Cluster Computing (2022) 25:2351–2368
https://doi.org/10.1007/s10586-021-03367-4

SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic

Anichur Rahman[1] · Chinmay Chakraborty[2] · Adnan Anwar[3] · Md. Razaul Karim[4] · Md. Jahidul Islam[5] · Dipanjali Kundu[1] · Ziaur Rahman[4] · Shahab S. Band[6]

Received: 13 May 2021 / Revised: 29 June 2021 / Accepted: 18 July 2021 / Published online: 29 July 2021

Abstract

The industrial ecosystem has been unprecedentedly affected by the COVID-19 pandemic because of its immense contact restrictions. Therefore, the manufacturing and socio-economic operations that require human involvement have significantly intervened since the beginning of the outbreak. As experienced, the social-distancing lesson in the potential new-normal world seems to force stakeholders to encourage the deployment of contactless Industry 4.0 architecture. Thus, human-less or less-human operations to keep these IoT-enabled ecosystems running without interruptions have motivated us to design and demonstrate an intelligent automated framework. In this research, we have proposed "EdgeSDN-I4COVID" architecture for intelligent and efficient management during COVID-19 of the smart industry considering the IoT networks. Moreover, the article presents the SDN-enabled layer, such as data, control, and application, to effectively and automatically monitor the IoT data from a remote location. In addition, the proposed convergence between SDN and NFV provides an efficient control mechanism for managing the IoT sensor data. Besides, it offers robust data integration on the surface and the devices required for Industry 4.0 during the COVID-19 pandemic. Finally, the article justified the above contributions through particular performance evaluations upon appropriate simulation setup and environment.

Keywords SDN · IoT · NFV · OpenFlow · Security · Privacy · COVID-19 · Industry 4.0

✉ Chinmay Chakraborty
cchakrabarty@bitmesra.ac.in

Anichur Rahman
anis_cse@niter.edu.bd

Adnan Anwar
adnan.anwar@deakin.edu.au

Md. Razaul Karim
razaulce15004@gmail.com

Md. Jahidul Islam
jahid@cse.green.edu.bd

Dipanjali Kundu
dipanjali_kundu@niter.edu.bd

Ziaur Rahman
zia@iut-dhaka.edu

Shahab S. Band
shamshirbands@yuntech.edu.tw

[1] National Institute of Textile Engineering and Research (NITER), Constituent Institute of the University of Dhaka, Savar, Dhaka, Bangladesh

[2] Electronics and Communication Engineering, Birla Institute of Technology, Mesra, Jharkhand, India

[3] Centre for Cyber Security Resaerch and Innovation (CSRI), Deakin University, Melbourne, VIC 3220, Australia

[4] Mawlana Bhashani Science and Technology University, Tangail, Bangladesh

[5] Green University, Dhaka, Bangladesh

[6] National Yunlin University of Science and Technology, 123 University Road, Section 3, Douliu, Taiwan

1 Introduction

The world is currently struggling against an invisible force that is Corona Virus (COVID-19). Millions of people from all over the world have been affected by the virus within a very short period of time, where the most developed countries such as USA, UK, France, Italy etc suffered most although they have the advanced medical systems [1]. The world itself, as well as governments, scholars, and individuals, are battling with this problematic situation and seeking innovative solutions. COVID-19's present condition has taught us many new things and has created many new behaviors. It has influenced a country's overall structure, including industrial, health, supply chain, and many other sectors, and has brought many changes to everyone's lifestyle. To cope with the current situation, it is imperative to implement various innovations. This pandemic condition enforced us to isolate ourselves from the society, and this also holds true for the manufacturing sectors and industries. Again, the traditional way of production and manufacturing system is not being able to keep pace with the law of social distancing.

In this pandemic, since almost every work is done over the cloud, safety and protection is a significant concern in IoT applications. Figure 1 illustrates the isolation and the lockdown scenario. Many devices are connected for information sharing and in such situation, more extra devices are being connected to meet the daily performance in the workplaces. Since the rate of working from home has been increased dramatically, the cloud portals are having too many service requests to deal with. One critical aspect is that the response time should be minimized, and resources should always be available.

However, here an architecture (EdgeSDN-I4COVID) is proposed to accelerate the productivity of different industries. To work from home for the prevention of COVID-19, Internet of Things (IoT) networks on the application of Industry 4.0 is applied at the bottom layer. For the maintenance and collection of the high volume of data from IoT devices, Software Defined Networking (SDN) is kept with the common SDN–IoT gateway where it is the multi-controller SDN. Network Function Virtualization (NFV) is used to support the extra services and to reduce the complexity of hardware implementation. It can provide service on demand such as storage. Apart from this, every data will be stored on the cloud in a secure database. The authors provided a comparative visualization with the traditional networking systems.

Fig. 1 Working from Home and cloud scenario in COVID-19 situation

To summarize, the contributions of this paper are as follows:

- This article provides a unified platform for a unit to unit communication in an industrial environment to tackle the demerits of COVID-19 pandemic in the industries.
- Authors address the SDN with NFV services, which employ the multiple controllers from the data layer with the control layer to the application layer that proportion the load balancing, partition the networks, and minimize the packet loss properly.
- We also utilize the SDN-based IoT framework for communicating data from bottom to top layer in the smart industry applications securely and efficiently which will ensure the reliability of the system during COVID-19.

Table 1 portrays of the abbreviations and associated notions used throughout this article. The rest of the paper is organized as follows: In Sect. 2, the authors analyze and discuss the background knowledge and literature works. Then, Sect. 3 provides the proposed architecture "EdgeSDN-I4COVID", and also discusses how the proposed architecture works properly. Sect. 4 presents the network design and implementation. Furthermore, results and discussions are presented in Sect. 5. Finally, the authors conclude the research in Sect. 6 and propose the future plan of this work.

2 Motivational background and related works

2.1 Background knowledge

In this segment, the authors cover the intellectual background based on emerging technologies such as IoT, SDN, Industry 4.0 for the COVID-19 outbreak.

The use of robotics, IoT, and other corresponding innovations have increased tremendously with the development Industry 4.0. IoT is a very powerful solution for a wide array of real-time problems, and that is possible through the sensors that are part of the Internet of Things

Table 1 Technical terms and abbreviations

Terms	Description
AI	Artificial Intelligence
AP	Application Plane
BC	Blockchain
CH	Cluster Head
CHS	Cluster Head Selection
CNN	Convolutional Neural Network
COVID-19	2019 Novel Coronavirus
CP	Control Plane
DoS	Denial of Service
DDoS	Distributed Denial of Service
DP	Data Plane
IoMT	Internet of Medical Things
IoT	Internet of Things
IR 4.0	Industrial Revolution 4.0
ML	Machine Learning
NFV	Network Function Virtualization
QoS	Quality of Service
RFID	Radio Frequency Identification
SARS-COV-2	Severe Acute Respiratory Syndrome Coronavirus 2
SC	Smart Contact
SDN	Software Defined Networking
TLS	Transport Layer Security

[2]. IoT, as a vital enabler for Industry 4.0, provides improved management, personalized service and efficient operation with sensor to sensor communication. Moreover, the sensors and the wireless communication system communicate for the overall production line and often take instant decisions where appropriate [3]. Some of the applying areas of this technology are depicted in Fig. 2.

Over the last few years, IoT has many applications in various fields illustrated in Fig. 3 such as Healthcare, Education, Smart Home etc. Applications based on IoT can obtain a cutting-edge development by combining the SDN technology. SDN is used to support network configuration and management with IoT applications that have a central controller [4], dynamically can be controlled, arranged, and configured using an SDN controller network and improves load balance [5]. The main purpose of implementing SDN is to reduce external response time and constant availability. Moreover, these technologies have different types of applications in various fields, such as smart cities, smart grids and buildings, industries, etc. Software defined networks can be easily re-programmable from a single location, and can, therefore, be attacked by a third party. Multiple controller failures occur because of the DoS and DDoS attacks [6]. The main aim of using multiple controllers is to balance the load between devices and controllers which minimizes the loss of the packets [7]. On the other hand, NFV is another recent technology for IT virtualization. This program is responsible for saving energy, increasing the network scalability, and managing loads. The efficient combination of both technologies will enhance security and privacy. Some researchers have proposed numerous solutions to improve network security and also improve performance [8] but couldn't fully solve the problems properly. In this work, authors present an effective "EdgeSDN-I4COVID" architecture to analyze the smart industry capabilities in the pandemic situation

