Hindawi
Security and Communication Networks
Volume 2022, Article ID 3370408, 12 pages
https://doi.org/10.1155/2022/3370408

Research Article

5G and Blockchain Enabled Lightweight Solutions for Containing COVID-19

Mohsin Kamal[1] **Abdulah Jeza Aljohani**[2,3] **Eisa Alanazi**[4] **and Fahad R. Albogamy**[5]

[1] *KIOS Research and Innovation Center of Excellence, University of Cyprus, Nicosia 1678, Cyprus*
[2] *Department of Electrical and Computer Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[3] *Center of Excellence in Intelligent Engineering Systems (CEIES), King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[4] *University of Umm Al-Qura, Makkah, Saudi Arabia*
[5] *Computer Sciences Program, Turabah University College, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*

Correspondence should be addressed to Mohsin Kamal; kamal.mohsin@ucy.ac.cy

Received 6 August 2021; Accepted 3 December 2021; Published 15 February 2022

Academic Editor: Muhammad Ahmad

Due to the global pandemic of COVID-19, there is an urgent need to utilize existing technologies to their full potential. Internet of things (IoT) is regarded as one of the most trending technologies with a great potential in fighting against the coronavirus outbreak. In this study, we examine the current status of IoT applications related to COVID-19, identify their deployment and operational challenges, and suggest possible opportunities to further contain the pandemic. Furthermore, we perform analysis by examining the IoT implementation in which internal and external factors are discussed. We suggest by presenting results that lightweight security algorithms, blockchain-based solutions for enabling end-to-end security and privacy, and 5G for IoT devices to tackle the bandwidth issues for scalable IoT networks are few of the solutions in containing the COVID-19.

1. Introduction

The Internet of things (IoT) consists of a complex network of smart devices that frequently exchange data over the Internet [1]. It has renovated the actual world objects into clever virtual objects. The goal of IoT is to unite everything in our world under a mutual arrangement, helping the users in not only controlling the objects around them but also keeping them up to date about the state of things [2]. IoT devices sense the environment and send the acquired data to the Internet cloud without the requirement of human-to-human or human-to-machine interaction. IoT has become an integral part of today's modern era of communication where tens of millions of devices are connected via IoT and the number is growing rapidly [3].

IoT has the potential to play a vital role in various fields of life, such as health systems [4], autonomous vehicles [5], home and industrial automation [6], intelligent transportation [7], and smart grids [8]. Sensors obtain data of related information from the environment and use the Internet cloud as a medium of delivering information to the relevant body or organization [9]. The core concept behind IoT is the realization of multiple devices communicating with each other seamlessly. This has the promise of better utilization of available resources, reduction in cost, and minimizing manual interaction. As the 2019 coronavirus disease (COVID-19) continues to spread across the globe, it is inevitable to discuss and articulate the IoT potential during pandemics. As of August 6, 2021, the number of COVID-19-confirmed cases has exceeded 80 million [10]. Researchers from different fields continue to investigate and generate diverse solutions, which could help in combating the COVID-19 [11].

IoT comes up with the ingredients needed to help the countries in minimizing the effect of COVID-19. IoT has a wide range of applications, which would be effective to make sure that all the guidelines of safety and precautions provided by health officials are followed. IoT has a scalable network, which has the potential to deal with huge amount of data received from sensors used by number of applications to fight against COVID-19. Furthermore, the reliable IoT networks decrease the delivery time of crucial information, which can help in providing timely response during the global pandemic of COVID-19 [12]. The role of IoT was never needed to the extent to which it is required now because of coronavirus outbreak.

The key contributions of this study are as follows:

(i) This study discusses the effectiveness of IoT in combating the global pandemic of COVID-19

(ii) Several scenarios are examined in which IoT can help in reducing the outbreak of coronavirus

(iii) We have analyzed the possible challenges that the IoT-based solutions encounter in combating the coronavirus

(iv) We present the solutions for the challenges by providing the results

The rest of the study is organized as follows. Section 2 presents the important applications of IoT in the perspective of COVID-19. The challenges in implementing the IoT are described in Section 3. The SWOT analysis is performed in Section 4. The solutions to tackling the challenges in deploying the IoT are presented in Section 5. The study is concluded in Section 6.

2. Applications of IoT to Combat COVID-19

The seamless connections and vigorous integration with other technologies have enabled the IoT to be one of the promising technologies that will change our lives [13]. The applications of IoT in combating this global pandemic can be spread to several sectors, which can play a major role in reducing the risk of coronavirus outbreak [14]. Figure 1 shows potential applications in which IoT technologies can be useful and effective in combating the COVID-19. The following subsections will examine the capability of the IoT in fighting against COVID-19.

2.1. Internet of Health Things and Digital Telehealth. Internet of Health Things (IoHT) is an application of IoT, which aims to connect patients to healthcare facilities to monitor human body vital signs using communication infrastructure [15]. Telemedicine is getting popular in remote areas where accessibility to a quality physician is limited due to different factors. For example, heart rate, electrocardiography, diabetes, and vital body signs can be remotely monitored without the physical presence of patients [16]. An example of the remote data acquisition using IoHT system is shown in Figure 2. The sensors and actuators receive data from patient and send the information to the cloud using a local gateway. The doctor examines the data using any mobile or desktop application provided to them and notifies the patient or medical staff taking care of the patient about the report [17].

Telehealth can play a very important role during the COVID-19 outbreak [18]. A portal is created where patients interact with the doctors and the treatment is provided remotely. The benefit of employing a secured IoHT system in COVID-19 is that the physicians do not come in direct contact with the patients, hence avoiding the spread of virus [19]. Many countries have started operating the digital telehealth in this time of crisis. Health Arc [20] is used in the USA, Canada, and United Kingdom, which provides IoT-based healthcare devices to the patients whose data are continuously monitored by the medical staff. The data are analyzed, and the suggestions and prescription are provided to the patients on their mobiles or tablets. ContinuousCare provides services in India [21], HealthNet Connect [22] is used in six different states of the USA, and SehatYab [23] providing services in Pakistan is among the leading telehealth service providers. A person with COVID-19 symptoms can use assessment tool provided on the digital platform such as “COVID-19 Gov PK mobile app” [10] provided by the government of Pakistan, which is accessed by the physicians remotely. Using this tool, patients are timely guided and many precious lives can be saved. Furthermore, it also serves to reduce the number of hospitalizations, readmissions, and density of patients in hospitals, all of which help in improving the quality of life and providing timely treatment to COVID-19 patients.

2.1.1. IoT-Enabled Ambulances. Medical staff associated with ambulances are usually dealing with very high-pressure and error-prone situations [24]. During the current pandemic of COVID-19, the situations have become even more tensed and pressurized for medical staff dealing COVID-19 patients. The IoT-aided ambulances offer an effective solution in which remote medical experts suggest necessary actions to the medical staff dealing with the patient in the ambulance. This leads to the timely response and effective handling of patient. Figure 3 shows the smart ambulance, which is equipped with IoT-based technology. WAS vehicles [25] provide smart solution-based emergency vehicles. The radio-frequency identification (RFID)-based equipment is connected to wireless local area network (WLAN). The information of patient is remotely accessible by the concerned medical staff.

