COVID-19: Opportunities and challenges in 5G-enabled Internet of Things

Kamal Daw Ghanem[1] and Nofal Javed[2]

[1]M.Sc Student Electrical and Electronics Engineering,Atilim University,Ankara,Turkey
[2]M.Sc Student Electrical and Electronics Engineering,Atilim University,Ankara,Turkey

Abstract– The Internet of Things (IoT) network is witnessing tremendous growth in the number of wireless technologies and smart sensors. In future, it is expected that trillions of devices will have ubiquitous connectivity. The existing communication technologies such as 3G and 4G will not be able to efficiently manage the massive volume of traffic generated from the IoT networks with achieving scalability and energy-efficiency. To address the challenges, we first research the advancements done in IoT architecture recently. Then we survey the applications and challenges associated with enabling connectivity of trillion devices with existing communication architecture. The survey explores the techniques that can be beneficial in detecting the symptoms of recent virus COVID using the IoT network. The challenges associated with enabling the 5G communication technologies in IoT will also be explored. Finally, we outline and enumerate future research open challenges.

***Index Terms*—Internet of Things, Pandemic, Block chain, Machine learning, Deep learning**

I. Introduction

Internet of Things (IoT) is a next-generation communication architecture in which billions of objects will have the ability to communicate with each other intelligently and adaptively [1], [2]. The IoT-enabled networks can be integrated into a variety of applications such as smart industries, smart health-care, smart agriculture and smart grids [3]. The IoT network will enable connectivity of billions of devices using communication technologies such as WiFi, ZigBee, 3G and 4G, and as a result, a massive amount of real-time traffic will be generated from the IoT networks. The IoT networks consist of a heterogeneous network with having stringent quality of service (QoS) requirements [4].

The traditional Internet and wireless communication technologies such as 3G and 4G cannot manage the large volume of real-time traffic generated from IoT networks [5]. The IoT architecture, as shown in Figure 1, can be divided into three layers. The sensing layer is responsible for collecting useful information from the physically connected IoT network. The network can be a smart health-care network where IoT sensor implanted on the human body can generate traffic related to body parameters, or smart city where IoT devices installed in the building will generate the traffic related to temperature, machines etc. The delivery network is responsible for forwarding the traffic generated from different IoT networks to Internet using a gateway. The existing literature [6], [7] has focused on sensing and delivery layers in the IoT architectures. The function of analytical layer is to perform data-analytic using an optimization technique or machine learning approach. The IoT networks are based on generating large data-sets and its not possible to analyze the traffic using traditional techniques. Thus, analytic layer will analyze the IoT traffic using machine learning approach to perform actions adaptively.

The advancement in the IoT systems such as artificial intelligence and data-analytic with ubiquitous connectivity of devices can be very useful in the smart health-care industry. The IoT devices can be implanted in the human body for measuring the health-related parameters such as heartbeat, sugar level, cholesterol level etc. In [8] the researchers proposed an IoT-based smart health-care system for managing the traffic related to the human body parameters. The software-defined networking approach is used for managing the IoT-based traffic for forwarding the traffic to the destination. Thus, IoT can be an effective solution for monitoring the health-based traffic and provides an early symptom for prevention of infectious diseases such as COVID 19. One of the most important issue for stopping the disease such as COVID 19 is to trace, identify and monitor the infected people so it cannot infect more people. The IoT network can be very effective in tracing and identifying infected people. The IoT sensor can be implanted in the body of infected people, and the movement of the people can be tracked [9]. One of the issues in tracking the infected people will to securely store the personal data of the victims. Block-chain is a recent mechanism that can secure the data of patients in a series of chains.

The traditional communication architectures such as 3G and 46 cannot manage the massive flux of traffic generated from IoT networks with having QoS requirements and data-analytic layer. Thus, the proposed paper surveys the recent challenges applications for IoT networks in terms of 5G networks. Moreover, the recent pandemic COVID 19 is explored in detail with respect to IoT, how can IoT networks used for identifying the symptoms and restrict the infected people for further increase of the disease.

The key contribution of the paper is as follow.