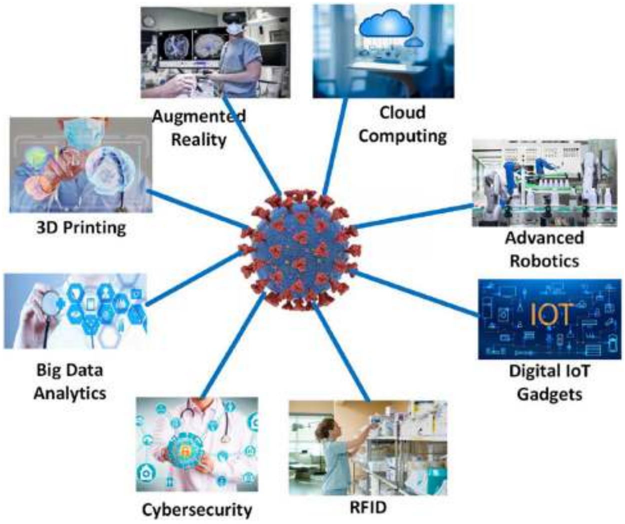


Fig. 2 Applications of industry 4.0 fight against Covid-19

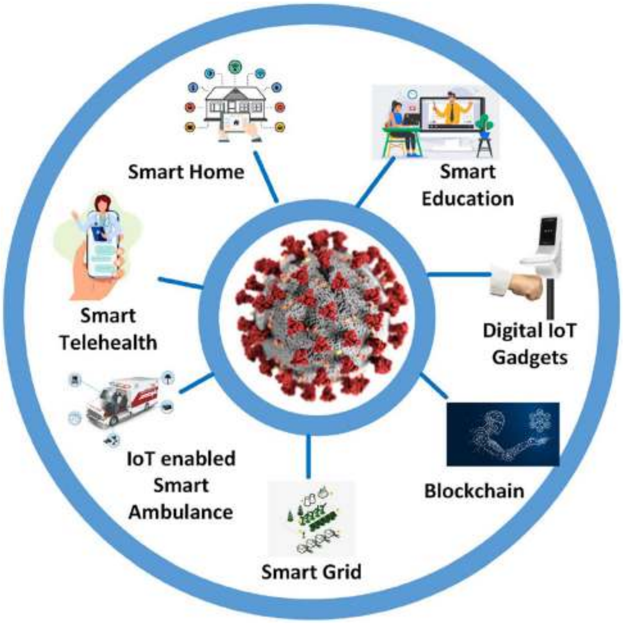


Fig. 3 Applications of IoT to fight against COVID-19

like "HCoV-19". A combination of SDN with NFV and IoT, which greatly enhances the exceptional security and reliability is provided to build smart industrial networks. Additionally, several researchers had previously discussed security issues using both (SDN and IoT) technology [9].

2.2 Related works

Several researchers recently finding way to find the solution of the current collapsed situation due to the contagious disease. In this section, authors are going to present several reviews of recent works in the literature.

Owing to the COVID-19 situations, many enterprises have been shut down and many factories and local stores are about to close down. They face many problems in terms of cost control, the sanitation of their workers, and many more [23–25]. In [26], several approaches have been suggested to tackle the pandemic situation in which IR 4.0 will play a critical role [27]. However, in this work they have suggested a way to handle the overall situation. Still there is lot more work that need to be done to solve the current stage of pandemic condition. In another similar research [28], identified some key issues and studied the IR 4.0 to solve these challenges related to the stores where retailers have great impact. Building trust between the supplier and the customer is a big challenge. In [10], the authors identified the need of revolution 4.0 in order to maintain the masking as well as the disposal of these masks and other related things that are used to fight against the COVID-19 situation. Revolution 4.0 launched many different creative concepts, such as home employment, telemedicine, online education, online certification. However, in order to make use of the advantages of IR 4.0, the overall system needs to be more stable and trustworthy. A significant amount of technologies such as NFV, SDN will help IR 4.0 develop further to gain a stable environment.

The SDN survey in [29] addressed issues of scalability in the SDN approach. At the same time, authors also provided some SDN-based mechanisms such as multimedia routing mechanisms, inter-domain routing, resource reservation, queue management, and scheduling techniques, QoE awareness, network monitoring, and other QoS-centric tools in [30]. In [31, 32], authors discussed the application of SDN in computer networking's security purpose, as the programmability of SDN provides an improvement in network security. Further, the SDN [33] has a distributed controller cluster that resolves reliability, scalability, fault tolerance, and interoperability issues. Besides, the IoT Infrastructure is used to build a reference architecture to ensure end-to-end service over multiple [34] SDN domains. In addition, [35] discussed IoT networking efficiently, based on the SDN approach. In [36], authors presented a concept of SDN that is used to allow centralized control and configuration of network devices.

Another research work proposed in [37] introduces an SDN based architecture for IoT technology with the correction of security. Authors in [9, 38, 39] considered the security of different SDN inventions and suggested the most appropriate security mechanism based on security demands. From 2012 to 2016, the authors refreshed various aimed SDN architecture and security solutions for IoT in [40]. They also analyzed various existing SDN solutions based on IoT and compared them. Also, another secure mechanics, introduced by authors in [8] proposed to handle various assails. The authors proposed SDN for the Middlebox arrangement and flow table capacity constraints. Moreover, authors in [41] presented an excellent combination of the SDN and the IoT environment. They highlighted the relative analysis of both solutions (SDN & IoT) and gave a simple overview of those directions. Furthermore, in [42] the authors have discussed the case studies. The smart factory energy planning includes wireless power transfer from IoT implements in the smart industry. Another study in [43] provides an analytical research on smart factories. Next, authors suggested a framework to investigate the elements and features of smart factory systems. In paper [44], authors proposed a software-defined infrastructure that is deployed in an Industry 4.0 network environment.

In summary, various researchers presented different works in the IoT network based on SDN with NFV. They also implemented numerous applications in the SDN–IoT fields, based on security. Table 2 indicates the core points of some currently done research works. The proposed one is compared with them too in the table. In this work, we have proposed SDN with NFV protection in the IoT environment, especially for smart industry (specially industry 4.0 applications) management to manage during COVID-19 period.

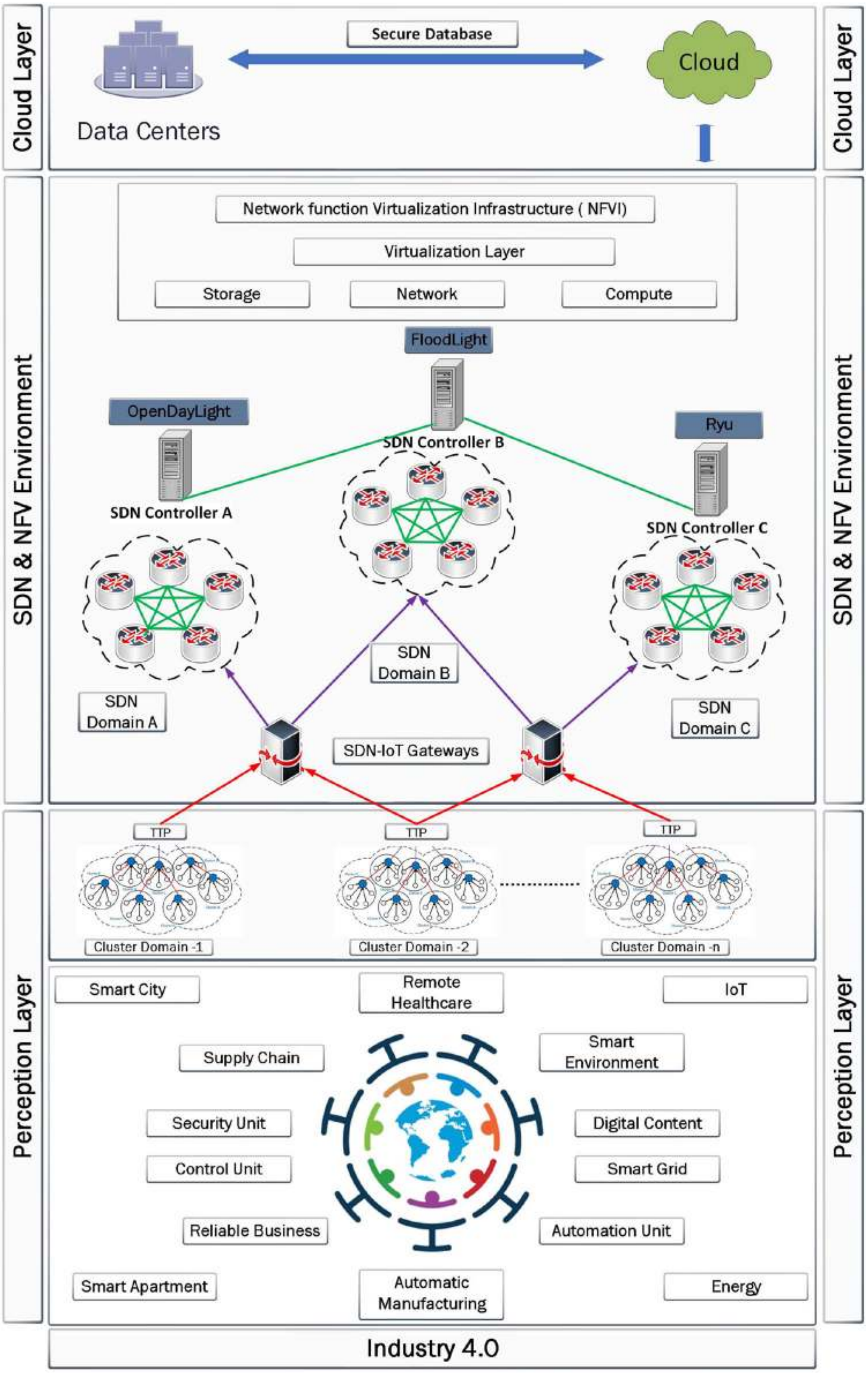
3 Proposed "EdgeSDN-I4COVID" Framework for smart industry management

To manage more effectively during the COVID-19 situation by utilizing SDN–IoT implementation, the authors present an SDN–IoT with NFV based network architecture, as depicted in Fig. 4. However, this framework has been divided into several connected stages for presenting the proposed methodology.