2.1.2. IoT-Enabled Healthcare and Safety Devices. IoHT-aided equipment is classified into two categories, i.e., personal and clinical [26]. Personal-aided IoHT gadgets are used for self-monitoring of health [27]. The most common gadgets used are Apple watch [28] and Fitbit [29]. The user tracks the heartbeat, exercise, sleep, nutrition, and weight using these gadgets. These are useful in fighting against COVID-19 as well because rest and sleep become very important factors for the patients suffering from this disease. The patient can see his reports on the portals provided by these gadget makers and provide information to the related physicians if required. IoT-based wearable gadgets can help in reducing the spread of coronavirus if certain algorithms are implemented to the existing devices. The wearable devices notify in real time if

(i) The social distancing protocol is violated

(ii) Any COVID-19 patient is in the locality

(iii) The area was declared as danger zone by the government in the perspective of coronavirus outbreak

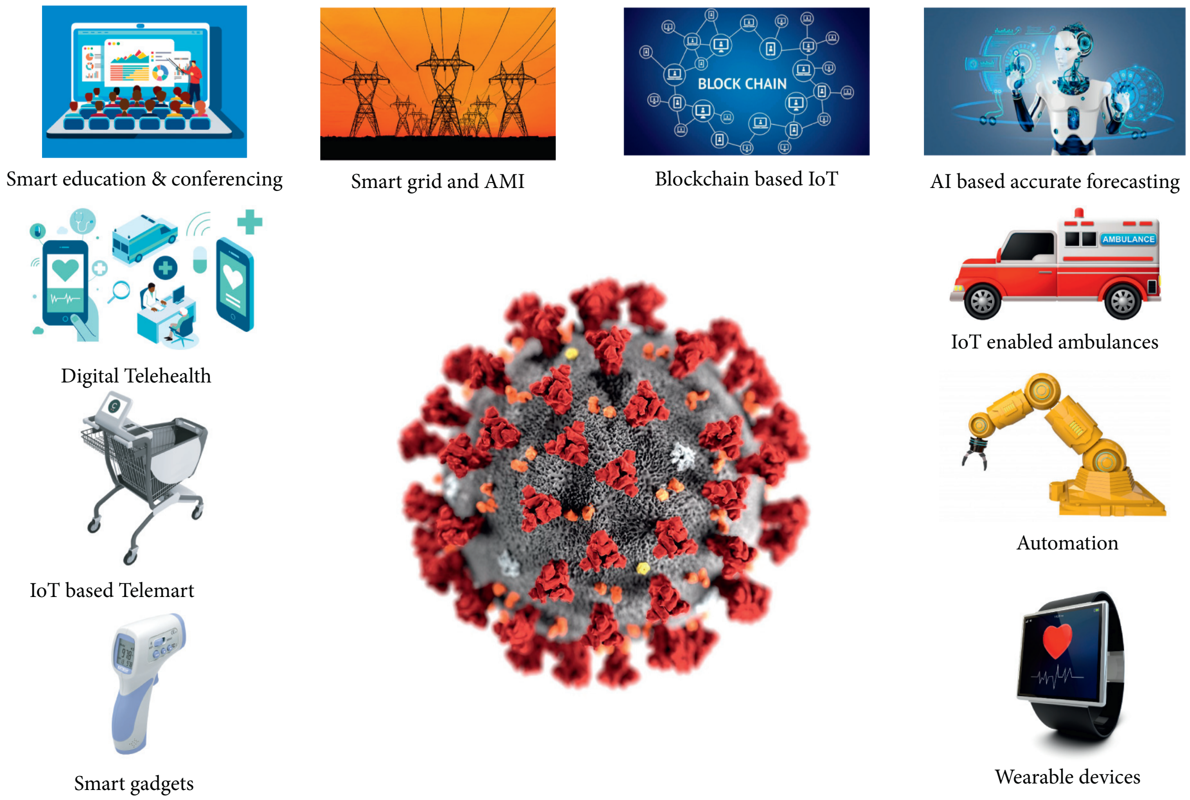


Figure 1: Potential IoT applications to combat COVID-19.

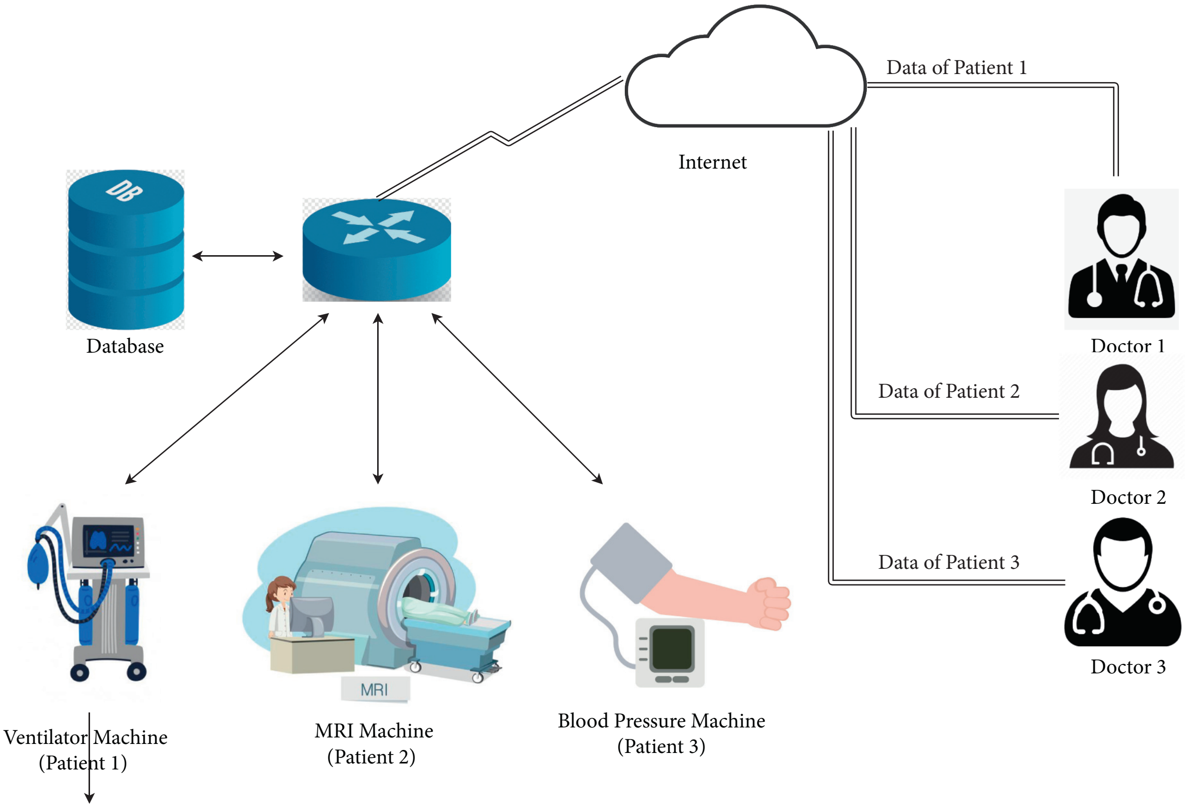


Figure 2: Remote examination of medical patients by the doctors in IoT.

