2021.

[63] W. Yanez, R. Mahmud, R. Bahsoon, Y. Zhang, and R. Buyya, "Data allocation mechanism for Internet-of-Things systems with blockchain," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3509–3522, Apr. 2020.

[64] T. Mustafa and A. Varol, "Review of the Internet of Things for healthcare monitoring," in *Proc. 8th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Jun. 2020, pp. 1–6.

[65] K. Park *et al.*, "LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical Internet of Things," *IEEE Access*, vol. 8, pp. 119387–119404, 2020.

[66] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," *IEEE Access*, vol. 8, pp. 52018–52027, 2020.

[67] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things infrastructure: Classification, challenges, and future work," in *Proc. Int. Conf. Internet Things Service*. Cham, Switzerland: Springer, Sep. 2017, pp. 11–18.

[68] B. Ahlgren, M. Hidell, and E. C.-H. Ngai, "Internet of Things for smart cities: Interoperability and open data," *IEEE Internet Comput.*, vol. 20, no. 6, pp. 52–56, Nov./Dec. 2016.

[69] E. de Matos *et al.*, "Context information sharing for the Internet of Things: A survey," *Comput. Netw.*, vol. 166, Jan. 2020, Art. no. 106988.

[70] N. Pathak, A. Mukherjee, and S. Misra, "Reconfigure and reuse: Interoperable wearables for healthcare IoT," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Jul. 2020, pp. 20–29.

[71] P. Pace *et al.*, "INTER-health: An interoperable IoT solution for active and assisted living healthcare services," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 81–86.

[72] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.

[73] E. Lee, Y.-D. Seo, S.-R. Oh, and Y.-G. Kim, "A survey on standards for interoperability and security in the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1020–1047, 2nd Quart., 2021.

[74] N. Y. Philip, J. J. P. C. Rodrigues, H. Wang, S. J. Fong, and J. Chen, "Internet of Things for in-home health monitoring systems: Current advances, challenges and future directions," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 300–310, Feb. 2021.

[75] N. Pathak, S. Misra, A. Mukherjee, and N. Kumar, "HeDI: Healthcare device interoperability for IoT-based e-Health platforms," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 16845–16852, Dec. 2021.

[76] S. Balakrishna and M. Thirumaran, "Semantics and clustering techniques for IoT sensor data analysis: A comprehensive Survey," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. 2020, pp. 103–125.

[77] B. Rana, Y. Singh, and P. K. Singh, "A systematic survey on Internet of Things: Energy efficiency and interoperability perspective," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 8, Aug. 2021, Art. no. e4166.

[78] A. Tolba and Z. Al-Makhadmeh, "Predictive data analysis approach for securing medical data in smart grid healthcare systems," *Future Gener. Comput. Syst.*, vol. 117, pp. 87–96, Apr. 2021.

[79] M. Gheisari *et al.*, "OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city," *Future Gener. Comput. Syst.*, vol. 123, pp. 1–13, Oct. 2021.

[80] G. Manogaran *et al.*, "Machine learning assisted information management scheme in service concentrated IoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2871–2879, Apr. 2021.

[81] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases," *IEEE Syst. J.*, vol. 15, no. 1, pp. 85–94, Mar. 2021.

[82] R. Bosri, A. R. Uzzal, A. Al Omar, M. Z. A. Bhuiyan, and M. S. Rahman, "HIDEchain: A user-centric secure edge computing architecture for healthcare IoT devices," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 376–381.

[83] S. R. Hassan, I. Ahmad, S. Ahmad, A. Alfaify, and M. Shafiq, "Remote pain monitoring using fog computing for e-healthcare: An efficient architecture," *Sensors*, vol. 20, no. 22, p. 6574, Nov. 2020.

Muhammad Adil (Graduate Student Member, IEEE) received the Associate Engineer degree in electronics from the School of Electronic, Civil Aviation Pakistan, in 2010, and the Bachelor of Science degree in computer science (four years program) and the Master of Science degree in computer sciences (two years program) from the Virtual University of Pakistan, Lahore, in 2017 and 2020, respectively, with specialization in computer networks. He has CCNA and CCNP certifications. He is currently a Researcher with the Global Foundation for Cyber Studies and Research. He has many publications in prestigious journals, such as IEEE Internet of Things Journal (IEEE IoT), IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Industrial Informatics (IEEE TII), IEEE Transactions on Network Science and Engineering (TNSE), IEEE Access, *IEEE Micro Magazine*, *Computer Networks* (Elsevier), *Sustainable Cities and Society*, and *Sensors* (MDPI). His research interests include different routing protocols, security, and load balancing in WSN, the IoT, and UAVs. He is a member of the Computer Society, Industrial Electronics, Cybersecurity, Young Professionals, and LJPC-U.K. He is reviewing for prestigious journals, such as IEEE Access, IEEE Sensors Journal, IEEE Systems Journal, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Transactions on Cognitive Communications and Networking, IEEE Transactions on Green Communications and Networking, IEEE Wireless Communications Letters, *IET Communications*, *Computer Networks*, and *Telecommunication Systems*.