Table 2 Summary of current research works

Work and Year	Technologies	Research Objective	Comparison of recent research work with regard to:
Javaid et al. (2020) [10]	AI, IR 4.0	Managing COVID-19	An in depth review on the technologies of IR 4.0 to manage the pandemic stage.
Ndiaye et al. (2020) [11]	IoT, AI, Big data	Electronic health management system	A survey on the existing technologies such as, IoT, artificial intelligent to assist the health system in order to survive in this pandemic situation.
Ranaweera et al. (2020) [12]	5G, Multi access edge computing	Remote patient monitoring and without contact support to patient	A edge computing mechanism based on multi accessibility for providing treatment or health advice to COVID-19 affected patients remotely.
Abdel-Basset et al. (2020) [13]	Blockchain, IR 4.0, IoMT, 5G	Assist physicians to take quick actions to serve the patients.	Smart architecture to track the COVID-19 patients and manage PPE.
Garg et al. (2020) [14]	IoT, Blockchain	Development of a framework to minimize the outspread of the Covid 19	A framework on block chain's trust mechanism and RFID based tracing system to track the movement of animals and humans to control the spread of this infection.
Singh et al. (2020) [15]	IoT	Prediction of an outbreak and screening patients remotely	An IoT based smart framework to fight in the pandemic situation in every aspect.
Otoom et al. (2020) [16]	IoT, machine learning, cloud architecture	Collecting and analyzing past record of patient affected by coronavirus	Collection of data for detection of COVID-19 patient at early stage using machine learning algorithms.
Kolhar et al. (2020) [17]	CNN, IoT, Edge and Cloud computing	Face detection mechanism to assist the imposing of mask	Implemented a three layer framework to detect the face of human to monitor the movement of human.
Rahman et al. (2020) [18]	IoT, web tool, m-health	Defend pandemic using benefits of IoT	The technological assessment to help the whole world to survive in this pandemic.
Marbouh et al. (2020) [19]	Blockchain, Ethereum	Secured tracking mechanism	A comprehensive review on the scopes and applications of the secured blockchain technology.
Tsang et al. (2021) [20]	IoT, Blockchain	Examining the layered architecture of BIoT	Nine broad categories of the combined Blockchain and IoT structure in the perspective of research and development that is actually the core part of any industry.
Xu et al. (2019) [21]	IoT, Industry 4.0, Cloud computing, Cyber-physical systems, and Big data	Highlighted the potential guideline for Industry 4.0 to obtain a fully autonomous system	Big data methods are being used to enhance the scalability and security of Industry 4.0. In addition, in industry 4.0, a connection between cyber-physical systems and big data being developed.
Aheleroff et al. (2021) [22]	IoT, Cloud computing, Industry 4.0	Identified appropriate Industry 4.0 technologies and a holistic reference framework to finish the most difficult Digital Twin-enabled applications	Establish a strong connection between Digital Twin capabilities as a service and mass personalization. Smart scheduled maintenance, real-time tracking, and remote control are among the additional resources available.

Fig. 4 Proposed Framework



3.1 Industry 4.0 and application layer in pandemic

In this era of pandemic, the whole world is struggling hard to reduce the chances of getting affected by this virus. However, there are some preliminary measures that can help to reduce the spread of the virus. The social distancing and wearing a mask may decrease the chances of getting affected according to a study presented in [45]. This study shows that the possibility of transmission reduced by half with any additional distance of 3 m. As a consequence, people are living by the law of social distance and isolation that increased the working from home users. They need to do almost everything remotely. With the revolution of industry 4.0, it could be possible to move forward and tackle this situation.

3.2 Construction of perception layer for COVID situation

IoT-enabled devices like routers, switches, firewalls, and other storage devices help to forward data through the SDN-enabled gateway protocol efficiently. On the other hand, an SDN dynamic controller can be able to provide the IoT devices data, and the OpenFlow protocol aids this process. The proposed framework "EdgeSDN-I4COVID" provides reliable remote systems that will help to survive in this HCoV-19 situation by using IoT technologies properly. This IoT sensor-based data aids to reach the desired layer to the greater extent. In addition, these data are collected by the Cluster Head Selection (CHS) approach [7] as depicted in Fig. 5.

This technique forwards the data saving a significant amount of energy which is priceless in pandemic condition like COVID. Moreover, with the help of the SDN platform, the network is separated into three-layers such as data, control layer, and another one is application layer.

3.2.1 Applications of IoT to COVID-19

IoT will support the citizens with advanced automation and management during the lockdown and restriction of the social movement. The quick transferring of these services is also achievable as the services offered by IoT as it is linked to the internet. In this regard, IoT might be the best option to combat the current troublesome situation. The present situation made the health system almost collapsed. So the application area of IoT in the medical system is vast. From patient admission to patient monitoring and discharge, everything can be monitored and managed with the help of the interconnected sensors and devices [46]. The utility of IoT and artificial intelligence in the diagnosis of COVID-19 and in observing someone's health condition, is substantial [47]. Additionally by analyzing the previous reports of COVID patients, it can also be possible to predict the future condition of the infection rate and the death rate. According to the prediction the clinical staff can get ready for the future challenges which is far better than fighting against a situation that is totally unpredictable. The random forest algorithm can predict the possible cases, death rate by analyzing the data collected from sources and able to predict with an accuracy rate 94 percent [48]. In order to predict the risk of COVID-19 after classifying the dataset using SVM, ANFIS model can predict the risk with higher accuracy [49]. Apart from this, supervised machine learning shows immense performance to classify the disease using epidemiology which could also be employed to the IoT network [50]. Though there are myriad number of features, an effective sub-features could be estimated statistical models [51]. To trace the location where the number of COVID positive patient are immense, various services and application of IoT can be helpful since these information can be accessed by mobile phone or laptop in real time. Due to the lockdown situation, doctors are now a days more dependent on telemedicine that is another great example of application of IoT [15, 18].

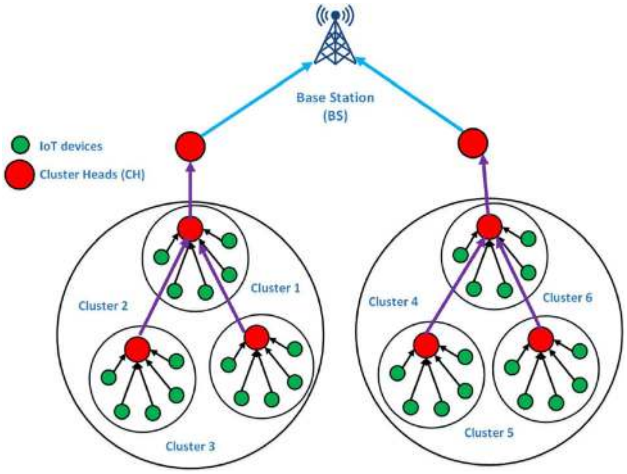


Fig. 5 IoT data selection scenario

3.2.2 Challenges of IoT for COVID-19 Pandemic

From the above-discussed section, it is evident that IoT with its capability of connectivity over the internet is a blessing to fight against the pandemic. However, there are a few challenges. The first and the most concerning issue is that the data, which is transferred over the cloud. It is vulnerable to the attacks and the attraction of hackers. The timeliness is another issue. As the total system is interconnected and dependent on each others functionalities, for this reason, to ensure that the data transmitted to the right destination within the shortest possible time, is another key concern. The sensors used in these kinds of services, are not from the same vendor. However, the formation of the sensor can be easily accessed by the providers. In order to overcome these issues, the authors proposed architecture using SDN and NFV that will enhance the security of it [28, 52, 53]. NFV can ensure the scalability and the issues of load balancing in the network. The real time data can be monitored with the help of Wireshark. Table 3 is a reflection of this section in which, the challenges and the technologies that could reduce them, are pointed out.

Table 3 Challenges and solutions

Challenges	Solutions
Security of the Data	SDN and OpenFlow Protocol
Time Management	SDN–IoT Gateway
Difference of Sensor Domain	IoT and NFV
Scalability and Load Balancing	NFV
Data Capturing and Monitoring	Wireshark
Life time and Energy Consumption	IoT Data Selection Procedure

3.2.3 Solution to Maintain Social Distancing Using IoT

In order to reduce the transmission of the virus known as coronavirus, the first and the most important thing is to wear a mask and disinfect hands properly, and the second is to preserve social isolation. For tracking the most affected area, IoT applications can be a great help. Again, evidence from newspaper outlets and other social media will also be beneficial, as when something unusual occurs, media covers that news. And with these results, IoT will determine whether or not a region is in a danger zone. Thus after sensing the environment under danger, people can stop or take proper action, such as wearing masks, avoiding busy areas, and so on. More recent work and meetings have been performed using several cloud-based apps, such as zoom, google meet, and Skype. Where it can be handled over the phone or laptop, to prevent a physical confrontation. In several nations, the school sector is already taking advantages of these innovations. Online classes, online presentations, online examinations are occurring all over the world. However, when several crucial discussions are taking place over the internet, maintaining the security of the software is now a significant concern. In this respect, the authors suggested a secure infrastructure capable of preserving the confidentiality of interconnected computers to secure data that is distributed through the cloud [11]. Securing the health related data can be done though the use of modular encryption process in the field of mobile computing [54].

3.3 SDN and NFV environment

In the pandemic situation, people obviously use remote platforms to perform their jobs and some sorts of daily chores like shopping, medication etc. These types of activities render a myriad information where SDN acts as a data organizer and controller. Such kind of technology performs different operations through distinct number of layers by means of plane.