Contributions

- We survey the existing 3G and 4G communication technologies in IoT networks and what challenges the networks can face in terms of traffic management with the

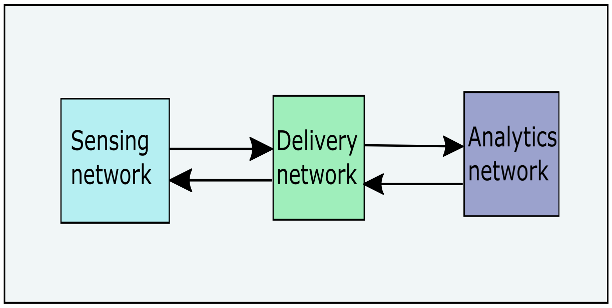

Fig. 1. IoT layers

data-analytic layer.

- How can 5G network effective for IoT networks in efficiently managing the IoT traffic
- Finally, the recent COVID virus is affecting the human beings and how can IoT networks securely help in identifying the symptoms related to the IoT networks.

II. MOTIVATION

The IoT has gained much attention from the IT community and industry with the rapid adaptation of modern smart networks in the area of communication and networking aspects. The performance of the IoT network is dependent on communication and networking technologies as IoT systems may have diverse network requirements such as high reliability, security, availability, high speed and QoS requirement. However, the existing communication networks such as 3G and 4G cannot provide services and smooth connectivity for the massive amount of traffic generated from IoT devices. Nowadays, pandemic COVID 19 is a serious threat to for human beings. The survey will also explore the research areas in IoT that can be beneficial for reducing the effect of corona with making the personal traffic of the patients secure. Thus, we are motivated to search how IoT devices implanted in the human body can detect the symptoms of corona in advance using machine learning algorithms. Moreover, what are the challenges involved in shifting from 4G to 5G communications?

III. LITERATURE REVIEW

The IoT is physically connected networks that aim to function without intervention of human being in an adaptive manner [10]. The IoT architecture consists of three layers, as shown in Figure 2 that can be discussed below.

1) Sensor layer:: The first layer is the physically connected devices that are used for collecting the traffic from the networks. The first layer shows that the smart device can be implanted on a human body to measure the traffic related to the human being, or agriculture-related traffic or smart city where the IoT devices can be used to measure the traffic related to temperature, heat and other important parameters of the community [11].

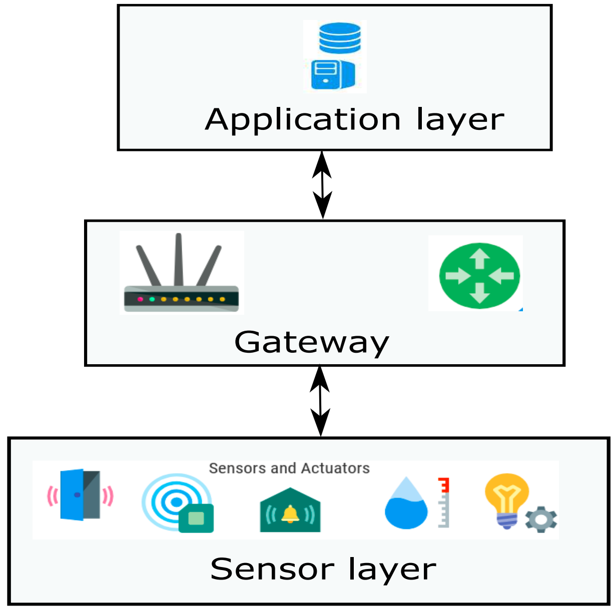

Fig. 2. IoT network architecture

2) Gateway:: The second most important component of the IoT architecture is the gateway that is used to link the IoT networks with the Internet using communication technologies such as 3G, 4G, WiFi and ZigBee. The IoT networks are becoming complex and generating a massive amount of data from different networks, and the traditional communication protocols such as 3G and 4G networks cannot manage the resources of the network. Thus, gateway is an important component of the IoT network.

3) Application layer:: The application layer is responsible for managing the traffic generated from the IoT networks. The health-care application can have a team of professional doctors, where the data related to health is monitored. Moreover, smart grid, agriculture and the smart city can be other important applications.