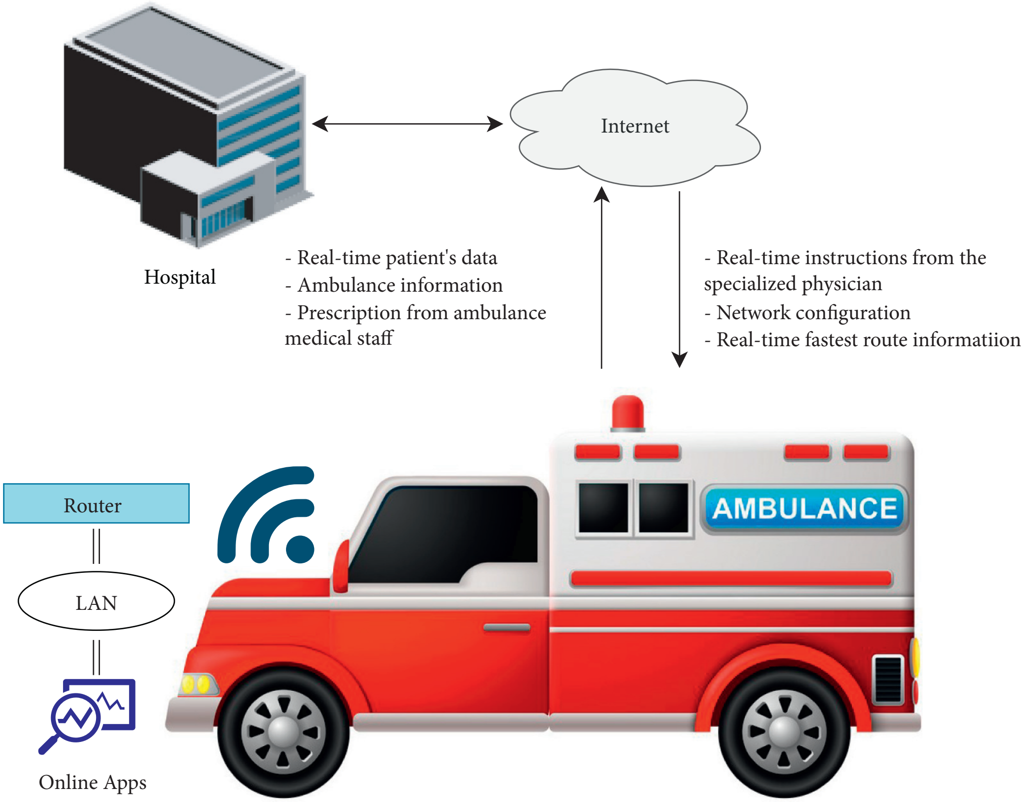

Hospital
Internet
- Real-time patient's data
- Ambulance information
- Prescription from ambulance medical staff
- Real-time instructions from the specialized physician
- Network configuration
- Real-time fastest route informatiion
Router
LAN
Online Apps
AMBULANCE

Figure 3: IoT-based smart ambulance system.

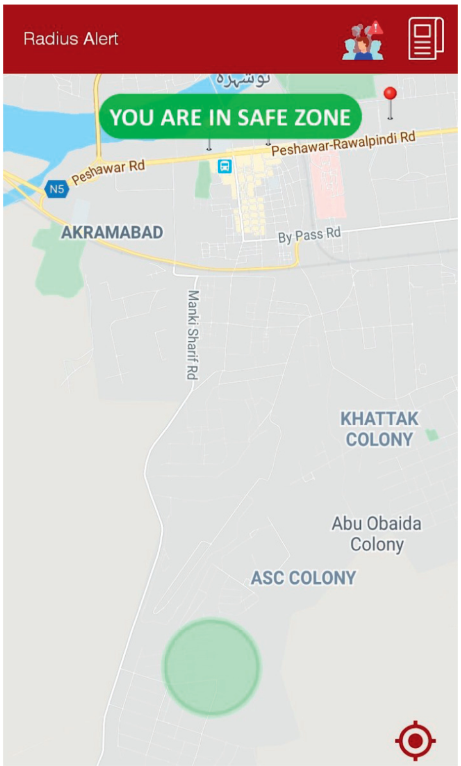
Figure 4 shows the presence of user in safe zone [10]. If a user moves in the area, which is danger zone with respect to COVID-19 patients, the device intimates in real time and user can maximize precautions to stay safe from coronavirus. Apple and Google have recently partnered in developing a contact tracing technology, which helps in reducing the spread of coronavirus [30, 31]. The app is downloaded on the phone in which the data of user are inserted manually. The app neither shares the location of the user nor shares the user's identity. The technology disguises the user's identity by generating a random sequence of numbers that change after every few minutes. Using Bluetooth, the user's phone detects any other phone in proximity, which also has opted for the app. Both phones exchange these random numbers. The user, if tested positive for COVID-19, updates this information in the app. Every phone that was in contact with the COVID-19 patient's phone in last 14 days get notification that they were in contact with COVID-19 patient and should quarantine themselves. Singapore has made it compulsory for all the arriving passengers to wear monitoring wristbands to contain the spread of COVID-19. The wristband uses Global Positioning System (GPS) and Bluetooth to help the authorities in identifying the location of the user. The authorities will be able to ensure that the arriving passengers follow the quarantine rules defined by the government [32].

Clinical IoHT includes the monitoring of person under the supervision of physician as shown in Figure 2. A list of IoT-enabled clinical applications is presented in [33]. The list includes devices to monitor the spread of cancer, continuous glucose monitoring, connected inhalers, asthma monitor, and many more. During this global pandemic, many healthcare gadgets can provide opportunities of real-time remote supervision. These gadgets are smart enough to provide results, which can be seen remotely by medical staff [34]. There are limitations to these clinical IoHT devices as well, which may cause unreliable results [35]. It can have a system to activate alarm if any unforeseen situation occurs. In the perspective of COVID-19, IoT-based ventilators and temperature monitors can help in providing the timely assistance to patients. The patient status can be monitored remotely if ventilators are connected to the cloud. The IoT-based temperature monitoring device can help in keeping the real-time record of everyone in the database. The record can be checked in later date if required [36].

3. Challenges of IoT in the Wake of COVID-19

Implementing IoT is never an easy task to perform. Furthermore, when implementing IoT for COVID-19, there are many challenges involved, few of which are described below.

3.1. Scalability. With the advent of digital technology, the number of IoT devices is growing exponentially [37]. The reason is that they are not limited to only one application, but there are many applications of IoT, which are in practice these days. According to a recent survey, there is a massive


Radius Alert

YOU ARE IN SAFE ZONE

Figure 4: Real-time area monitoring for COVID-19 patients.

increase in the use of home automation appliances from 2018 to 2022 [38]. The trend is represented in Table 1.

Scalability is a big challenge in implementing IoT to fight against the global pandemic of COVID-19. A large number of devices are required in IoHT alone to accurately sense the vital signs of the patients and forward those to the Internet cloud. As for now, the active cases are approximately 3.7 million worldwide. Each IoT gadget needs to have multiple sensors. Implementing IoT for this highly scaled scenario is a big challenge. The devices required are large in number, and large amount of data will float around these small IoT nodes.

Forecasts show that the IoT connections will double from 2019 to 2024 by reaching 24 billion [39]. Currently, there are no cases reported in which the scalability was an issue to interrupt seamless transmission of IoT devices, but the reports show that the Internet usage has been increased to 60% during the pandemic [40]. The IoT devices in health care have not yet been groomed to its full potential, but the demand will increase with time [41]. Due to scalability, the energy requirements and the need of accurate real-time performance in noisy environment have also increased [42]. With the sheer volume of data generated by a large number of distributed sensors, another challenge is to capture, integrate, store, and process the data [43]. Most of the healthcare IoT systems use rechargeable batteries, which have a very short life span. One potential approach to prolong the lifetime of the battery is to harvest energy [44].

Table 1: Expected growth in domestic IoT applications from 2018 to 2022 (in million units).

System	2018	2022	Growth (%)
Video entertainment	310.5 m	457.5 m	10
Home monitoring and security	97.7 m	244.9 m	26
Smart speakers	99.8 m	230.5 m	23
Lighting	37.7 m	104.6 m	29
Thermostats	13.6 m	37.5 m	29
Others	84.5 m	189.3 m	22

3.2. Security and Privacy Issues.

Due to the scalability and energy limitations of IoT devices, the security solutions should be energy-efficient and algorithms defined to secure the IoT network should have less computational complexities to offer end-to-end data protection, consumer privacy, and secure authentication [45, 46]. Thus, lightweight security algorithms need to be designed in order to implement security in IoT. With the outbreak of coronavirus, the security requirements of IoT-enabled networks have increased. The security should be enabled for both three-layered and service-oriented architectures of IoT [47]. The security concerns in implementing IoT with respect to COVID-19 are as follows:

(i) The data that are sent from the sensors attached to the body of COVID-19 patient should be accurate

(ii) The data should successfully reach the destination

(iii) The data should not be forged

(iv) The data should not be intercepted from the communication path

(v) The data stored in the memory of the IoT device should not be accessible to everyone

The security primitives should be taken considering IoT devices, which have low computational capabilities. Besides being lightweight, the required security algorithms should be accurate and must be able to keep user's trust intact [9]. Security primitives include specific attack detection, channel state masking, intrusion detection, localization, and data provenance. A single change to the data can cause major problems. For example, if any misleading change in medical health reports of COVID-19 patient generated by IoT devices is sent to doctors, then it can cause major problems during the global pandemic of COVID-19. Ensuring the trust of both IoT healthcare device user and medical staff receiving the reports from the remote devices is a big challenge.