3.3.1 Data Plane

In SDN environment, the data layer, is also called an infrastructure layer [55]. It is the lowest layer within the SDN climate, as shown in Fig. 6. This plane provides an activated SDN gateway to effectively link IoT forwarding devices such as a router, switch, firewall, storage, etc. This can also have two types of switches, such as virtual switches, similar to software-based switches typically operating on Linux OS and another one is physical switches associated with hardware-based switches. The plane uses the higher flow of physical forwarding devices. Apart from this, it switches into the network-based application domains responsible for forwarding, expending, and exchanging network packets [56]. A more stable TLS connector is being used to link the network forwarding devices and SDN controllers with each other. The data plane and the SDN controller(s) then communicate via the OpenFlow protocol. After that, all the overheads of the data passes through the control layer to constitute decisions for a data packet. The data plane captures all IoT transmission data from the layer of IoT infrastructure to bring it efficiently into the smart industry environment. Besides, the SDN-enabled data layer is responsible for efficiently providing all sensor data to the industry 4.0 applications. Thus, with the aid of Industry 4.0 technologies, a smart and safe framework can be built specifically with this SDN and NFV. It will solve several problems that the present world is facing because of the pandemic. The use of technology

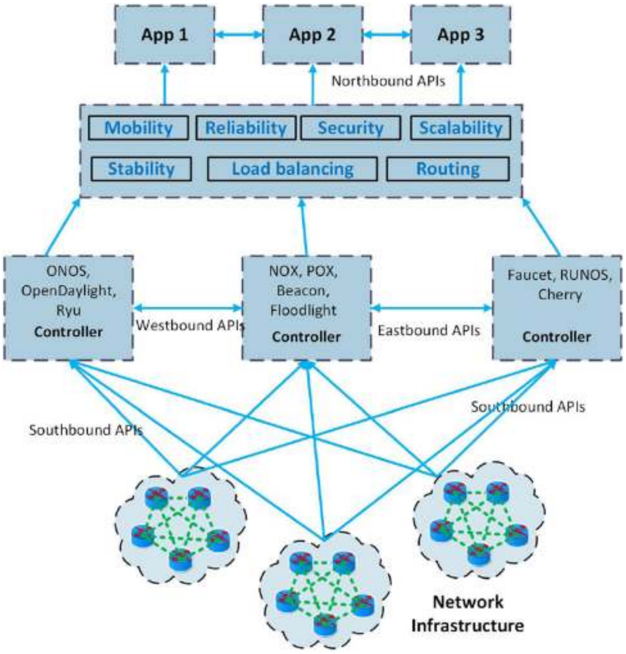


Fig. 6 SDN architecture

would help every sector, particularly the health sector, in the avoidance of many uncertain situations [57, 58].

3.3.2 Control Plane

The Control Plane (CP) [59] is the major backbone of the architecture of the SDN. However, a controller includes elements such as a logical central and functional controller as primary components. In addition, the logic controller offers an extensive network connectivity service. In the SDN architecture, CP is able to map between the forwarding and application layers. It provides various forms of networking tools for the app that it would need. Moreover, CP architecture also contains some tremendous protocol such as OpenFlow, Operating systems like network OS (ONOS) and cloud OS(Openstack), OpenDayLight used for supporting OpenFlow protocol considered as a framework, another controller is named as Floodlight and beacons(Java-based). Following that, the controller adopted interfaces named southbound, northbound, and eastbound to interact appropriately. In addition, this layer can be able to provide some extra benefits like more stability, load balancing, reliability, routing, mobility, and so on into the desired system greatly as depicted in Fig. 6. Regarding this approach, this controller also enhances the networking system that can use high data security and privacy in the architecture of the smart industry management. This method thus protects safe and confidential user data. Another issue with this pandemic is that if they are merely suspected of this disease, people often face social abuses. The security of data is the top most need in this era of pandemic. As the present world is doing maximum work over the Internet that is, from education [60] to business every possible things are over the web so there is possibility that the data may not reach to the proper destination within time. This may cause serious problem in every sector. In this regard our proposed architecture might be a possible solution that can ensure the safety of data that is being transferred as well as the fast transmission of information.

3.3.3 Application Plane

The Application Plane (AP) contains all of the smart industry platform's elements and services. Then, the SDN-based scheme has committed a vast number of preferences dynamically to update the forwarding flow rules effectively. The AP also enhances networking services over the physical forwarding objects or virtual objects between the control and application platform. It admits more prominent stages of network configuration and management called network data analytics, and specialized functions that are expected to be treated in big data centers. Furthermore, this plane admits several smart industry services 4.0 environments [61] like smart energy, security, smart automation, load balancing, routing management, smart parking, control unit, smart healthcare, manufacturing, etc. as shown in Fig. 4. However, the NFV virtually manage the resources and perform different computational task within the IoT network. The other functionalities of NFV are discussed in the later section.

3.4 Smart industry management security and services during COVID-19

The coronavirus shifted the whole world to smart technology based environment. It has made every person realize the importance of a smart industrial system. A creative industry includes the safety and security unit, control unit, weather prediction sensor, water management unit, energy supplier and load manager unit, smart car parking, build sensor control unit, etc. [62]. Where the control unit maintains an automatic and manual industry management system as desired, the security unit provides the auto-secured process for smart industry control by detecting intruders. One of the most essential component of inventive industries is the power and energy supplier unit which can handle the entire industries energy load efficiently for each service activation. Besides, smart industries facilitate to make our life cost-effective and easier, maintain a more protected environment and more unharmed, generative and comfortable environment specially when everything is locked down [63]. In order to respond, a smart industry's automation unit can provide us with tremendous potentials such as fire detection systems, CCTV, access control systems and intelligent lighting, intelligent car parking, and so on. A productive industry can establish automation and highly protected secure services that can guide our lives. This automation also decreases social interaction in a wide range [26] that will help sustain social distance while retaining progress in any job on the bright side. Thus, this proposed architecture would control where the computer can work, and no human intervention is required. Above all, it will allow the overall industry 4.0 to thrive in pandemic situation by keeping development or other operations regular and also maintaining a less crowded place to work.

However, opportunities for Industry 4.0 are divided into six major categories, manufacturing versatility that exists during the manufacture of small lots; serial prototype speed; higher processing capacity; lower set-up costs and less system downtime; better product quality and less rejected manufacturing; and enhanced consumer perception of the goods [64]. It enables production lines, business processes, and departments to interact regardless of location, time zone, platform, or other factors. It allows information to be disseminated across the organization, gained without any human intervention by a sensor on a computer in one field.

Fig. 7 clarifies the effects of COVID-19 outbreak on the applications of Industry 4.0 where IoTs, Cybersecurity, Cloud Computing and Big Data Analytics suffered the most [28, 65]. Their performance declined the standard during the pandemic period. Some other technologies are also listed in the Figure. On the other hand, the SDN and NFV architecture can provide data protection, and different sorts of services as seen in Fig. 8. When the data is attacked or not reached at the destination within due time, it will make the current situation worse because the intruders could hack the overall system and take control of the system. The details functionality of SDN and NFV has been discussed in the previous sections. However, the overall industry 4.0 can be benefited with the aid of this SDN NFV-based stable architecture, which in turn will help the overall environment to survive the present Coronavirus situation. As the system is linked to the industry's networking system as shown in Fig. 8, the system will be able to create a more strong network that will distribute, monitor, and provide the necessary information inside the network domain with protection. Additionally, the waste disposal management is another concern [66]. As the waste itself may contain the virus so the disposal system must be properly monitored. This architecture will assist the monitoring of the waste disposal system as well.

4 Implementation and network design

4.1 Environment setup

In this section, we discuss the experimental setup to validate our proposed methodology. As the Emulator Mininet and Mininet-Wifi were used with OpenFlow protocol in the SDN environment. The authors simulated the experiment on the Ubuntu (GNU/Linux) operating system and the system has x86 processor (2.20GHz), 500GB SSD, 16 GB primary memory (RAM), 1TB ROM, and some other external memories. Besides, the Wireshark platforms have utilized to see the captured packets of the SDN-based IoT network. In addition, the summary of simulation setup as shown in Table 4.

4.2 Network topology design

The topology of more than 45 network nodes is shown in Fig. 9. With the above 45 nodes, the network topology can be broken down into 9 access points (APs) with 46 stations (sta) linked to them. After designing the topology, it can facilitate communication between nodes by pinging them and capturing traffic flow packets for each topology in the Wire shark platform. Furthermore, the graphs for this network can be thoroughly considered to make decisions about the effective utilization of each topology.