Hani Alshahrani (Member, IEEE) received the bachelor's degree in computer science from King Khalid University, Abha, Saudi Arabia, the master's degree in computer science from California Lutheran University, Thousand Oaks, CA, USA, and the Ph.D. degree from Oakland University, Rochester, MI, USA. Currently, he is a Faculty Member of Computer Science and Information Systems with Najran University, Najran, Saudi Arabia. His current research focuses on smartphones, the IoT, crowdsourcing security, and privacy.

Adel Rajab (Member, IEEE) received the bachelor's degree in computer science and information systems and the master's and Ph.D. degrees in computer science and engineering from the University of South Carolina, USA. He is currently working as an Associate Professor with the College of Computer Science and Information System (CSIS) and the Vice-Dean of Graduate Studies for Academic Affairs with Najran University, Najran, Saudi Arabia. His research interests are robotics, drones, machine learning, and bioinformatic OBS networks.

Asadullah Shaikh (Member, IEEE) received the B.Sc. degree in software development from the University of Huddersfield, U.K., the M.Sc. degree in software engineering and management from Gothenburg University, Sweden, and the Ph.D. degree in software engineering from the University of Southern Denmark. He is currently working as a Professor, the Head of Research and Graduate Studies, and the Coordinator of Seminars and Training with the College of Computer Science and Information Systems, Najran University, Najran, Saudi Arabia. He has more than 122 publications in the area of software engineering in international journals and conferences. He has vast experience in teaching and research. His current research topics are UML model verification, UML class diagrams verification with OCL constraints for complex models, formal verification, and feedback technique for unsatisfiable UML/OCL class diagrams.

Houbing Song (Senior Member, IEEE) received the M.S. degree in civil engineering from The University of Texas at Austin, El Paso, TX, USA, in December 2006, and the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in August 2012. In August 2017, he joined the Department of Electrical, Computer, Software, and Systems Engineering, Embry–Riddle Aeronautical University, Daytona Beach, FL, USA, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory. He served on the Faculty of West Virginia University, Charlottesville, from August 2012 to August 2017. In 2007, he was an Engineering Research Associate with the Texas A&M Transportation Institute, Dallas, TX, USA. His research has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360, USA Today, U.S. News and World Report, Fox News, the Association for Unmanned Vehicle Systems International, Forbes, WFTV, and New Atlas. His research interests include cyber-physical systems, cyber security and privacy, the Internet of Things, edge computing, AI/machine learning, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking.

Ahmed Farouk (Member, IEEE) received the M.Sc. and Ph.D. degrees from Mansoura University, Mansoura, Egypt. He is currently an Assistant Professor. Prior to that, he was a Postdoctoral Research Fellow with Wilfrid Laurier University, Waterloo, ON, Canada; and Ryerson University, Toronto, ON, Canada. He is one of the top 20 technical co-founders of the Quantum Machine Learning Program by the Creative Destruction Laboratory, University of Toronto, Toronto. He is exceptionally well-known for his seminal contributions to theories of quantum information, communication, and cryptography. He has authored or coauthored 62 articles in reputed and high-impact journals, such as *Scientific Reports* (Nature) and *Physical Review A*. The exceptional quality of his research is recognized nationally and internationally. He was selected by the Scientific Review Panel of the Council for the Lindau Nobel Laureate Meetings to participate in the 70th Lindau Nobel Laureate Meeting. He is selected as the top 25 of innovate TO 150 Canada to showcase the best of Toronto's next generation of change-makers, innovators, and entrepreneurs. He is also selected as the IEEE and IET Young Professional Ambassador and as a Moderator for the new IEEE TechRxiv. His volunteering work is apparent since he was appointed as the Chair of the IEEE Computer Chapter for the Waterloo–Kitchener area and the editorial board for many reputed journals, such as *Scientific Reports* (Nature), *IET Quantum Communication*, and IEEE Access. He is currently an Associate Editor of IEEE Canadian Review.