With the advancement in AI and ML, many new doors have opened up for the researchers to contribute to reducing the spread of COVID-19. The use of these technologies is specifically promising in contact tracing. Besides all the advantages, the advent of these technologies has raised ethical challenges. The surveillance of social contact has caused the fear of disrupting the commitment of privacy and autonomy of social groups [48]. One of the biggest challenges is to provide solutions to the community without compromising the privacy and user's trust.

3.3. Limited Spectrum and Bandwidth.

As the number of IoT devices is increasing, more bandwidth is required to send all the information from sensors to the cloud. At present, most of the IoT devices use the licensed spectrum offered by the mobile operators. With the growth of these devices, the bandwidth requirements have also increased. The data face latency in Internet protocol (IP) networks, which sometimes cause erroneous data transfer because the data packet is retransmitted if it fails to reach the destination initially. So, latency might occur due to the number of retries establishing a connection and transmitting the message, due to the nature of the protocol to reliably transmit data. Currently, many IoT devices use 4 G/LTE networks to perform their tasks. This limited spectrum of 3 G/LTE/4G will soon be not enough for large number of IoT devices [49].

During the pandemic of COVID-19, timely transfer of data from IoT devices to the concerning body is of utmost importance. Errors or delay in data may cause loss of precious human lives. If the bandwidth is high, the problems of latency and low data rates can be overcome.

4. Strength, Weakness, Opportunity, and Threat Analysis

Strength, Weakness, Opportunity, and Threat (SWOT) analysis for IoT is shown in Table 2. The internal factors are comprised of strengths and weaknesses, which are limited to the organizations or researchers who want to implement IoHT. The internal factors can be changed with time. Opportunities and threats are considered as external factors, which depend on the market and cannot be changed [50].

4.1. Strengths. Considering COVID-19 as test case, the accuracy of data in IoT is one of the strengths in implementing it. The sensors take real-time data from the environment and send it to the cloud [51]. This results in helping the patients to get on-time treatment, which can save many lives. If anyone has symptoms of COVID-19 and needs to consult physician, then IoT helps in providing platform of telehealth in which a person can take the advice of physician without visiting the hospital or clinic. This refers to the timely diagnosis of COVID-19. IoT can help in spreading the awareness related to the information and safety measures to take preemptive measures against coronavirus. Due to the importance of IoT to combat against the current global crisis of coronavirus, there is a high demand of IoT-based systems [52]. Integrating AI with IoT can help in better forecasting future needs to fight against COVID-19.

4.2. Weaknesses. The shortcomings and weaknesses cannot be ignored while considering the implementation of IoT to combat against this virus. Due to the requirements of large number of IoT devices and scalability, the data processing units should have high processing power. The data centers should be more to keep record of patients and related information. The whole IoT network should be highly secured, and the security algorithms should be designed in such a way that complexity is kept as low as possible [53]. As many devices will be sending data frequently to the cloud, the requirements of high bandwidth cannot be ignored. The mechanism should be designed where limited spectrum should be efficiently used. This can be done by frequency planning and reuse mechanism.

4.3. Opportunities. The opportunities are huge by implementing IoT to combat this global crisis of COVID-19. With the increase in IoT applications, the IoT industry can help in providing the jobs in local markets and effectively take its part in boosting the economy of any country. The use of millimeter wave (mmWave)-based 5G has not yet come into play for IoT networks, which provides large bandwidth and high data rate. The implementation of IoT can bend the tech giants toward the use of this large bandwidth mmWave, which operates between 3 GHz and 300 GHz [54]. This will open new doors in many areas of wireless communication networks. Currently, software-defined radios, cognitive radio networks, and cooperative communication can be applied in existing IoT networks to efficiently use the spectrum by sensing the empty spaces in licensed bands and using them for its operations.

4.4. Threats. The threats as external factors are few comparatively. Currently, IoT devices are compatible with the manufacturer of the same vendor [55]. There is a dire need of compatibility to develop competition among the vendors by integrating the platforms. This will help in the integration of different applications and services, which will increase the quality of IoT operations, and the applications will evolve with time. Besides, the range of unlicensed bands is very less. Most of the communication in IoT either uses cellular network or 2.4 GHz of Industrial, Scientific, and Medical (ISM) frequency band, which may cause interference if proper planning is not performed [56].

5. Solution to the Challenges in Combating COVID-19

The challenges involved in implementing the scalable IoT networks are undeniable, but solutions to these challenges are present in the literature, which can help in successfully deploying the IoT networks [9, 57]. Some of the prominent solutions are presented in the following subsections.

5.1. Lightweight Security Algorithms for Scalable IoT. Due to scalability, most of the IoT devices to measure vital signs are small in size and easily accessible. Measures must be taken to ensure that the data are protected and are efficiently received at the destination. In most cases, most of these healthcare IoT devices are not physically protected, so data security and provenance serve as the backbone for implementing IoT networks. Data can be easily forged if the proper security primitives are not used.

Various metrics such as angle of arrival, time of arrival, phasor information, and received signal strength indicators (RSSIs) can be used to develop lightweight security algorithms for IoT devices. Wireless channel characteristics of IoT healthcare devices are used to design the algorithms, which (i) protect the IoHT devices and (ii) due to their low

Table 2: SWOT analysis of IoT in the perspective of global pandemic.

Internal factors	
Strengths	Weaknesses
Accuracy of data	High processing server/fusion centers are required
On-time treatment	Scalability of IoT devices
Timely diagnosis	Huge data centers and data aggregation
Information of safety measure	Security and privacy preservation
High demand of IoT-based systems	High bandwidth requirements
Accurate forecasting	Limited spectral resources
External factors	
Opportunities	**Threats**
Creation of awareness about the requirement of IoT	Compatibility of devices
Creation of jobs	Use of unlicensed bands
Toward 5G for higher bandwidths	
Software-defined radios	
Cooperative communication	

computational complexities work efficiently in scalable environments. Figure 5(a) shows the RSSI variations of connected IoT devices, while Figure 5(b) provides a better insight by applying the Savitzky–Golay filter to the results achieved in Figure 5(a). In case of no adversary in the IoT network, there is a linear relationship between the RSSI variations. The RSSI values are converted into binary streams by quantification. The binary stream is referred to as the link fingerprints. These link fingerprints are encoded with symmetric key, and the resultant is sent to the server where it computes the Pearson correlation coefficient using the link fingerprints of connected IoT devices.

The computation of the Pearson correlation coefficient (PCC) is a very simple technique yet very accurate to detect any adversary in the IoT network [9]. The PCC is computed for both attack and non-attack scenarios, which are achieved as 0.9762 and 0.0632, respectively. Figure 5(c) presents the scenario when the IoHT is under attack and the communication path is changed. The communication between IoHT devices 1 and 2 is via an adversary. The RSSI variations are not linear, and hence, low PCC is computed. Applying the designed algorithms, the energy consumption of these IoT healthcare devices is as low as 26.99 mJ for 128 bit key size. This helps in prolonging the battery life of small IoT devices because the energy dissipation is very less. Some of the notable lightweight security algorithms present in the literature are summarized in Table 3.