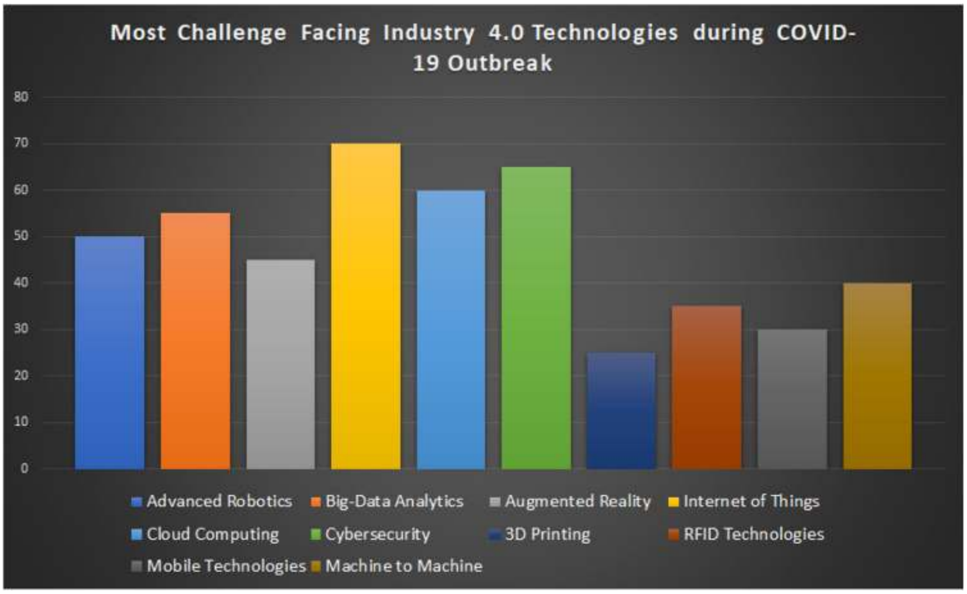


Fig. 7 Most challenge facing industry 4.0 technologies during COVID-19 outbreak

Fig. 8 Industry 4.0 smart services

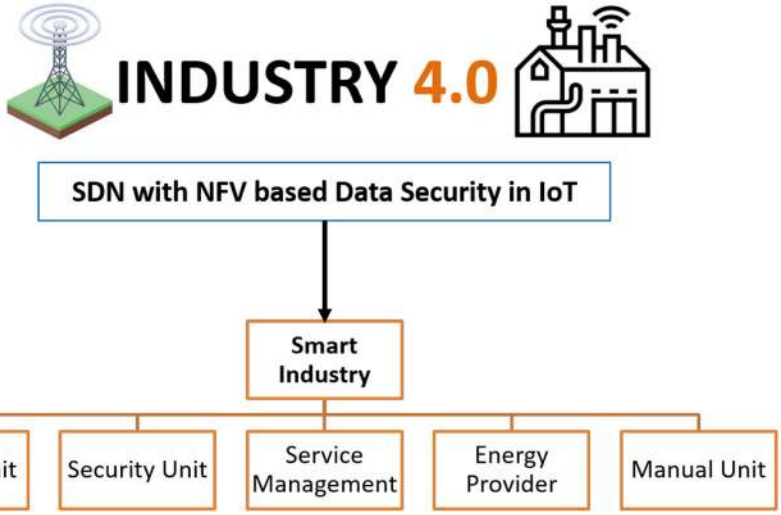


Table 4 Considered parameters for simulation setup

	Parameters name	Values
General parameters	Emulator	Mininet 2.2.2
	Packet Analyzer	Wireshark
	Simulation Area	3000m X 3000m
SDN Parameters	No. of SDN Controllers	7
	OpenFlow switches	8
	Gateways	4
	SDN Routing Protocol	OpenFlow
Measured parameters	Throughput comparisons	3000 Mb/s
	Data response time analysis	-
	Data failure rate	-
	Tcp Trace (Sequence number)	-
Others parameters	Number of IoT devices	300
	Simulation Times	500s
	Data Rate	10 Mbps
	Node Transmit Packet Size	512-1024 bytes

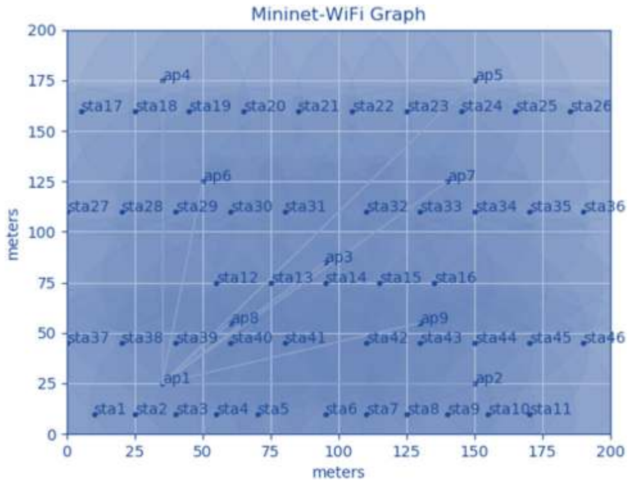


Fig. 9 Network topology design in mininet-WiFi platform

5 Results analysis and discussion

In this segment, authors have evaluated the performances of the depicted model in various parameters like Throughput, Response time, Packet failure rate, and Sequence number (Tcp Trace).

5.1 Throughput analysis

In Fig. 10 demonstrates the no. of 50, 100, and 200 nodes suitably. In addition, the 200 nodes show a much better appearance than the no. of 50 and 100 nodes.

Where the throughput means how much data can be transmitted in a distinct time from one location to another in Kilobits Per Second (Kbps). Furthermore, the authors compared the core system and proposed system (200

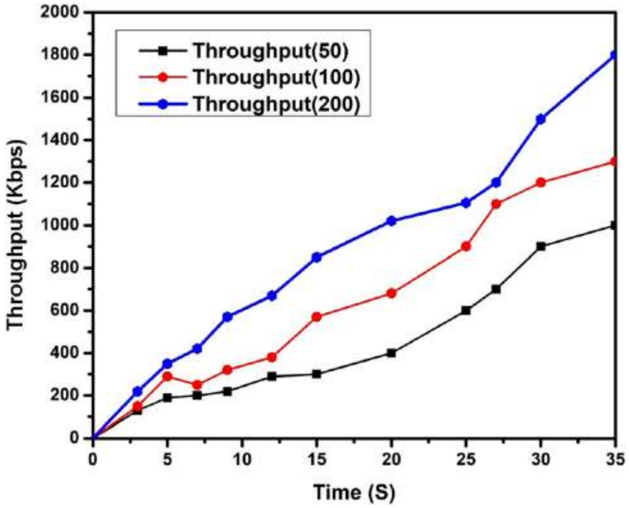


Fig. 10 Throughput comparisons (50 vs. 100 vs. 200 nodes) with Respect to Transaction Time

nodes) to evaluate the performance, as shown efficiently in Fig. 11. Then, the presented model has been exhibited better performance than the core system because it is free from unwanted attacks.

5.2 Response time comparison

For calculating response time Fig. 12 essentially shows an overview of results based on the number of devices. When the number of devices increases, the response time for each also increases. The response time for both, however, is nearly similar at the initial stage. But performing after a particular time, we have notified the involvement of some attacks such as DDoS, Flooding, Malware attack, the proposed system will show better performance than the existing traditional model. As a result, all devices in the smart industrial environment respond swiftly using the presented model.

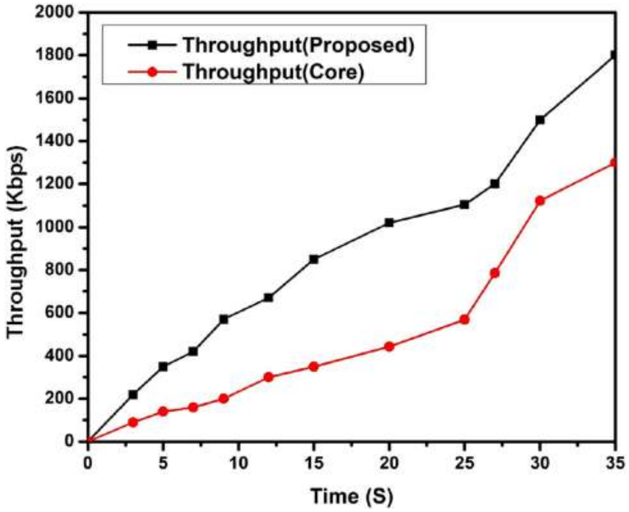


Fig. 11 Throughput comparisons with respect to transaction time

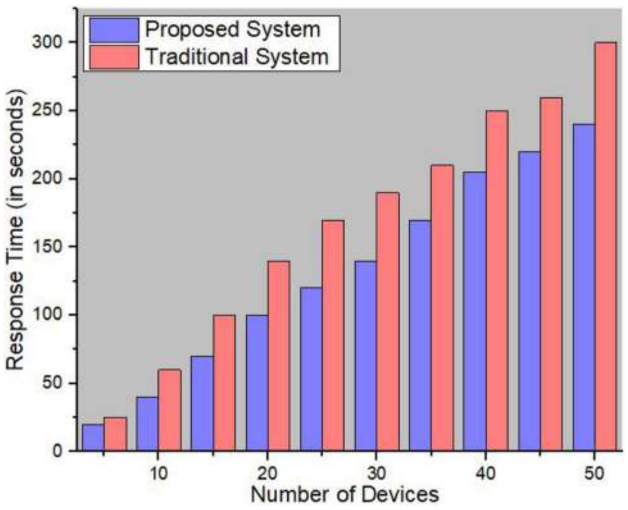


Fig. 12 Response time comparisons with respect to the number of devices

5.3 Analysis of packet failure rate

Figure 13 shows the rate of data failure for the different number of packets. The study shows that the suggested scheme achieves the minimum node failure rate in the lower commit of attacks. Also, the authors has found that the rate of node failure for both was initially lower. Besides with the increasing number of packets, the rate of failure is also growing. Hence, they have found that the node failure rate is mainly 8% without involving our proposed scheme; on the other hand, the system rate is provided only 6%. Yet the node failure ratio is 80% to 90% after a limited time in the traditional system. On the contrary, the failure rate of

