Research article

Future Smart Connected Communities to Fight COVID-19 Outbreak

Deepti Gupta [a,*], Smriti Bhatt [b], Maanak Gupta [c], Ali Saman Tosun [a]

[a] Department of Computer Science, University of Texas at San Antonio, One UTSA Circle, San Antonio, TX 78249, USA
[b] Department of Computing and Cyber Security, Texas A&M University-San Antonio, One University Way, San Antonio, TX 78224, USA
[c] Department of Computer Science, Tennessee Tech University, 1 William L Jones Drive, Cookeville, TN 38505, USA

ARTICLE INFO

ABSTRACT

Internet of Things (IoT) has grown rapidly in the last decade and continues to develop in terms of dimension and complexity, offering a wide range of devices to support a diverse set of applications. With ubiquitous Internet, connected sensors and actuators, networking and communication technology along with artificial intelligence (AI), smart cyber-physical systems (CPS) provide services rendering assistance and convenience to humans in their daily lives. However, the recent outbreak of COVID-19 (also known as coronavirus) pandemic has exposed and highlighted the limitations of contemporary technological deployments especially to contain the widespread of this disease. IoT and smart connected technologies together with data-driven applications can play a crucial role not only in the prevention, mitigation, or continuous remote monitoring of patients, but also enable prompt enforcement of guidelines, rules, and administrative orders to contain such future outbreaks.

In this paper, we envision an IoT and data-supported connected ecosystem designed for intelligent monitoring, pro-active prevention and control, and mitigation of COVID-19 and similar epidemics. We propose a gamut of synergistic applications and technology systems for various smart infrastructures including E-Health, smart home, supply chain management, transportation, and city, which will work in convergence to develop 'pandemic-proof' future smart communities. We also present a generalized cloud-enabled IoT implementation framework along with scientific solutions, which can be adapted and extended to deploy smart connected ecosystem scenarios using widely used Amazon Web Services (AWS) cloud infrastructures. In addition, we also implement an E-Health RPM use case scenario to demonstrate the need and practicality for smart connected communities. Finally, we highlight challenges and research directions that need thoughtful consideration and across the board cooperation among stakeholders to build resilient communities against future pandemics.

* Corresponding author.
 E-mail addresses: deepti.mrt@gmail.com (D. Gupta), sbhatt@tamusa.edu (S. Bhatt), mgupta@tntech.edu (M. Gupta), ali.tosun@utsa.edu (A.S. Tosun).

1. Introduction and Motivation

COVID-19 is an infectious disease caused by a newly discovered coronavirus (SARS-CoV-2) and is rapidly spreading around the world. According to the World Health Organization (WHO), COVID-19 has already affected 215[1] countries and territories around the world and continues to spread rapidly across other regions. The highly contagious coronavirus outbreak was declared a "pandemic" on March 11, 2020. WHO reports[2] that the number of positive cases has dramatically surged, with nearly 34.5 Million reported cases and 1.03 Million fatalities as of October 01, 2020. In order to control the spread of the pandemic, lockdowns, quarantines, and stay home orders have been issued by several nations across the globe, which has crippled national and world economy with critical consequences to workers, employers, and investors. In addition, the industries, businesses, and travel restrictions restrain the supply of goods and services, and the economic disruptions will continue to have a long-term impact on global supply chains and economy. In the United States, unemployment rates[3] spiked to 14.7% in April 2020 - its highest level since the Great Depression, in addition to fear of a stronger second wave of the disease looming during the fall season.

Currently, with no cure or vaccine for this disease, the first line of defense to fight against this pandemic is a combination of preventative measures and mitigation strategies. As suggested by the WHO, the U.S Centers for Disease Control and Prevention (CDC[4]) and several other federal organizations suggest social distancing, environmental surface cleaning, self-isolation, travel restrictions, local and national lockdowns, quarantine, limits on large gatherings, restrictions on opening businesses, and school closures, as some of the preventive measures that are needed to limit the spread of the disease. However, these guidelines impose restrictions which hinder the way of *normal* life for humans. It has become a big challenge to swiftly implement and enforce such measures on a large scale across cities, nations, and around the world. We believe that to effectively enforce and monitor the preventive controls and mitigation strategies for COVID-19, IoT together with its key enabling computing technologies including cloud, AI and data-driven applications can play a pivotal role.

There are several existing examples of the use of technology to control the spread of COVID-19. Solutions have been proposed to manage large gatherings of individuals to limit the infected cases. The U.S. CDC has introduced a self-checker[5] application enabled with cloud platform, which helps a patient to make decisions to find appropriate healthcare services through questionnaires. However, most people do not have any symptoms who are known as the silent spreaders/asymptomatic carriers. Therefore, conducting large scale testing for everyone is paramount to slow the spread. The US is conducting nearly 1 Million[6] tests every day (as of Oct 01, 2020) to early determine and isolate patients which also helps in treatment. Taiwan[7] leveraged database from national health insurance and integrated it with its immigration and customs database to begin the creation of big data for analytic, and generated real-time alerts during a clinical visit based on travel history and clinical symptoms to aid case identification.