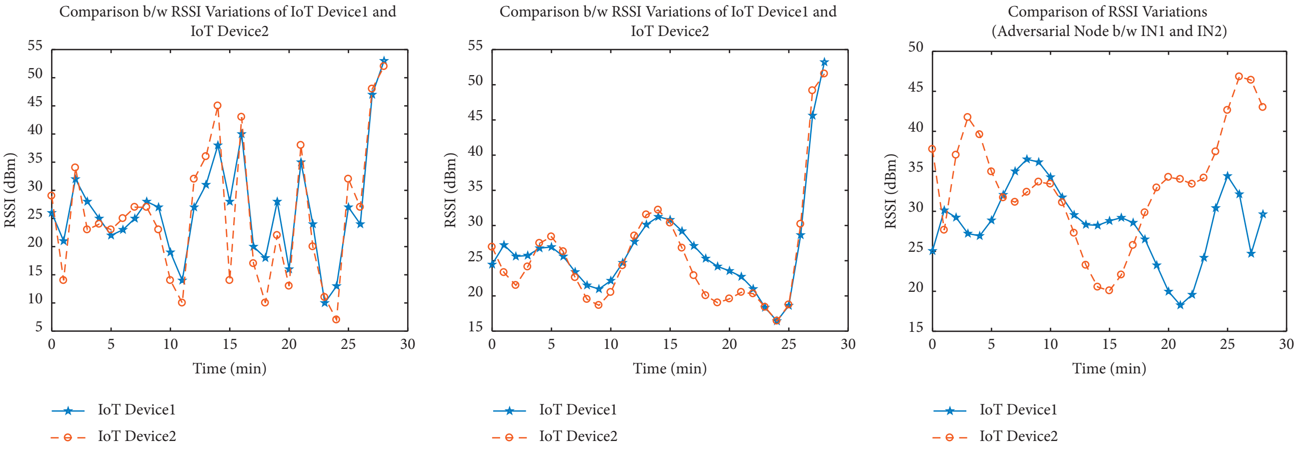
5.1.1. Blockchain for Connected Healthcare Units and Privacy Preservation. Blockchain is the rapidly growing technology, which became famous because of a virtual currency called Bitcoin. The use of blockchain is expanded to many fields [61]. Blockchain enables privacy and security for data sharing [62, 63]. A blockchain-based IoT system presented in [64] stores the private key at IoT device, while the public keys are stored at Ethereum. Blockchain can be implemented for connected healthcare units as shown in Figure 6 in which all healthcare units are connected to each other. Each healthcare unit acts as a block, and accurate data transfer is made possible by implementing blockchain-based IoT network. For example, the medical record of a patient received from one healthcare unit to another can be verified by generating a HASH and comparing it with all the HASH values present in the ledger.

Blockchain technology can also be used to secure end-to-end data. The security and privacy preservation are made sure if IoT is integrated with blockchain. Important data of medical records and the record of all available healthcare kits and other resources are verified by any official by checking whether the record is in its authentic form or is it forged. The SHA2 algorithm is applied on the data along with the private key (K) associated with medical healthcare unit, nonce (N), and previous hash (HASH_p). Mathematically,

$$\mathrm{HASH} = \mathrm{SHA1}\left(\mathrm{Data}, K_i, N_i, \mathrm{HASH}_p\right). \quad (1)$$

A difficulty level (d) is selected based on which the miners mine the data and add it to the blockchain. In 1, N is iterated until the HASH is achieved according to the d. Figure 7 shows that as the payload size increases, the mining time also increases. For a 10 kB data, if the $d = 3$, the achieved mining time of a single miner is less than 0.2 seconds. The trade-off is between the data size and d, i.e., if the data size is high, d should be low. All HASH values are sent to the cloud where a distributed ledger is created. The data can be checked in later date for its authentication. Even a single-digit change in the report generates a different hash. Due to this, any forgery can be detected.

This can be applied to the supply chain in which each supply point becomes a block and adds its hash to a decentralized ledger. The data (which could be the count of equipment) can be verified at any stage or precisely at the destination by looking at the HASH values in the ledger. If all HASH values match, then the supply has reached successfully. Figure 8 shows the same procedure in which the ledger is updated with the HASH values generated by each block. At each block, the HASH is verifiable, while in the last block, the data are slightly changed and a different HASH is generated. While at the ledger, the HASH values generated and presented at the ledger are not matched with the HASH of block number 3.

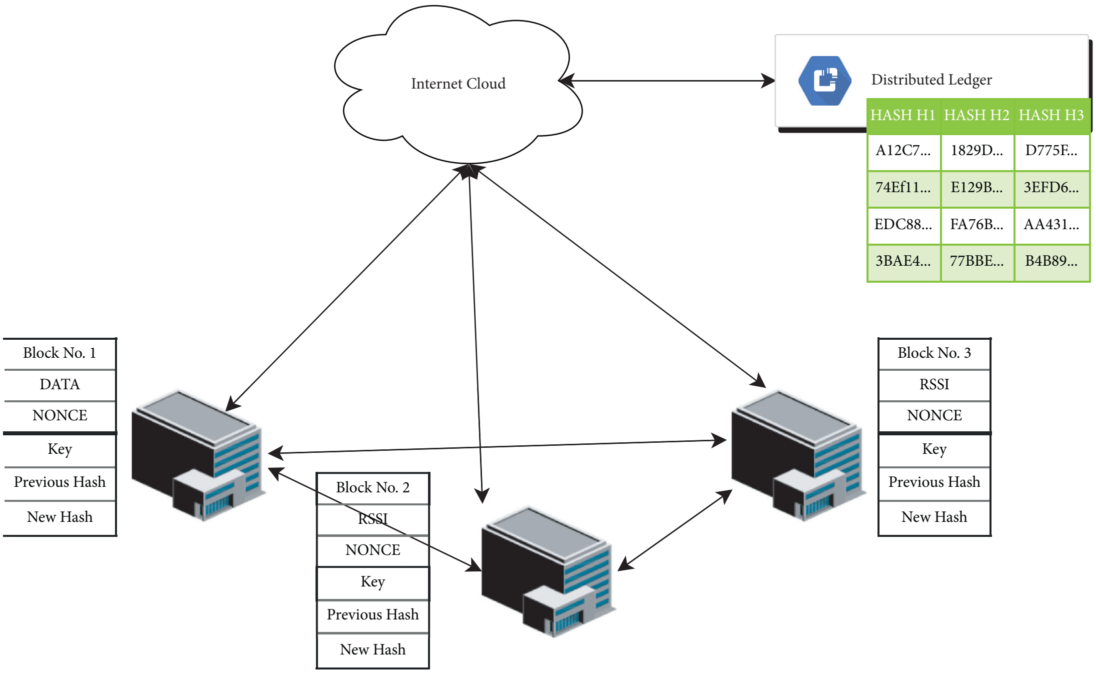


(a) (b) (c)

Figure 5: Comparison of RSSI values achieved from connected IoT devices in both attack and non-attack cases. (a) RSSI variations of connected IoT devices. (b) Applying the Savitzky–Golay filter to RSSI variations in (a). (c) Adversary in between IoT nodes.

Table 3: Lightweight security algorithms in the literature to combat various attacks in IoT network.

Security requirements	Gope and Sikdar [58]	Dong et al. [59]	Ali et al. [60]	Kamal and Tariq [9]
MITM attack	✓	✓	✓	✓
Jamming	✓	×	✓	✓
Data tempering	×	×	✓	✓
Replay attack	✓	×	×	×
Location proximity	×	×	×	✓
Data provenance	×	×	✓	✓



HASH H1	HASH H2	HASH H3
A12C7...	1829D...	D775F...
74Ef11...	E129B...	3EFD6...
EDC88...	FA76B...	AA431...
3BAE4...	77BBE...	B4B89...