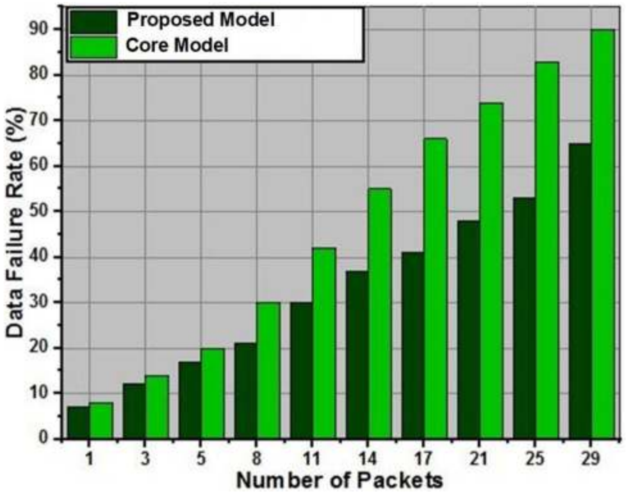


Fig. 13 Nodes failure rate comparisons with respect to the number of packets

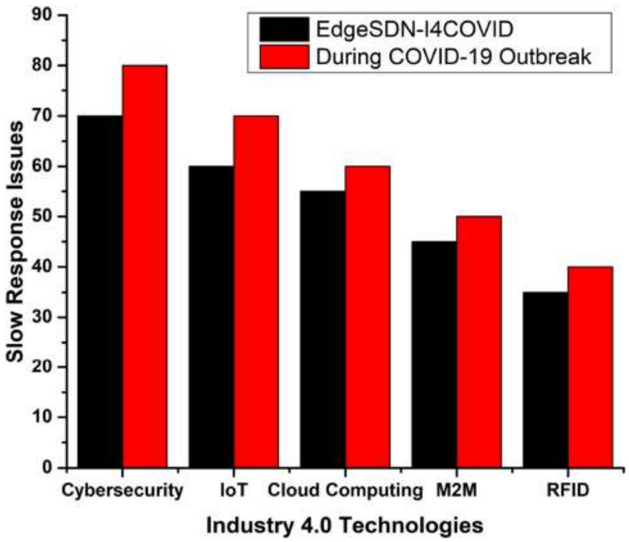


Fig. 14 Response issues with respect to the technologies [10, 28]

the presented system is just 50 to 60 percent. Therefore, the above review means that the proposed protected method achieves a more advantageous node failure rate, which is substantially a minimum rate without an essential number of packets than the previous study did.

5.4 Discussion

From the performance analysis, it is obvious that the system will be fruitful at the application level. The primary intention of the proposed architecture is to supply an environment where lots of people can continue their business online without any issue of service failure due to the excess strike to the network during especial issues such as a lockdown. The proposed one has the better throughput and response time compared to the traditional and core models that also include less data failure, so there will be no concern regarding these types of issues. Different industries can not continue their production because of the isolation of their experts. Industry 4.0 is the procession in the field of network technology with a high speed of the Internet and various services, as a result, the proposed architecture will be able to fulfill the demand for a real-time working environment. In the light of the benefits of our architecture, Fig. 14 shows the slow response

Table 5 Comparative summary among different architectures and the proposed one

Works	Technologies				COVID-19	Findings
	IoT	SDN	NFV	IR 4.0		
Kumar et al. [2]	✓	X	X	X	✓	A monitoring system to decrease the spread of COVID-19 viral disease
Javaid et al. [10]	X	X	X	✓	✓	Industry 4.0 technology can assist in the proper isolation of an infected patient, thus minimizing disease spread
Kumar et al. [28]	X	X	X	✓	✓	Recognized twelve significant problems in the retail sector and adopted Industry 4.0 technology to tackle them.
Abdel et al. [13]	✓	X	X	✓	✓	The disruptive technologies are utilized to dissolve and restrict the spread of COVID-19 and COVID-19's patients assure the consequence of an intelligent model
Garg et al. [14]	✓	X	X	X	✓	Study the different type of contact tracing application available and provided a better solution for tracing in order to restrict or identify the spread of the virus
Ndiaye et al. [11]	✓	X	X	✓	✓	An overview of IoT based healthcare system to fight against pandemic and future of healthcare system incorporating big data, drone and other latest technologies.
Singh et al. [15]	✓	X	X	X	✓	Identified framework of IoT to handle the lockdown situation due to pandemic worldwide by ensuring secured virtual meeting monitoring healthcare system remotely and online education system as well.
Otoom et al. [16]	✓	X	X	X	✓	With the aid of machine learning algorthims the authors in this work proposed a framework that can identify cases of COVID-19 by analysis the sysmptoms accurately and without delay.
Kolhar et al. [17]	✓	X	X	X	✓	Biometric system with the assistance of IoT to restrict the movement of the people during lockdown also to detect whether there is a mask on the face or not.
Rahman et al. [18]	✓	X	X	X	✓	Studied the possibilities of IoT models to fight against enquoteHCoV-19
Proposed Work	✓	✓	✓	✓	✓	Provided an SDN–IoT based intelligent model for Industry 4.0 and Incorporated among the technologies such as IoT, SDN, NFV, and Cloud to meet the demands for the COVID-19 situation

percentage of our model comparing to some of the technologies of Industry 4.0 where "EdgeSDN-I4COVID" performs with less average response time. However, the presented architecture will be consummated to the Industry 4.0 applications during such kinds of outbreaks. Besides, a comparative summary is given in Table 5 to visualize the basic difference of the proposed system from the other studies to get a better establishment of our work. As mentioned in the Table 5 it is clear that there has been great work to fight against COVID-19 but included only IoT and IR 4.0. Further, the proposed study provided an SDN–IoT-based intelligent model for Industry 4.0 and Incorporated among the technologies such as IoT, SDN, NFV, and Cloud to meet the demands for the COVID-19 situation. Additionally, the suggested method performs better by minimizing the node failure rate compared to the traditional system. Also, the response time in presence of attacks shows better performance than the conventional model. There are a lot of advanced researches in the field of the network including the COVID situation but this one is the most technically sound and advanced.

6 Conclusion

This paper proposed the architecture, incorporating SDN with NFV technology, an IoT-SDN model with multiple controller execution in order to manage an automated industrial system during the spread of the virus SARS-COV-2 condition. Due to the outbreak, the present world is depending on the internet and performing almost every important activities over the cloud. In this context, the proposed system model able to provide enormous automation with security and privacy within the networking system that will make the industry 4.0 application efficient and reliable in order to effectively manage the pandemic situation. This system enables an intelligent and smart industry too and also helps us to maintain isolation and keep social distancing while encouraging the adoption of Industry 4.0. Additionally, our described model can handle numerous attacks, but it's still in the process of developing. In near future, we will include the distributed Blockchain technology to handle data confidentially as well as more security in the current model.

Acknowledgements This research has no funding.

Author Contributions CC, AA, AR, ZR and SS designed the study. AR, MRK, DK and MJI wrote the manuscript; AR, MRK, MJI and DK collected data. SS, CC, AR, ZR, and AA edited the manuscript; MRK, AR, MJI and DK carried out the analyses. MJI, MRK and AR generated all figures and tables. All authors have read and approved the final version of the paper.

Declarations

Conflict of Interest The authors declare no competing financial and non-financial interests.

References

1. https://www.worldometers.info/coronavirus/ (Worldometers, Accessed on: 30.03.21)
2. Kumar, K., Kumar, N., Shah, R.: Role of iot to avoid spreading of covid-19. Int. J. Intell. Netw. **1**, 32–35 (2020)
3. Zeng, J., Huang, J., Pan, L.: How to balance acute myocardial infarction and covid-19: the protocols from sichuan provincial people's hospital. Intensive Care Med. **46**(6), 1111–1113 (2020)
4. Mukherjee, B.K., Pappu, M.S.I., Islam, M.J., Acharjee, U.K.: An SDN based Distributed IoT Network with NFV Implementation for Smart Cities. In press: 2nd International Conference on Cyber Security and Computer Science (ICONCS-2020) (Springer, 2020)
5. Rahman, A., Islam, M.J., Sunny, F.A., Nasir, M.K.: Distblocksdn: A distributed secure blockchain based sdn-iot architecture with nfv implementation for smart cities. In: 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), pp. 1–6 (2019). https://doi.org/10.1109/ICIET48527.2019.9290627
6. Yao, G., Bi, J., Guo, L.: On the cascading failures of multi-controllers in software defined networks. In: 2013 21st IEEE International Conference on Network Protocols (ICNP) pp. 1–2 (2013)
7. Islam, M.J., Mahin, M., Roy, S., Debnath, B.C., Khatun, A.: Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation for smart cities. In: 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), pp. 1–6. IEEE (2019)
8. Liu, Y., Kuang, Y., Xiao, Y., Xu, G.: Sdn-based data transfer security for internet of things. IEEE Internet Things J. **5**(1), 257–268 (2017)
9. Kalkan, K., Zeadally, S.: Securing internet of things with software defined networking. IEEE Commun. Mag. **56**(9), 186–192 (2017)
10. Javaid, M., Haleem, A., Vaishya, R., Bahl, S., Suman, R., Vaish, A.: Industry 4.0 technologies and their applications in fighting covid-19 pandemic. Diabetes & Metabolic Syndrome: Clinical Research & Reviews (2020)
11. Ndiaye, M., Oyewobi, S.S., Abu-Mahfouz, A.M., Hancke, G.P., Kurien, A.M., Djouani, K.: Iot in the wake of covid-19: a survey on contributions, challenges and evolution. IEEE Access **8**, 186821–186839 (2020)
12. Ranaweera, P.S., Liyanage, M., Jurcut, A.D.: Novel mec based approaches for smart hospitals to combat covid-19 pandemic. In: IEEE Consumer Electronics Magazine (2020)
13. Abdel-Basset, M., Chang, V., Nabeeh, N.A.: An intelligent framework using disruptive technologies for covid-19 analysis. Technological Forecasting and Social Change p. 120431 (2020)
14. Garg, L., Chukwu, E., Nasser, N., Chakraborty, C., Garg, G.: Anonymity preserving iot-based covid-19 and other infectious disease contact tracing model. IEEE Access **8**, 159402–159414 (2020)
15. Singh, R.P., Javaid, M., Haleem, A., Suman, R.: Internet of things (iot) applications to fight against covid-19 pandemic. Diabetes Metab. Syndr. Clin. Res. Rev. **14**(4), 521–524 (2020)
16. Otoom, M., Otoum, N., Alzubaidi, M.A., Etoom, Y., Banihani, R.: An iot-based framework for early identification and monitoring of covid-19 cases. Biomed. Signal Process. Control **62**, 102149 (2020)