In [12] an IoT-based network is used for detecting the symptoms related to COVID-19. The researchers proposed a drone-based architecture that is installed with sensors for recording the symptoms such as high temperature. If any person is detected with high fever, the drone forwards its location, image to the management team for taking further actions for reducing the spreading of the virus. In [9], a three linkage IoT-based architecture has been proposed for detecting the symptoms of COVID-19 disease. One of the key issues identified is that existing communication technologies such as 3G and 4G cannot manage the resources of the network efficiently. They used the 5G communication architecture for performing the functionalities of data-analytic. The paper verifies that 5G communication architecture can be very effective for performing data analysis. The 5G architecture has significantly better abilities compared to the existing communication architectures [13]. The peak uplink rate of 5G can exceed 10 Gbps, and the peak downlink rate can achieve 20 Gbps. Furthermore,

International Journal of Scientific & Engineering Research Volume 11, Issue 6, June-2020
ISSN 2229-5518

Fig. 3. Three linkage IoT based architecture for COVID-19

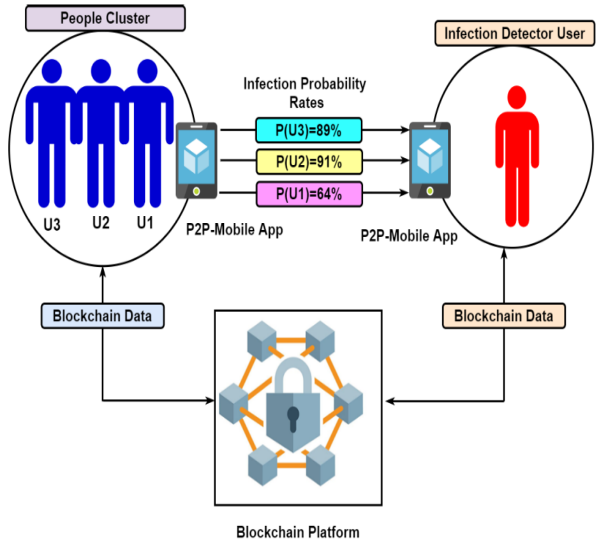

Fig. 4. Block-chain architecture for COVID-19 [16]

the 5G will significantly reduce the latency and improve the overall performance of the network. Therefore, 5G can provide new opportunities in the area of health-care, specifically for COVID-19. In [14] the authors proposed a video surveillance system for controlling the current pandemic. They argued that already modern infrastructure is installed such as internet access, smartphones, and wearable technologies, the role of technology can be used for data analysis and collection of the data related to the COVID-19. The concluded with future work to explore the automated alert systems for time detecting of diseases such as corona.

In [15], researchers have explored that with the advent of smart devices integrated with machine learning approach can solve the problem of identifying the patients of COVID-19. The framework is known as mobile health; however, one of the key challenges will be to explore the capabilities of edge and cloud computing for improving the performance of the network.

One of the current challenges in the current pandemic is to build an architecture that can detect and verify the unknown case of C0VID-19. In [16] the authors explored the blockchain technology that can use the time stamping, decentralized storage and peer-to-peer advantages for verifying the unknown cases of the COVID-19 virus. The blockchain architecture proposed by architecture can be seen in Figure 3 that uses a Peer-to-Peer communication architecture for detecting the sources of infection within a cluster of people. The P2P application will forward the message within a cluster automatically to show the infected person within a cluster. In [17] the authors survey the recent advancement related to Industry 4.0 in COVID-19. The paper concluded that Industry 4.0 can satisfy the requirements of the health-care systems specially in terms of COVID-19 for proper treating of the patients. Thus, there is a research gap in the area of Industry 4.0 for designing an architecture that can detect the early symptom's of the patients. In [18], the researchers proposed a smart monitoring system that integrates the blockchain and IoT technology for monitoring the patients of the COVID-19. The architecture is based on IoT as shown in Figure 5 that collects the physical and location of the isolated people and forward it to a master device. The smart device is responsible for formatting the data and transferring it to smart contract. The algorithm is implemented in the smart chain where a threshold is define that compares with the patients analyzed data. If patients data exceed the threshold, a notification is forwarded to the smart contract which notifies the isolated patients, and the event is stored in a blockchain.

IV. IoT Applications

The IoT has applications in the following domain.