Figure 6: Blockchain-based connected healthcare units.

5.2. Toward 5G for Higher Bandwidth. With the advent of IoT, the demand of bandwidth has increased. For the organizations working on deploying IoT devices, the bandwidth shortage has motivated them in the exploration of the underutilized mmWave frequency spectrum for future IoT networks. mmWave ranges from 3 GHz to 300 GHz [54].

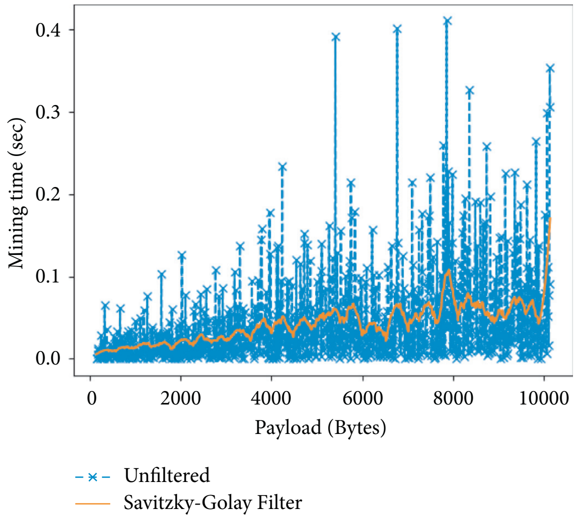
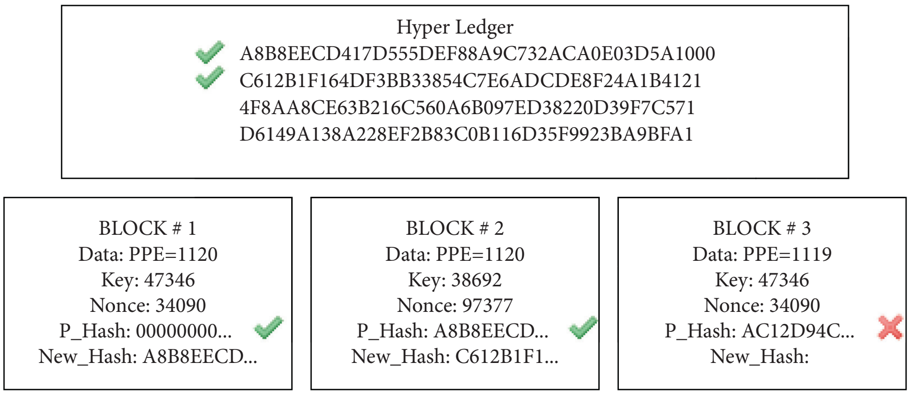


FIGURE 7: Blockchain-based connected healthcare units.



Hyper Ledger

✓ A8B8EECD417D555DEF88A9C732ACA0E03D5A1000
✓ C612B1F164DF3BB33854C7E6ADCDE8F24A1B4121
4F8AA8CE63B216C560A6B097ED38220D39F7C571
D6149A138A228EF2B83C0B116D35F9923BA9BFA1

BLOCK # 1
Data: PPE=1120
Key: 47346
Nonce: 34090
P_Hash: 00000000... ✓
New_Hash: A8B8EECD...

BLOCK # 2
Data: PPE=1120
Key: 38692
Nonce: 97377
P_Hash: A8B8EECD... ✓
New_Hash: C612B1F1...

BLOCK # 3
Data: PPE=1119
Key: 47346
Nonce: 34090
P_Hash: AC12D94C... ✗
New_Hash:

FIGURE 8: Blockchain-based security showing mismatch of hash in ledger for block number 3.

Spectrum at 28 GHz, 38 GHz, and 70–80 GHz looks especially promising for next-generation cellular systems. Because of large bandwidths, multi-gigabits per second can be achieved. 5G using mmWave spectrum provides promising benefits in other application scenarios such as wearable networks, vehicular communications, or autonomous robots [65].

As the frequency spectrum range is broad, more bandwidth is available at these frequencies. The capacity (C) is increased, which solves the problem of scalability in IoT networks because mathematically,

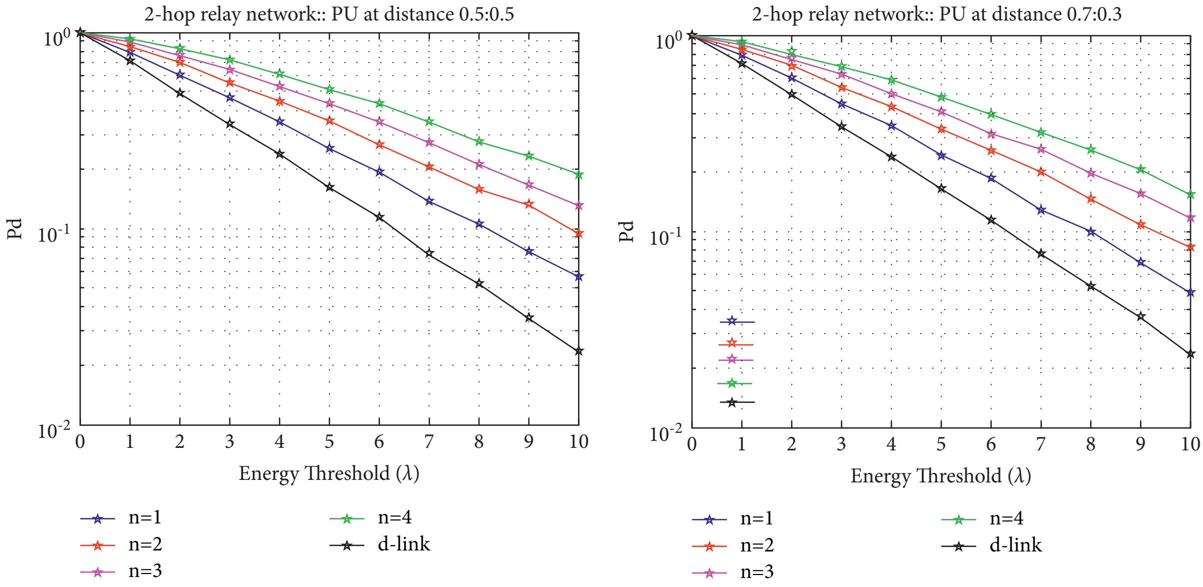
$$C = \mathrm{BW} \times \log_2 (1 + \mathrm{SNR}), \tag{2}$$

where BW represents the bandwidth and SNR is the signal-to-noise ratio. Due to higher attenuation in free space, the same frequency is reused at shorter distances. The security and privacy are better because of the limited range and narrow beamwidths [66]. As the frequency is high, then the wavelength is small, and hence, small antenna size helps in integrating the large array of antennas on a chip or printed circuit boards (PCBs). The comparison [67] of 3G and 4G (existing solutions for IoT to send sensor data to cloud) with the 5G is presented in Table 4. It is evident that moving to 5G will help in the better performance of IoT devices [68], specifically in IoHT, where the low latency and high data rate are key factors for efficient and effective performance.

5.2.1. Cognitive Radio-Enabled IoT. Cognitive radio merged with IoT is called cognitive radio IoT (CRIoT) [57]. Spectrum allocation is always been done traditionally in a licensed fashion. It has been observed that most of the licensed spectrum is not completely utilized. Cognitive radios are proposed as a viable solution to the frequency reuse problem [69]. While using cognitive radio parameters, IoT devices are capable of sensing the environment and adjusting the configuration parameters automatically [70]. The IoT devices sense the availability of free spectrum referred as holes in the spectrum and communicate in the sensed holes without interfering with the licensed user called primary user (PU) [71]. This helps in uninterrupted data communication and efficient utilization of licensed spectrum.