17. Kolhar, M., Al-Turjman, F., Alameen, A., Abualhaj, M.M.: A three layered decentralized iot biometric architecture for city lockdown during covid-19 outbreak. IEEE Access **8**, 163608–163617 (2020)
18. Rahman, M.S., Peeri, N.C., Shrestha, N., Zaki, R., Haque, U., Ab Hamid, S.H.: 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)
19. Marbouh, D., Abbasi, T., Maasmi, F., Omar, I.A., Debe, M.S., Salah, K., Jayaraman, R., Ellahham, S.: Blockchain for covid-19: review, opportunities, and a trusted tracking system. Arab. J. Sci. Eng. **45**, 9895–9911 (2020)
20. Tsang, Y., Wu, C., Ip, W., Shiau, W.L.: Exploring the intellectual cores of the blockchain-internet of things (biot). Journal of Enterprise Information Management (2021)
21. Xu, L.D., Duan, L.: Big data for cyber physical systems in industry 4.0: a survey. Enterprise Inf. Syst. **13**(2), 148–169 (2019)
22. Aheleroff, S., Xu, X., Zhong, R.Y., Lu, Y.: Digital twin as a service (dtaas) in industry 4.0: an architecture reference model. Adv. Eng. Inf. **47**, 101225 (2021)
23. Bartik, A.W., Bertrand, M., Cullen, Z.B., Glaeser, E.L., Luca, M., Stanton, C.T.: How are small businesses adjusting to covid-19? Early evidence from a survey. Tech. rep, National Bureau of Economic Research (2020)
24. Bartik, A.W., Bertrand, M., Cullen, Z., Glaeser, E.L., Luca, M., Stanton, C.: The impact of covid-19 on small business outcomes and expectations. Proc. Natl. Acad. Sci. U.S.A. **117**(30), 17656–17666 (2020)
25. Gomm, M.L.: Supply chain finance: applying finance theory to supply chain management to enhance finance in supply chains. Int. J. Logist. Res. Appl. **13**(2), 133–142 (2010)
26. Bragazzi, N.L.: Digital technologies-enabled smart manufacturing and industry 4.0 in the post-covid-19 era: lessons learnt from a pandemic (2020)
27. Cheng, J., Chen, W., Tao, F., Lin, C.L.: Industrial iot in 5g environment towards smart manufacturing. J. Ind. Inf. Integr. **10**, 10–19 (2018)
28. Kumar, M.S., Raut, R.D., Narwane, V.S., Narkhede, B.E.: Applications of industry 4.0 to overcome the covid-19 operational challenges. Diabetes Metab. Syndr. Clin. Res. Rev. **14**(5), 1283–1289 (2020)
29. Karakus, M., Durresi, A.: A survey: control plane scalability issues and approaches in software-defined networking (sdn). Comput. Netw. **112**, 279–293 (2017)
30. Murat, K.., Arjan, D.: Quality of service (qos) in software defined networking (sdn): a survey. J. Netw. Comput. Appl. **80**, 200–218 (2017)
31. Sahay, R., Meng, W., Jensen, C.D.: The application of software defined networking on securing computer networks: a survey. J. Netw. Comput. Appl. **131**, 89–108 (2019)
32. Rahman, A., Islam, M.J., Saikat Islam Khan, M., Kabir, S., Pritom, A.I., Razaul Karim, M.: Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network. In: 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), pp. 1–6 (2020). https://doi.org/10.1109/STI50764.2020.9350419
33. Abdelaziz, A., Fong, A.T., Gani, A., Garba, U., Khan, S., Akhunzada, A., Talebian, H., Choo, K.K.R.: Distributed controller clustering in software defined networks. PLoS ONE **12**(4),(2017)
34. Cerroni, W., Buratti, C., Cerboni, S., Davoli, G., Contoli, C., Foresta, F., Callegati, F., Verdone, R.: Intent-based management and orchestration of heterogeneous openflow/iot sdn domains. In: 2017 IEEE Conference on Network Softwarization (NetSoft), pp. 1–9. IEEE (2017)
35. Jacquenet, C., Boucadair, M.: A software-defined approach to iot networking. ZTE Commun. **1**, 012 (2016)
36. Bull, P., Austin, R., Popov, E., Sharma, M., Watson, R.: Flow based security for iot devices using an sdn gateway. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 157–163. IEEE (2016)
37. Al Shuhaimi, F., Jose, M., Singh, A.V.: Software defined network as solution to overcome security challenges in iot. In: 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 491–496. IEEE (2016)
38. Rahman, A., Nasir, M.K., Rahman, Z., Mosavi, A., Shahab, S., Minaei-Bidgoli, B.: Distblockbuilding: a distributed blockchain-based sdn-iot network for smart building management. IEEE Access **8**, 140008–140018 (2020)
39. Islam, M.J., Mahin, M., Khatun, A., Roy, S., Kabir, S., Debnath, B.C.: A comprehensive data security and forensic investigation framework for cloud-iot ecosystem. GUB J. Sci. Eng. **4**, 64–75 (2019)
40. Tayyaba, S.K., Shah, M.A., Khan, O.A., Ahmed, A.W.: Software defined network (sdn) based internet of things (iot) a road ahead. In: Proceedings of the International Conference on Future Networks and Distributed Systems, pp. 1–8 (2017)
41. Yassein, M.B., Aljawarneh, S., Al-Rousan, M., Mardini, W., Al-Rashdan, W.: Combined software-defined network (sdn) and internet of things (iot). In: 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), pp. 1–6. IEEE (2017)
42. Bagdadee, A.H., Zhang, L., Remus, M.S.H.: A brief review of the iot-based energy management system in the smart industry. In: Artificial Intelligence and Evolutionary Computations in Engineering Systems, pp. 443–459. Springer (2020)
43. Mabkhot, M.M., Al-Ahmari, A.M., Salah, B., Alkhalefah, H.: Requirements of the smart factory system: a survey and perspective. Machines **6**(2), 23 (2018)
44. Ma, Y., Chen, Y., Chen, J.: Sdn-enabled network virtualization for industry 4.0 based on iots and cloud computing. In: 2017 19th International Conference on Advanced Communication Technology (ICACT), pp. 199–202 (2017)
45. Chu, D.K., Akl, E.A., Duda, S., Solo, K., Yaacoub, S., Schünemann, H.J., El-harakeh, A., Bognanni, A., Lotfi, T., Loeb, M., et al.: Physical distancing, face masks, and eye protection to prevent person-to-person transmission of sars-cov-2 and covid-19: a systematic review and meta-analysis. The Lancet (2020)
46. Singh, R.P., Javaid, M., Haleem, A., Suman, R.: Internet of things (iot) applications to fight against covid-19 pandemic. Diabetes Metab. Syndr. Clin. Res. Rev. **14**(4), 521–524 (2020)
47. Chakraborty, C., Abougreen, A.N.: Intelligent internet of things and advanced machine learning techniques for Covid-19. EAI Endorsed Trans. Pervasive Health Technol. **7**(26), e1 (2021)
48. Iwendi, C., Bashir, A.K., Peshkar, A., Sujatha, R., Chatterjee, J.M., Pasupuleti, S., Mishra, R., Pillai, S., Jo, O.: Covid-19 patient health prediction using boosted random forest algorithm. Front. Public Health **8**, 357 (2020)
49. Iwendi, C., Mahboob, K., Khalid, Z., Javed, A.R., Rizwan, M., Ghosh, U.: Classification of covid-19 individuals using adaptive neuro-fuzzy inference system. Multimedia Syst. (2021). https://doi.org/10.1007/s00530-021-00774-w
50. Muhammad, L., Algehyne, E.A., Usman, S.S., Ahmad, A., Chakraborty, C., Mohammed, I.A.: Supervised machine learning models for prediction of covid-19 infection using epidemiology dataset. SN Comput. Sci. **2**(1), 1–13 (2021)
51. Bhuyan, H.K., Chakraborty, C., Pani, S.K., Ravi, V.: Feature and subfeature selection for classification using correlation coefficient and fuzzy model. IEEE Trans. Eng. Manag. (2021). https://doi.org/10.1109/TEM.2021.3065699