1) Smart Home: The smart home is a kind of IoT network where devices are installed in the home and connected to the Internet that performs decisions autonomously based on data generated from the sensors, therefore, improving the lifestyle of users for easily controlling the home appliances. The devices in the smart home communicate regularly with the environments. The IoT devices will generate a massive volume of traffic, and traditional communication architectures need to be upgraded. Moreover, the machine learning algorithms need to be further explored to improve the performance of the devices in the smart home.

2) Intelligent transportation systems: The intelligent transportation system (ITS) is used to monitor the transportation network efficiently [19]. The ITS is based on the following network components such as RFID, vehicle subsystem, onboard unit (OBU), roadside unit (RSU) to ensure system efficiency, availability, reliably of transportation systems. The

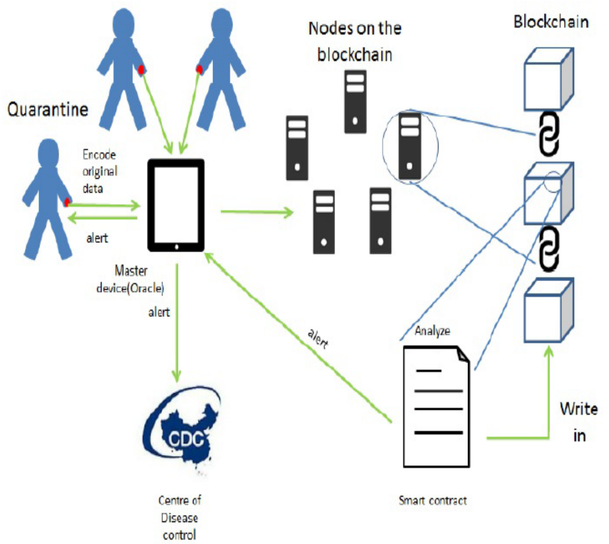

Fig. 5. Smart monitoring system for COVID-19 [18]

vehicles in the IoT are generating a massive volume of traffic with traffic such as video streaming, audio and VoLTE, thus existing communication architectures such as 3G and 4G cannot manage the stringent QoS requirement of the users. Hence, research is needed to explore the advantages of using 5G in communication.

3) Smart city:: The smart city aims to improve the lifestyle of the residents through gathering and to control the IoT based information from their devices. The IoT enabled applications such as health, homes, transportation etc. fall under the category of smart city [20]. The traffic of the smart city performs data analytic using the machine learning algorithms and upgraded communication architectures are needed to performing the data-analytic functionality without delay.

4) Smart Healthcare:: The smart health-care is playing an important role in improving the lifestyle of patients and humans. The IoT devices are implanted in the patients and human body that gathers the traffic related to the human body. The smart health-care traffic can be divided into periodic physiological and emergency traffic [8]. The emergency traffic can be heart attack, ECG, higher sugar and glucose level, and this type of traffic is delay-sensitive and needs to be forwarded on the paths that have less delay. Similarly, periodic physiological traffic is normal traffic such as sugar and glucose level of patients every hour. The smart health-care traffic needs to satisfy the stringent QoS requirement of the traffic. Hence, a research gap exists in exploring the next generation communication architectures such as 5G for providing services to the IoT based health-care systems.

V. Challenges in IoT

The following are the challenges associated with IoT with using the 5G technology.

A. *Scalability*

The next-generation networks will be based on applications like smart grid, smart cities, smart health-care. Each application will have heterogeneous networks with having different service requirements [21]. The 5G has to efficiently allocate the resources of the IoT network. One of the major issue with IoT networks will be a scalability issue. Secondly, how to interconnect different IoT heterogeneous networks with the existing 5G networks is a significant challenge. Thus, there exists a research gap in exploring the area of scalability with heterogeneous networks.