Table 4: Comparison of 3G, 4G, and 5G technologies.

Parameter	3G	4G	5G
Frequency range	1.8 – 2.5 GHz	2 – 8 GHz	3 – 300 GHz
Latency	100 – 500 ms	20 – 30 ms	<10 ms
Data rate	2 Mbps	2 Mbps – 1 Gbps	>1 Gbps



(a)

(b)

Figure 9: P_d for the various cases based on the position of relay in CRIoT. (a) Relay is equidistant from PU and SU. (b) Relay is placed close to SU and far from PU.

This can be achieved by deploying relays in the CRIoT. The relays sense the spectrum and provide the unused bands to the secondary users (SUs). The real challenge arises in the deployment of these relays, i.e., where to place these relays. The simulations are performed for various test cases in which energy of the spectrum is sensed against a defined (T_d). The results are presented in Figure 9 in which it is observed that as the relays are placed closer to the SU and away from PU (Figure 9(b)), the probability of detection (P_d) of sensing the PU in the CRIoT decreases.

6. Conclusion

During the outbreak of the global challenge of COVID-19 pandemic, the reliance on technologies such as IoT, AI, blockchain, big data analytics, and cloud computing has increased. IoT plays a major role in reducing the risks of coronavirus spread by providing platforms, which help in following the protocols defined by WHO. IoT-based healthcare units provide timely response by medical staff to deal with COVID-19 patients. Blockchain-based IoT networks help in better management of the supply chain and detect any forgery in data. The challenges in implementing IoT networks cannot be ignored. To deal with the scalability, 5G using mmWave-based communication system provides support to enable end-to-end communication. The need for lightweight security is also obvious because the IoT devices are small in size and large in number. The solution suggests to implement algorithms, which have less computational cost.

Data Availability

The data are available upon request to Dr. Mohsin Kamal (kamal.mohsin@ucy.ac.cy).

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding this study.

Acknowledgments

The authors would like to acknowledge the support from Taif University Researchers Supporting Project Number (TURSP-2020/331), Taif University, Taif, Saudi Arabia. This work was supported by the Ministry of Health (MoH), Saudi Arabia, Grant No. 935. The authors, therefore, gratefully acknowledge the MoH technical and financial supports. Furthermore, the previous version of this manuscript is present as arXiv at Cornell University's website (https://arxiv.org/abs/2007.12268) [72].

References

[1] C. R. Srinivasan, B. Rajesh, P. Saikalyan, K. Premsagar, and E. S. Yadav, "A review on the different types of Internet of Things (IoT)," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 11, no. 1, pp. 154–158, 2019.

[2] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: a systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[3] M. A. A. Garadi, A. Mohamed, A. K. A. Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, 2020.

[4] K. D. Saranya, R. Krishnamurthy, K. N. H. Srinivas, T. S Rao, and I. S. Amiri, "IoT-based health monitoring system using beaglebone black with optical sensor," *Journal of Optical Communications*, vol. 1, 2019.

[5] D. Minovski, C. Åhlund, and K. Mitra, "Modeling quality of IoT experience in autonomous vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3833–3849, 2020.

[6] S. Aheleroff, X. Xu, Y. Lu et al., "IoT-enabled smart appliances under industry 4.0: a case study," *Advanced Engineering Informatics*, vol. 43, Article ID 101043, 2020.

[7] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-based lightweight and secured V2V communication in the internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 3997–4004, 2021.

[8] X. C. Yin, Z. G. Liu, L. Nkenyereye, and B. Ndibanje, "Toward an applied cyber security solution in IoT-based smart grids: an intrusion detection system approach," *Sensors*, vol. 19, no. 22, p. 4952, 2019.

[9] M. Kamal and M. Tariq, "Light-weight security and data provenance for multi-hop Internet of Things," *IEEE Access*, vol. 6, Article ID 34439, 2018.

[10] Ministry National Health Services, "COVID-19 Global," 2021, http://covid.gov.pk/stats/global/.

[11] S. Mavrikou, G. Moschopoulou, V. Tsekouras, and S. Kintzios, "Development of a portable, ultra-rapid and ultra-sensitive cell-based biosensor for the direct detection of the SARS-CoV-2 S1 spike protein antigen," *Sensors*, vol. 20, no. 11, 2020.

[12] Z. Allam and D. S. Jones, "On the coronavirus (COVID-19) outbreak and the smart city network: universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management," *Healthcare*, vol. 8, no. 1, p. 46, 2020.

[13] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in iot security: current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, 2020.

[14] N. Saeed, B. Ahmed, T. Y. A. Naffouri, and M.-S. Alouini, "When Wireless Communication Faces COVID-19: Combating the Pandemic and Saving the Economy," 2020, https://arxiv.org/abs/2005.06637.

[15] J. J. P. C. Rodrigues, D. B. D. R. Segundo, H. A. Junqueira et al., "Enabling technologies for the Internet of health things," *IEEE Access*, vol. 6, Article ID 13129, 2018.

[16] J. E. Hollander and B. G. Carr, "Virtually perfect? Telemedicine for COVID-19," *New England Journal of Medicine*, vol. 382, no. 18, pp. 1679–1681, 2020.

[17] A. Poppas, J. S. Rumsfeld, and J. D. Wessler, "Telehealth is having a moment: will it last?" *Journal of the American College of Cardiology*, vol. 75, 2020.

[18] A. C. Smith, E. Thomas, C. L. Snoswell et al., "Telehealth for global emergencies: implications for coronavirus disease 2019 (COVID-19)," *Journal of Telemedicine and Telecare*, vol. 26, Article ID 1357633X20916567, 2020.

[19] B. Siwicki, "Updated: a guide to connected health device and remote patient monitoring vendors," 2020, https://www.healthcareitnews.com/news/guide-connected-health-device-and-remote-patient-monitoring-vendors/.

[20] Health Arc, "Remote patient monitoring made easy," 2019, https://web.healtharc.io/.

[21] Continious Care, "Better health outcomes guaranteed," 2021, https://www.continuouscare.io/remote-monitoring/.

[22] HealthnetConnect, "Healthcare Delivery, remimagined," 2021, https://healthnetconnect.com/.

[23] Sehatyab, "Tele-medicine to resuscitate primary care in pakistan," 2021, https://sehatyab.com/hazarnaimat/tele-medicine-resuscitate-primary-care-pakistan/.

[24] E. Park, J. H. Kim, H. S. Nam, and H. J. Chang, "Requirement analysis and implementation of smart emergency medical services," *IEEE Access*, vol. 6, Article ID 42022, 2018.

[25] Was, "Making vehicles special," https://www.was-vehicles.com/en/home.html.

[26] H. Habibzadeh, K. Dinesh, O. R. Shishvan, A. B. Dandry, G. Sharma, and T. Soyata, "A survey of healthcare internet-of-things (hiot): a clinical perspective," *IEEE Internet of Things Journal*, vol. 7, 2019.

[27] M. Ghanavatinejad, M. Tavakoli, and M. M. Sepehri, "A clustering model for gadgets and apps in patient monitoring in HIOT environment in health field," *Journal of Hospital*, vol. 18, no. 1, pp. 21–30, 2019.

[28] Apple Inc, "The No.1 smartwatch in the world. Times two," 2021, https://www.apple.com/lae/watch/.

[29] Fitbit Inc, "At fitbit, health & fitness come first," 2021, https://www.fitbit.com/global/eu/home.

[30] Apple Inc, "Apple and google partner on covid-19 contact tracing technology," 2020, https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

[31] Google Inc, "Exposure notifications: using technology to help public health authorities fight covid-19," 2020, https://www.google.com/covid19/exposurenotifications/.