In April, New York City[8] reported 13% positive cases of COVID-19. The fatality rate of this city is 11% as of May 10, and 0.5% of fatalities have been in nursing homes. Nursing homes are the most vulnerable spot in terms of health risks. Technology can assist in enforcing the prevention measures and mitigation strategies in nursing homes to flatten the curve of fatality rate. Some states Iowa, Minnesota, Tennessee, and Texas have partially reopened, and models[9] have predicted that the number of cases and fatalities will increase as the country moves towards reopening businesses and cities. These pieces of evidence show that communities are not prepared to reopen, operate, and handle such pandemics. There are several requirements to assist in tracking and monitoring COVID-19 patients, such as to enforce wearing masks in public area, proper sanitizing, social distancing, mass quarantine for mild-symptoms people, and testing at a large scale. According to Harvard Global Health Institute[10], 31 states in the United States have insufficient testing levels, and 10 states would need at least 10,000 more tests a day to begin a gradual reopening. For instance, in April 2020, New York, the state with the largest number of cases, needed to increase testing by more than 10,000 per day. Due to a lack of enough testing kits, an antibody test online is offered for those people who recently got sick and think that they might have COVID-19.

In today's world, not having network capability in a device limits the market potential for that device. As a result, there are a large number and various types of network connected IoT devices providing convenience and ease of life to humans. With new technological advancements, this trend is expected to continue and grow in the future. IoT market[11] is currently valued at $267 billion per year and is expected to reach $520 billion by 2021. Another recent article[12] predicted more than 100 billion devices to be internet-connected by 2025.

---

1 https://www.who.int/emergencies/diseases/novel-coronavirus-2019
2 https://coronavirus.jhu.edu/map.html
3 https://www.usnews.com/news/economy/articles/2020-05-08/second-wave-of-coronavirus-joblessness-prompts-comparisons-to-great-depression
4 https://www.cdc.gov/coronavirus/2019-ncov/index.html
5 https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/testing.html
6 https://coronavirus.jhu.edu/testing/individual-states
7 https://jamanetwork.com/journals/jama/article-abstract/2762689
8 https://www1.nyc.gov/site/doh/covid/covid-19-data.page
9 https://www.nytimes.com/2020/05/04/us/coronavirus-live-updates.html
10 https://globalepidemics.org/2020/04/27/states-that-fall-short-on-testing/
11 https://www.forbes.com/sites/louiscolumbus/2018/08/16/iot-market-predicted-to-double-by-2021-reaching-520b/#82674f91f948
12 https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf
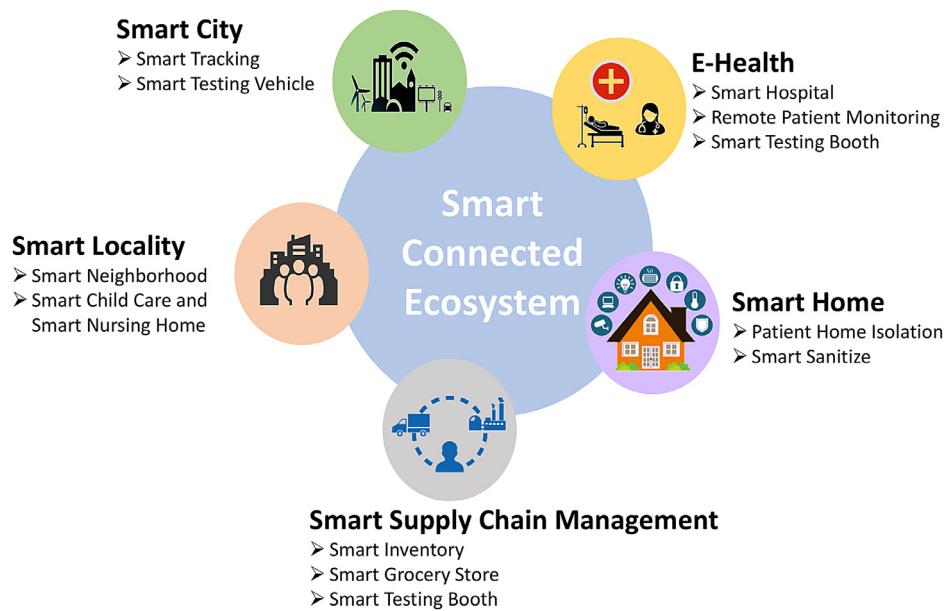
Fig. 1. An overview of converging smart connected ecosystem.