B. *Interoperability*

A large number of connected IoT devices proposes a challenge in providing seamless end-to-end interoperability between heterogeneous networks [24]. The different IoT networks will be connected using different communication technologies such as ZigBee, WiFi, 3G, 4G and 5G. Thus, one of the major issue in deployment of the 5G technology will be to provide seamless interoperability between different IoT networks. A significant challenge that needs to be addressed when considering MTC for the IoT - which aims at achieving connectivity between anything, everything, anywhere, and at any-time - is the seamless end-to-end interoperability among the non-homogenous and entirely different network technologies which have been presented in the earlier sections and between the heterogeneous IoT devices. This will enable the connectivity of a wide range of devices across the various communication networks and perhaps the realization of the IoT concept, which enables heterogeneous devices to be connected through a communication technology to connect, communicate, share, and collect essential data or information with other related smart devices or applications [25]. To achieve this level of interconnections, elusive interoperability must be deployed across all devices among all network technologies considering their make, model, network provider, as well as the manufacturers of their network infrastructure. This means that in order to achieve massive IoT deployment, sooner or later, we ought to enable these devices to be able to get connected with other devices or nodes regardless of the hardware infrastructure they are using and their application programming interface (API). In the modern world today, we have fragmented systems that fail to guarantee interoperability between heterogeneous devices. For massive IoT applications to be achieved, standardization and interoperability between the various communications technologies are of great importance in meeting consumers' requirements that need to be redressed.

However, the availability of various protocols and standards under implementation by diverse institutions in the current world, to resolve the cutthroat nature of the IoT presents us with significant and unprecedented setbacks for interoperability [23]. Lastly, the heterogeneous nature of the IoT networks and devices has also been counted as other major issues that make interoperability between different devices more challenging and complex. With the emergence of new

TABLE I
SUMMARY OF EXISTING LITERATURE

Reference	Pros	Cons
[12]	Drone used for detecting symptoms of COVID-19 patients	Privacy is not considered
[9]	IoT-based three layer architecture of detecting symptoms	The communication architecture is not defined
[13]	The 5G communication can be effective for data-analytic	The architecture is not explored
[15]	Machine learning approach for detecting symptoms of COVID-19 patients	Unsupervised algorithms are not explored.
[16]	Block chain enabled technology for COVID-19	Machine learning approach is not explored using block chain
[21]	Smart-healthcare system using IoT network is explored	The Quality of service is not explored
[8]	SDN-enabled healthcare system	The architecture is not scalable.
[22]	Security attacks explored in IoT	Data-analytic area is not explored.
[23]	Heterogeneous nature of IoT network explored	New communication architectures are required.
[18]	Security of COVID-19 explored	The machine learning algorithms are not explored in detail.
[21]	Scalability of IoT network explored	New communication architectures are required.

communication technologies which introduce many integration challenges including common practices, service descriptions, standards and discovery mechanisms which need to be adequately addressed to ensure that an enabling interoperable environment is established between the IoT heterogeneous networks.

C. Security

The massive number of connected IoT devices with heterogeneous networks poses new threat and security challenges. The threats can be hacking in the smart meters, malicious code attacks, sniffing, and Denial of Service (DoS) attacks [22]. The implementation of the 5G technology needs to upgrade security algorithms such as implementing machine learning algorithms that can secure the current IoT networks. The blockchain techniques should be incorporated into the networks to make the IoT networks further secure. The paradigm shift wireless communication technologies and M2M communications have observed a substantial increase in the number of devices connected to communication networks in the IoT, leading to increased security threats, which help born new security issues. The security attack can be in the form of hacking in smart meters, sniffing attacks, and denial of service (DoS). Thus, the integration of IoT networks with heterogeneous networks such as smart grid, smart health-care, smart agriculture may expose to a security threat. There is a research area to make the IoT networks more secure.

1) Network mobility: Coverage, mobility of the networks, and reachability are some of the wide-open research fields under the umbrella of the IoT that need timely redressal for compelling deploying of Critical and large IoT use cases as metrics for measuring performance since a maximum of the IoT service applications are destined to be rolled out to the mobile users. This is an essential characteristic of the IoT to ensure that users ought to be connected anywhere. Apart from that, It also aims to provide users with their required services while users are still on the go. Smart devices connected on a wireless media might essentially observe disruption in services as a possibility of the device in movement (moving away from one specific server towards another one). It is the need of the hour to enact a mechanism which will govern this mobile nature of nodes, which will also ensure to supervise and administer the unprecedented increase of smart devices in the IoT networks. In [26], a very scalable approach was proposed which nominates a ”leader” who in turn is responsible for taking care of the group mobility keeping in view some kind of unique analysis metrics, which is directly impacted by the pattern of mobility followed to connected nodes. Considering the massive number of IoT devices, effective and efficient installation of more bases stations will be needed in order to cope up with connectivity needs of all the kind of networks. Moreover, one must also take into account the fresh services of the nascent enacted 5G networks for the IoT when scrutinizing the complications of devices in motion in the IoT architecture.