[32] AS inc, "Singapore to make arriving passengers wear monitoring wristbands," 2020, https://en.as.com/en/2020/08/06/latest_news/1596723358_452783.html/.

[33] Econsultancy, "10 Examples of the internet of things in healthcare," 2019, https://econsultancy.com/internet-of-things-healthcare/.

[34] H. H. Nguyen, F. Mirza, M. A. Naeem, and M. Nguyen, "A review on iot healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback," in *Proceedings of the 2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 257–262, IEEE, Wellington, New Zealand, 2017.

[35] I. U. Din, A. Ahmad, M. Guizani, and M. Zuair, "A decade of internet of things: analysis in the light of healthcare applications," *IEEE Access*, vol. 7, Article ID 89967, 2019.

[36] M. N. Mohammed, H. Syamsudin, S. Al-Zubaidi, R. A. K. S. Ramli, and E. Yusuf, "Novel COVID-19 detection and diagnosis system using IOT based smart helmet," *International Journal of Psychosocial Rehabilitation*, vol. 24, no. 7, 2020.

[37] A. Gupta, R. Christie, and P. R. Manjula, "Scalability in internet of things: features, techniques and research challenges," *International Journal of Computational Intelligence Research*, vol. 13, no. 7, pp. 1617–1627, 2017.

[38] F. Richter, "Infographic: smart home technology poised for blockbuster growth," 2018, https://www.statista.com/chart/15736/smart-home-market-forecast/.

[39] G. S. M. Associations, "Iot connections forecast: the impact of covid-19," 2020, https://www.gsma.com/iot/resources/iot-connections-forecast-the-impact-of-covid-19/.

[40] B. Ryan, "The internet is under huge strain because of the coronavirus. experts say it can cope — for now," 2020, https://www.cnbc.com/2020/03/27/coronavirus-can-the-internet-handle-unprecedented-surge-in-traffic.html/.

[41] Eseys .inc., "Internet of healthcare things (ioht) trends," 2020, https://www.eseye.com/internet-of-healthcare-things-ioht-trends/.

[42] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[43] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-based big data storage systems in cloud computing: perspectives and challenges," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 75–87, 2016.

[44] A. S. Adila, A. Husam, and G. . Husi, "Towards the self-powered internet of things (iot) by energy harvesting: trends and technologies for green iot," in *Proceedings of the 2018 2nd International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS)*, 2018.

[45] M. N. Aman, M. H. Basheer, and B. Sikdar, "Data provenance for iot with light weight authentication and privacy preservation," *IEEE Internet of Things Journal*, vol. 6, no. 6, Article ID 10441, 2019.

[46] M. N. Aman, M. H. Basheer, and B. Sikdar, "A lightweight protocol for secure data provenance in the internet of things using wireless fingerprints," *IEEE Systems Journal*, vol. 15, 2020.

[47] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[48] D. Leslie, "Tackling COVID-19 through responsible AI innovation: five steps in the right direction," *Harvard Data Science Review*, 2020.

[49] M. Cudak, A. Ghosh, T. Kovarik et al., "Moving towards mmwave-based beyond-4G (B-4G) technology," in *Proceedings of the 2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, 2013.

[50] T. Berry, "How to Do a SWOT Analysis for Better Strategic Planning," 2021, https://articles.bplans.com/how-to-perform-swot-analysis/.

[51] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: technologies, challenges, and opportunities," *IEEE Access*, vol. 5, Article ID 26521, 2017.

[52] M. S. Rahman, N. C. Peeri, N. Shrestha, R. Zaki, U. Haque, and S. H. A. Hamid, "Defending against the novel coronavirus (covid-19) outbreak: how can the internet of things (iot) help to save the world?" *Health Policy and Technology*, vol. 9, 2020.

[53] L. D. Xu, W. He and S. Li, Internet of things in industries: a survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[54] T. S. Rappaport, S. Sun, R. Mayzus et al., "Millimeter wave mobile communications for 5G cellular: it will work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.

[55] S. Sonune, D. Kalbande, A. Yeole, and S. Oak, "Issues in IoT healthcare platforms: a critical study and review," in *Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2)*, 2017.

[56] T. S. Rappaport, "Wireless communications–principles and practice, (the book end)," *Microwave Journal*, vol. 45, no. 12, pp. 128-129, 2002.

[57] D. Tarek, A. Benslimane, M. Darwish, and A. M. Kotb, "A New Strategy for Packets Scheduling in Cognitive Radio Internet of Things," vol. 178, Computer Networks, Article ID 107292, 2020.

[58] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580–589, 2019.

[59] Z. Dong, R. Espejo, Y. Wan, and W. Zhuang, "Detecting and locating man-in-the-middle attacks in fixed wireless networks," *Journal of Computing and Information Technology*, vol. 23, no. 4, pp. 283–293, 2015.

[60] S. T. Ali, V. Sivaraman, D. Ostry, G. Tsudik, and S. Jha, "Securing first-hop data provenance for bodyworn devices using wireless link fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2193–2204, 2014.

[61] V. Ribeiro, R. Holanda, A. Ramos, and J. J. P. C. Rodrigues, "Enhancing key management in lorawan with permissioned blockchain," *Sensors*, vol. 20, no. 11, 2020.

[62] A. Celesti, A. Ruggeri, M. Fazio, A. Galletta, M. Villari, and A. Romano, "Blockchain-based healthcare workflow for telemedical laboratory in federated hospital IoT clouds," *Sensors*, vol. 20, no. 9, p. 2590, 2020.

[63] A. Ahmed, Q. Nasir, and M. A. Talib, "Blockchain for government services—use cases, security benefits and challenges," in *Proceedings of the Fifteenth Learning and Technology Conference (L&T)*, p. 112, 2018.

[64] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proceedings of the Nineteenth International Conference on Advanced Communication Technology (ICACT),*, pp. 464–467, IEEE, PyeongChang, Republic of Korea, 2017.

[65] T. Lv, Y. Ma, J. Zeng, and P. T. Mathiopoulos, "Millimeter-wave NOMA transmission in cellular M2M communications for internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1989–2000, 2018.

[66] T. Yilmaz and B. A. Ozgur, "On the use of the millimeter wave and low terahertz bands for internet of things," in *Proceedings of the 2015 IEEE second World Forum on Internet of Things (WF-IoT)*, pp. 177–180, IEEE, Milan, Italy, 2015.

[67] E. Ezhilarasan and M. Dinakaran, "A review on mobile technologies: 3g, 4g and 5g," in *Proceedings of the Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)*, pp. 369–373, IEEE, Tindivanam, India, 2017.

[68] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From iot to 5g i-iot: the next generation iot-based intelligent algorithms and 5g technologies," *IEEE Communications Magazine*, vol. 56, no. 10, 2018.

[69] A. Shakeel, R. Hussain, A. Iqbal, I. L. Khan, Q. u. Hasan, and S. A. Malik, "Analysis of efficient spectrum handoff in a multi-class hybrid spectrum access cognitive radio network using Markov modelling," *Sensors*, vol. 19, no. 19, p. 4120, 2019.

[70] J. A. Ansere, M. Kamal, E. Gyamfi, F. Sam, M. Tariq, and A. Mohammed, "Energy efficient resource optimization in cooperative Internet of Things networks," *Internet of Things*, vol. 12, Article ID 100302, 2020.

[71] S. Mir, I. Bari, M. Kamal, and H. Ali, "Constraint waveform design for spectrum sharing under coexistence of radar and communication systems," *IEEE Access*, vol. 9, Article ID 46093, 2021.

[72] M. Kamal, A. Aljohani, and E. Alanazi, "IoT meets covid-19: status, challenges, and opportunities," 2020, https://arxiv.org/abs/2007.12268.