IoT comprises a large number of novel consumer devices including HDMI sticks, IP cameras, smartwatches, connected light bulbs, smart thermostats, health and fitness trackers, smart locks, connected sprinkler systems, garage connectivity kits, window and door sensors, smart light switch, home security systems, smart ovens, smart baby monitors, and blood pressure monitors. However, mostly these IoT devices are used in a distributed manner based on users' requirements. IoT including smart sensors, actuators, and devices and data-driven applications can enable future smart connected communities to strengthen the health and economical postures of the nations to fight against the current COVID-19 situation and other future pandemics efficiently. These smart devices have the potential to be a major breakthrough in efforts to control and fight against the current pandemic situation. IoT is an emerging field of research, along with the ubiquitous availability of smart technologies, as well as increased risks of infectious disease spread through the globalization and interconnection of the world necessitates its use for predicting, monitoring, and tracking to prevent from COVID-19.

In this paper, we present a holistic vision of IoT-enabled smart communities utilizing various IoT devices, applications, and relevant technologies (e.g., AI, Machine Learning (ML), Blockchain, etc.). Fig. 1 shows an overview of the smart connected ecosystem with real-world scenarios in diverse application domains focusing on detection, prevention, and mitigation of COVID-19 and similar outbreaks. The major contributions of this paper are as follows.

- We present an extensive review of IoT along with emerging technologies currently used (and proposed) to control the pandemic crisis, and enlists the focus, contributions, and weaknesses of relevant research works. We outline some of the COVID-19 symptoms, preventive measures, mitigation strategies, and current problems and challenges to understand the needs of proposed connected ecosystem.
- We present an overview of adaptable multi-layered IoT architecture supporting edge, virtual objects, and cloud layer, and reflect interactions between them to focus on data-driven and connected smart applications catering to limit the COVID-19 outbreak.
- We design a smart connected ecosystem by developing multiple synergistic IoT application frameworks including E-Health, Smart Home, Supply Chain Management, Transportation, and Smart City. We introduce the convergence of these domains and offer novel use cases and application scenarios for early COVID-19 detection, prevention, and mitigation.
- We present a general implementation framework that can be used for adapted and extended to enable smart communities use case scenarios utilizing a real-world cloud-enabled IoT platform, Amazon Web Services (AWS). We also design specific algorithms which can be used in different scenarios as required. In addition, we also implement a Remote Patient Monitoring (RPM) use case within the E-Health domain very relevant to COVID-19 patients in home isolation and enforcing quarantine.
- Lastly, we identify and highlight current challenges and interdisciplinary research directions, including security and privacy, performance efficiency, interoperability and IoT federation, implementation challenges, policy and guidelines, ML and big data analytics, to enable and empower future smart connected communities.

The remainder of this paper is organized as follows. Section 2 presents the literature review on role of computing and data-driven technologies with IoT to control COVID-19. Section 3 discusses the essential characteristics to diagnose, prevent, and mitigate COVID-19 disease. Section 4 presents a multi-layered architecture for IoT enabled future smart and resilient

communities, whereas Section 5 discusses convergence of connected ecosystem scenarios in various IoT application domains. Section 6 discusses a general implementation framework of smart connected communities using a real-world cloud-enabled IoT platform and deploys a proof of concept test bed for Remote Patient Monitoring (RPM) use case. Section 7 highlights open research challenges and future directions, followed by conclusion in Section 8.

2. Related Work and Relevant Background Study

Extending the use of IoT along with emerging technologies can play a significant role in dealing with COVID-19. This work justifies that IoT has influenced healthcare and other areas of our lives significantly. In current situation, hospital practitioners are working hard to help infected patients, and we are living a new normal with new rules, such as state leaders' mandate rules to maintain six feet distance and wear masks in public places. Broaden use of IoT technology enables us to deal with COVID-19 or any future pandemic situation. For instance, the Chinese government[13] installed CCTV cameras at home or apartment door of those under a quarantine period to monitor the patient activity. Human activities also measured through a linear model [1] based on the state-space method. Drones are used to notify people to wear their masks, and digital barcodes on mobile apps highlight the health status of individuals. Researchers at the University of Michigan together with the team at Voxel51[14] have presented the Physical Distancing Index (PDI) to help track how COVID-19 news or events impact human activity around the globe in real-time. The free AI-powered interactive tool enables users to explore a day-by-day timeline of social activity in some of the world's most populated areas to track social distancing. Currently, Voxel51 gathers and analyzes historical and real-time video streams from public street cameras in Ann Arbor, Detroit, Times Square; Abbey Road in London; Fremont Street in downtown Las Vegas; Seaside Heights in New Jersey; a beach in Ft. Lauderdale; and intersections in Dublin and Prague.