2) Network congestion: Network congestion and the associated overload is another critical plus unavoidable confrontation that requires to be reduced to optimum levels in the growth of the IoT because of the fact that smart devices connected with each other offer a critical role in making up the signalling load in case of the mobile network when putting in contrast with the legacy human-to-human transmission of traffic in cellular networks. This congestion in network degenerates the performance and quality of service (QoS) in IoT. Another demanding issue which is highly pertinent with MTC in this scenario is the capability to harbour the enormous traffic that will be produced as a result of the gigantic volume of different MTC devices that will bring into play congestion in the networks. Thus, it becomes obligatory for the Internet Protocols (IP) to propose a very efficient solution for dealing with congestions in the network. It is also an undeniable fact that in today's era, there are some network systems which, despite greater connectivity of devices, still have the provision of most stable internet connectivity by the exploitation of IP with Transmission Control Protocol in the transport layer of OSI model. But we must also understand that the present day TCP cannot be utilized with the nascent IoT mainly due the IoT traffic architecture. This architecture differentiates entirely from the legacy networks already in place today.

3) Standard regulation body: The use of blockchain and AI in the health-care sector, like coronavirus fighting, should be taken into factor carefully with the given regulatory laws. While the features of blockchain and AI can deliver benefits, they also put at risk the legal and regulatory challenge if no party is responsible and can be held accountable for. For instance, in the blockchain network, it will be very essential to recognize what law might apply to transactions and what appropriate risk management should be put into place [117]. Regarding AI, it might be straightforward to create some kind of legal arrangement and internal governance designs that will enact the governing law for AI operations in health-care [27]. Specially, we also envisage legal issues about the created content, personal information running on blockchain and AI platforms, such as issues with copyright infringement and personal defamation.

4) Privacy for Corona patient: In the corona-virus tracking applications, how to protect people's privacy is imminently pertinent. The governments can make use of mobile location data to help record the outbreak escalation. Still, these solutions must warrant the confidentiality of user-produced data, especially sensitive information, such as a residential address, banking credentials, shopping trends, etc. The governmental agencies may impose privacy legislation on user tracking mobile apps to confirm the safety and security of the public. Besides, nowadays, many health-care organizations and institutions are gathering data from their patients via electronic health-care records that help monitor the COVID- 19 disease symptoms and serve remedy and prescribe cure [18]. In such health-care activities, the conflict engagement between data collection and user privacy is unavoidable that demand solution by-laws and reinforcement from the concerned authorities.

5) Optimized block chain architecture: Blockchain platforms should be optimized to attain best performances in terms of short network latency, expanded throughput, and improved security, which can prepare blockchain to become an excellent choice for emergency health-care applications like the COVID-19 pandemic. For instance, lightweight blockchain design in health-care is mandatory to optimize data verification and transaction communication for ultra-low latency information broadcasting [28]. Another expedient solution is to reduce the size of blockchain by chartering local and private blockchain networks; one of these is responsible for monitoring the plague in a particular area for a quick response. To envision this, building customized ledgers that can be implanted on local servers in the outbreak area can help to augment the blockchain performance.

6) Integration with other technologies: To achieve a state of the art efficient techniques in solving epidemic-related issues, blockchain and AI can be incorporated with alternative technologies to frame a comprehensive health-care system. For instance, recently, Taiwan leveraged big data as a promising technology combined with AI to curb the virus spread. Alibaba has also integrated AI with cloud computing for supporting coronavirus data analytics. The ingenious storage and high computation capability are the key features that the cloud can administer to promote AI analytics. More interestingly, China has exploited, just a while ago, the mobility of drones [132] to enhance the provisions of medical supplies [133]. Using drones would be the fastest way to deliver rudimentary facilities to the infected people living in the quarantine areas where all modes of transport are disrupted. Besides, drones also help to sustain the contactless monitoring of the outbreak. In the days to come, these promising technologies can be combined to build a highly advanced medical system for encountering the coronavirus-like epidemics.