52. Kumar, S., Raut, R.D., Narkhede, B.E.: A proposed collaborative framework by using artificial intelligence-internet of things (ai-iot) in covid-19 pandemic situation for healthcare workers. Int. J. Healthcare Manag **13**(4), 337–345 (2020)
53. Ndiaye, M., Oyewobi, S.S., Abu-Mahfouz, A.M., Hancke, G.P., Kurien, A.M., Djouani, K.: Iot in the wake of covid-19: a survey on contributions, challenges and evolution. IEEE Access **8**, 186821–186839 (2020). https://doi.org/10.1109/ACCESS.2020.3030090
54. Shabbir, M., Shabbir, A., Iwendi, C., Javed, A.R., Rizwan, M., Herencsar, N., Lin, J.C.W.: Enhancing security of health information using modular encryption standard in mobile cloud computing. IEEE Access **9**, 8820–8834 (2021)
55. Dargahi, T., Caponi, A., Ambrosin, M., Bianchi, G., Conti, M.: A survey on the security of stateful sdn data planes. IEEE Commun. Surv. Tutor. **19**(3), 1701–1725 (2017)
56. Rahman, A., Islam, M.J., Rahman, Z., Reza, M.M., Anwar, A., Mahmud, M.P., Nasir, M.K., Noor, R.M.: Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium. IEEE Access **8**, 209594–209609 (2020)
57. Nguyen, T., Duong Bang, D., Wolff, A.: 2019 novel coronavirus disease (covid-19): paving the road for rapid detection and point-of-care diagnostics. Micromachines **11**(3), 306 (2020)
58. Iyer, M., Jayaramayya, K., Subramaniam, M.D., Lee, S.B., Dayem, A.A., Cho, S.G., Vellingiri, B.: Covid-19: an update on diagnostic and therapeutic approaches. BMB Rep. **53**(4), 191 (2020)
59. Rahman, A., Islam, M.J., Montieri, A., Nasir, M.K., Reza, M.M., Band, S.S., Pescapè, A., Hasan, M., Sookhak, M., Mosavi, A.: Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot. IEEE Access **9**, 28361–28376 (2021). https://doi.org/10.1109/ACCESS.2021.3058244
60. Darma, D., Ilmi, Z., Darma, S., Syaharuddin, Y.: Covid-19 and its impact on education: Challenges from industry 4.0 (2020)
61. Mohamed, N., Al-Jaroodi, J., Lazarova-Molnar, S.: Leveraging the capabilities of industry 4.0 for improving energy efficiency in smart factories. IEEE Access **7**, 18008–18020 (2019)
62. Zakoldaev, D., Gurjanov, A., Shukalov, A., Zharinov, I.: The application of krone model to describe the production facilities of the industry 4.0 smart factories. J. Phys. Conf. Ser. **1333**, 72031 (2019)
63. Rahman, A., Sara, U., Kundu, D., Islam, S., Islam, M.J., Hasan, M., Rahman, Z., Nasir, M.K.: Distb-sdoindustry: Enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture. Int. J. Adv. Comput. Sci. Appl. **11**(9), 100 (2020)
64. Oztemel, E., Gursev, S.: Literature review of industry 4.0 and related technologies. J. Intell. Manuf. **31**(1), 127–182 (2020)
65. Kamal, M., Aljohani, A., Alanazi, E.: Iot meets covid-19: Status, challenges, and opportunities. arXiv preprint arXiv:2007.12268 (2020)
66. Chauhan, A., Jakhar, S.K., Chauhan, C.: The interplay of circular economy with industry 4.0 enabled smart city drivers of healthcare waste disposal. J. Clean. Prod. **279**, 154 (2020)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Anichur Rahman received the B.Sc. and M.Sc. degree in Computer Science and Engineering from Mawlana Bhashani Science and Technology University (MBSTU), Tangail, Bangladesh in 2017 and 2020 respectively. Currently, he is working as a Lecturer at Computer Science and Engineering (CSE), National Institute of Textile Engineering and Research (NITER), Constituent Institute of the University of Dhaka, Savar, Dhaka, Bangladesh since January 2020 to present. His research interests include Internet of Things (IoT), Blockchain (BC), Software Defined Networking (SDN), Image Processing, Machine Learning, 5G, Industry 4.0 and Data Science.

Chinmay Chakraborty Dr. Chinmay Chakraborty is an Assistant Professor (Sr.) in the Electronics and Communication Engineering, Birla Institute of Technology, Mesra, India. He worked at the Faculty of Science and Technology, ICFAI University, Agartala, Tripura, India as a Sr. Lecturer. He worked as a Research Consultant in the Coal India project at Industrial Engineering & Management, IIT Kharagpur. He worked as a Project Coordinator of the Telecommunication Convergence Switch project under the Indo-US joint initiative. He also worked as a Network Engineer in System Administration at MISPL, India. His main research interests include the Internet of Medical Things, Wireless Body Sensor Networks, Wireless Networks, Telemedicine, m-Health/e-health, and Medical Imaging. Dr. Chakraborty has published more than 100 papers at reputed international journals, conferences, book chapters, and books. He is an Editorial Board Member in the different Journals and Conferences. He is serving as a Guest Editor of MDPI-Future Internet Journal, Wiley-Internet Technology Letters, Springer-Annals of Telecommunications, Springer - International Journal of System Assurance Engineering and Management, Springer-Environment, Development, and Sustainability, and Lead Guest Editors of IEEE-JBHI, IGI-International Journal of E-Health and Medical Communications, Springer - Multimedia Tools and Applications, TechScience CMC, Springer - Interdisciplinary Sciences: Computational Life Sciences, Inderscience- International Journal of Nanotechnology, BenthamScience-Current Medical Imaging, Journal of Medical Imaging and Health Informatics, Lead Series Editor of CRC-Advances in Smart Healthcare Technologies, and also Associate Editor of International Journal of End-User Computing and Development, Journal of Science & Engineering, Int. Journal of Strategic Engineering, and has conducted a session of SoCTA-19, ICICC - 2019, Springer CIS 2020, SoCTA-20, SoCPaR 2020, and also a reviewer for international journals including IEEE Access, IEEE Sensors, IEEE Internet of Things, Elsevier, Springer, Taylor & Francis, IGI, IET, TELKOMNIKA Telecommunication Computing Electronics and Control, and Wiley. Dr. Chakraborty is co-editing several books on Smart IoMT, Healthcare Technology, and Sensor Data Analytics with Elsevier, CRC Press, IET, Pan Stanford, and Springer. He has served as a Publicity Chair member at renowned international conferences including IEEE Healthcom, IEEE SP-DLT. Dr. Chakraborty is a member of Internet Society, Machine Intelligence Research Labs, and Institute for Engineering Research and Publication. He received a Best Session Runner-up Award, Young Research Excellence Award, Global Peer Review Award, Young Faculty Award, and Outstanding Researcher Award. He was the speakers for AICTE, DST sponsored FDP and CEP Short Term Course.

Adnan Anwar is a Lecturer and Deputy Director of postgraduate cybersecurity studies at the School of Information Technology. Previously he has worked as a Data Scientist at Flow Power. He has over 8 years of research, and teaching experience in universities and research labs including NICTA, La Trobe University, and University of New South Wales. He received his PhD and Master by Research degree from UNSW. He is broadly interested in the security research for critical infrastructures including Smart Energy Grid, SCADA system, and application of machine learning and optimization techniques to solve cyber security issues for industrial systems. He has been the recipient of several awards including UPA scholarship, UNSW TFR scholarship, best paper award and several travel grants including ACM and Postgraduate Research Student Support (PRSS) travel grants. He has authored over 40 articles including high-impact journals (mostly in Q1), conference articles and book chapters in prestigious venues. He is an active member of IEEE for over 9 years and serving different committees.

Md. Razaul Karim received the B.Sc. degree in Computer Science and Engineering from Mawlana Bhashani Science and Technology University (MBSTU), Tangail, Bangladesh in 2020. His research interests include Image Processing, Machine Learning, Internet of Things (IoT), Blockchain (BC), Industry 4.0 and Data Science.

Md. Jahidul Islam received the B.Sc. and M.Sc. degrees in Computer Science and Engineering from Jagannath University (Jnu), Dhaka, in 2015 and 2017 respectively. Currently, he is working as a Lecturer and Program Coordinator (Day) at Computer Science and Engineering (CSE), Green University of Bangladesh (GUB), Dhaka, Bangladesh since May 2017 to present. He is a member of Computing and Communication and Human-Computer Interaction (HCI) research groups, CSE, GUB. His research interests include Internet of Things (IoT), Blockchain, Network Function Virtualization (NFV), Software Defined Networking (SDN), 5G, Industry 4.0, Machine Learning, HCI, and Wireless Mesh Networking (WMN).

Dipanjali Kundu received the B.Sc. degree in Computer Science and Engineering from Chittagong University of Engineering and Technology (CUET), Bangladesh in 2018. Currently, she is working as a Lecturer at Computer Science and Engineering (CSE), National Institute of Textile Engineering and Research (NITER), Constituent Institute of the University of Dhaka, Savar, Dhaka, Bangladesh since January 2020 to present. Her research interests include Machine Learning, Human Computer Interaction, Internet of Things (IoT), Blockchain (BC), Software Defined Networking (SDN) 5G, Industry 4.0 and Robotics.

Ziaur Rahman is currently a PhD Candidate at RMIT University, Melbourne, and an associate professor (currently in study leave) of the Department of ICT, MBSTU, Bangladesh. He was graduated from Shenyang University of Chemical Technology, China, in 2012 and completed Masters from IUT, OIC, in 2015. His articles received the best paper award and nomination in different international conferences and published in reputed journals. Also, he is an IEEE and ACM Graduate Member, Australian Computer Society (ACS) Associate Member as well. His research includes Blockchain, Industrial Internet of Things (IIoT), Cybersecurity, and Software Engineering.

Shahab S. Band received the M.Sc. degree in artificial intelligence from Iran, and the Ph.D. degree in computer science from the University of Malaya (UM), Malaysia, in 2014. He was an Adjunct Assistant Professor with the Department of Computer Science, Iran University of Science and Technology. He also severed as a Senior Lecturer with UM, Malaysia, and with Islamic Azad University, Iran. He participated in many research programs within the Center of Big Data Analysis, IUST and IAU. He has been associated with young researchers and elite club, since 2009. He supervised or co-supervised undergraduate and postgraduate students (master's and Ph.D.) by research and training. He has also authored, or coauthored papers published in IF journals and attended to high-rank A and B conferences. He is an Associate Editor, a Guest Editor, and a Reviewer of high-quality journals and conferences. He is a professional member of the ACM.