7) Conclusion and Future directions: This paper was intended to review the modern solutions currently in place for IoT, keeping in view large and variable perspectives. The IoT paradigm guarantees to provide a contributive networking environment through non-homogenous gadgets connected to each other. These devices comprise of joint systems of sensors and actuators embedded within, which are interconnected together to communicate within each other's sphere through a communication media which is mostly wirelessly operated. The real-world applications envisaged by IoT and the related requirements to ultimately conceptualize the notion of IoT was also put forward. From the analysis presented herewith, It has been made crystal clear that we cannot go for a single-fit-for-all solution that can be utilized since separate applicative and operating areas would require separate service provision. The difficulties encountered by the IoT vision were recommended to be taken into consideration for forthcoming deliberations, keeping the fact on board that we cannot use a single-fit solution in the rollout of the IoT use cases. Some of these identified impediments include but not limited to; scalability, network management, devices interoperability, and heterogeneous nature, security and privacy, mobility in networks, and their coverage. Similarly, the congestions caused by all these devices and their overheads cannot be ruled out at all. Interoperability among various device makes, and their heterogeneity is also a crucial impediment that needs to be taken on board due to the non-homogenous-nature of IoT and entirely different communication models that are made embedded for a unique standardization. Apart from that, congestion caused in the network also is an essential component because, with the presence of massively connected objects, the gigantic traffic that is going to be produced would inevitably contribute in bottleneck inside the network. And it will definitely lead to a highest-ever packet loss rate. Therefore, we are of the opinion that this calls us to devise an efficient system to uphold highest degrees of (QoS) as a lightweight context-aware congestion control (CACC) structure to administer and dominate the bottleneck problem and bit error rate in the IoT networks.

In this paper, we also intended to present a state-of-art survey on the utilization of blockchain and AI technologies to encounter the coronavirus (COVID-19) epidemic. We have first introduced a conceptual and visionary architecture that integrates blockchain and AI towards combating the coronavirus crisis. Specially, we have extensively discussed the critical roles of blockchain for solving the pandemic via five great solutions, including outbreak tracking, user privacy protection, safe day-to-day operations, medical supply chain, and donation tracking. By the same token, the potential of AI for dealing with the COVID-19 crisis has also been analyzed through five main application domains, namely outbreak estimation, coronavirus detection, coronavirus analytics, vaccine/drug development, and prediction of the future coronavirus-like outbreak. Some pertinent use cases and projects using blockchain and AI towards COVID-19 fighting have also been underpinned. Finally, we have identified some potential challenges and future directions. We believe our timely survey will shed valuable light on the research of the blockchain and AI for COVID-19 fighting as well as motivate the interested researchers and stakeholders to put more effort into using these promising technologies to combat the future coronavirus-like epidemics.

REFERENCES

[1] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–29, 2019.

[2] S. Maitra and K. Yelamarthi, "Rapidly deployable iot architecture with data security: Implementation and experimental evaluation," *Sensors*, vol. 19, no. 11, p. 2484, 2019.

[3] M. Agiwal, N. Saxena, and A. Roy, "Towards connected living: 5g enabled internet of things (iot)," *IETE Technical Review*, vol. 36, no. 2, pp. 190–202, 2019.

[4] L. Zhao, J. Wang, J. Liu, and N. Kato, "Optimal edge resource allocation in iot-based smart cities," *IEEE Network*, vol. 33, no. 2, pp. 30–35, 2019.

[5] H.-N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, "Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies," *Enterprise Information Systems*, pp. 1–25, 2019.

[6] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges," *IEEE wireless communications*, vol. 24, no. 3, pp. 10–16, 2017.

[7] H. Washizaki, N. Yoshioka, A. Hazeyama, T. Kato, H. Kaiya, S. Ogata, T. Okubo, and E. B. Fernandez, "Landscape of iot patterns," in *2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT)*. IEEE, 2019, pp. 57–60.

[8] F. Sallabi, F. Naeem, M. Awad, and K. Shuaib, "Managing iot-based smart healthcare systems traffic with software defined networks," in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2018, pp. 1–6.

[9] L. Bai, D. Yang, X. Wang, L. Tong, X. Zhu, C. Bai, and C. A. Powell, "Chinese experts' consensus on the internet of things-aided diagnosis and treatment of coronavirus disease 2019," *Clinical eHealth*, 2020.

[10] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, and Y. Wang, "A survey of internet of things communication using icn: A use case perspective," *Computer Communications*, 2019.

[11] S. A. Fatima, N. Hussain, A. Balouch, I. Rustam, M. Saleem, and M. Asif, "Iot enabled smart monitoring of coronavirus empowered with fuzzy inference system," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 6, no. 1, 2020.

[12] M. Mohammed, N. A. Hazairin, S. Al-Zubaidi, S. AK, S. Mustapha, and E. Yusuf, "Toward a novel design for coronavirus detection and diagnosis system using iot based drone technology," *International Journal of Psychosocial Rehabilitation*, vol. 24, no. 7, 2020.

[13] D. Li, "5g and intelligence medicine—how the next generation of wireless technology will reconstruct healthcare?" *Precision Clinical Medicine*, vol. 2, no. 4, pp. 205–208, 2019.

[14] M. S. Rahman, N. C. Peeri, N. Shrestha, R. Zaki, U. Haque, and S. H. Ab 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*, 2020.

[15] Q.-V. Pham, D. C. Nguyen, W.-J. Hwang, P. N. Pathirana *et al.*, "Artificial intelligence (ai) and big data for coronavirus (covid-19) pandemic: A survey on the state-of-the-arts," 2020.

[16] M. Torky and A. E. Hassanien, "Covid-19 blockchain framework: Innovative approach," *arXiv preprint arXiv:2004.06081*, 2020.

[17] M. Javaid, A. Haleem, R. Vaishya, S. Bahl, R. Suman, and A. Vaish, "Industry 4.0 technologies and their applications in fighting covid-19 pandemic," *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, 2020.

[18] C. Xiao, L. Zheng, F. Chen, and Y. Xiao, "Design and research of a smart monitoring system for 2019-ncov infection-contact isolated people based on blockchain and internet of things technology," 2020.

[19] P. Patel, Z. Narmawala, and A. Thakkar, "A survey on intelligent transportation system using internet of things," in *Emerging Research in Computing, Information, Communication and Applications*. Springer, 2019, pp. 231–240.

[20] I. A. T. Hashem, V. Chang, N. B. Anuar, K. Adewole, I. Yaqoob, A. Gani, E. Ahmed, and H. Chiroma, "The role of big data in smart city," *International Journal of Information Management*, vol. 36, no. 5, pp. 748–758, 2016.

[21] J. Jermyn, R. P. Jover, I. Murynets, M. Istomin, and S. Stolfo, "Scalability of machine to machine systems and the internet of things on lte mobile networks," in *2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2015, pp. 1–9.

[22] S. Ziegler, C. Crettaz, E. Kim, A. Skarmeta, J. B. Bernabe, R. Trapero, and S. Bianchi, "Privacy and security threats on the internet of things," in *Internet of Things Security and Data Protection*. Springer, 2019, pp. 9–43.

[23] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in internet of things: Taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, 2019.

[24] M. Elkhodr, S. Shahrestani, and H. Cheung, "The internet of things: new interoperability, management and security challenges," *arXiv preprint arXiv:1604.04824*, 2016.

[25] N.-N. Dao, M. Park, J. Kim, J. Paek, and S. Cho, "Resource-aware relay selection for inter-cell interference avoidance in 5g heterogeneous network for internet of things systems," *Future Generation Computer Systems*, vol. 93, pp. 877–887, 2019.

[26] H.-L. Fu, P. Lin, H. Yue, G.-M. Huang, and C.-P. Lee, "Group mobility management for large-scale machine-to-machine mobile networking," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 3, pp. 1296–1305, 2013.

[27] I. F. Akyildiz, S.-C. Lin, and P. Wang, "Wireless software-defined networks (w-sdns) and network function virtualization (nfv) for 5g cellular systems: An overview and qualitative evaluation," *Computer Networks*, vol. 93, pp. 66–79, 2015.

[28] D. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, "Blockchain and ai-based solutions to combat coronavirus (covid-19)-like epidemics: A survey," 2020.