Table 1 summarizes prior research along with their challenges and contributions to prevent and mitigate COVID-19 using specific technologies, such as IoT, ML, and Blockchain. In existing literature [2–15], various IoT-based solutions along with other technologies are proposed for smart healthcare. Various frameworks and systems are discussed in the context of healthcare for handling COVID-19. Here, critical analysis of current IoT based research shows that most of them are focused on a single use case; however, we need a holistic smart ecosystem comprising multiple entities and different stakeholders to handle current or similar future pandemic situations. Therefore, we present future smart connected communities to fight COVID-19 and appropriately handle future pandemic situations.

3. Essential Characteristics to Diagnose, Prevent and Mitigate COVID-19

Coronavirus transmits mainly by the infected person's saliva and nasal drips which spread during coughing and sneezing around anybody in close contact. Another source of infection is contaminated surfaces in surrounding and high-risk areas, such as door handles, railings, elevators, and public restrooms. COVID-19 is a highly contagious virus with an incubation period stretched from 2 days to 2 weeks after exposure. Symptoms of COVID-19 range from mild symptoms including fever, coughing and shortness of breath to severe symptoms including organ failure, such as kidney failure, and pneumonia. Researchers are still studying the virus to fully understand the characteristics and new symptoms of this disease. Recently, the U.S. CDC[15] added six new possible symptoms including chills, muscle pain, headache, sore throat, and loss of taste or smell. New York City[16] reported 73 cases of children with rare coronavirus inflammatory illness on May 7, 2020.

At this time, any specific treatment is not recommended for disease caused by the novel coronavirus, and no vaccine is currently available in the market. The treatment is subjective and depends on a case-by-case basis, where oxygen therapy shows positive effects as the treatment intervention for patients with severe infection. Mechanical ventilation may be necessary in cases of respiratory failure refractory to oxygen therapy. The U.S. CDC[17] and other resources explained early signs and symptoms, some preventive measures, and mitigation strategies. On March 19, 2020, the WHO[18] released the first edition of interim guidance on Infection Prevention and Control (IPC) strategies for identifying the coronavirus infection.

On March 28, 2020, the U.S. Food and Drug Administration (FDA[19]) provided emergency use authorization for hydroxychloroquine medicine to treat the people who are suffering from this virus in hospitals. Later, on April 24, 2020, FDA[20] warned against the use of hydroxychloroquine to treat this disease outside of the hospital setting or a clinical trial due to risk of heart rhythm problems. People can protect themselves by following some protective measures and help to slow the spread using mitigation strategies. Table 2 provides a comprehensive overview of the symptoms, preventive measures, mitigation strategies, and some challenges fighting COVID-19 disease.

---

[13] https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html

[14] https://pdi.voxel51.com/

[15] https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html

[16] https://www.nbcnewyork.com/news/local/73-ny-children-sick-with-rare-covid-related-illness-state-finds-with-one-death/2408285/

[17] https://www.cdc.gov/coronavirus/2019-nCoV/index.html

[18] https://www.who.int/publications-detail/infection-prevention-and-control-during-health-care-when-novel-coronavirus-(ncov) -infection-is-suspected-20200125

[19] https://www.fda.gov/media/136537/download

[20] https://www.fda.gov/drugs/drug-safety-and-availability/fda-cautions-against-use-hydroxychloroquine-or-chloroquine-COVID-19-outside-hospital-setting-or

Table 1

Current projects and research on IoT based solutions to mitigate COVID-19.

Paper Title	Focus/Objective	Contribution	Limitations
Chinese experts' consensus on the Internet of Things-aided diagnosis and treatment of coronavirus disease 2019 (COVID-19) [2]	Enables different levels of COVID-19 diagnosis and treatment among different doctors from different hospitals through the intelligent assistance of the nCapp system.	• Develops COVID-19 Intelligent Diagnosis and Treatment Assistant Program (nCapp) based on the Internet of Things. • Designs 15 easy-to-use questionnaires for intelligent processing.	• The data is based on questionnaires and is filled manually. • Security and privacy issues related to patient's personal data have not been discussed.
Artificial Intelligence (AI) applications for COVID-19 pandemic [3]	The role of AI as a decisive technology to analyze and prepare us for prevention and fight with COVID-19	• Identifies seven significant AI assisted applications for fight with COVID-19. Detects the cluster of positive cases and predicts where this virus will affect in future by collecting and analyzing all previous data.	• Tools are missing to implement each application. The answer of "How will author extract the data?" is missing. • The flow of each application has not been explained.
Industry 4.0 technologies and their applications in fighting COVID-19 pandemic [4]	Explores several useful technologies of Industry 4.0 to control and manage of COVID-19 pandemic.	• Presents ten technologies- Artificial intelligence, Big data, Internet of Things, Virtual reality, Holography, Cloud computing, Autonomous robot, 3D Scanning, 3D Printing and Biosensor.	• Only medical concern has been discussed here, transportation and other topics related to industry have not been discussed.
Role of IoT to avoid spreading of COVID-19 [5]	Presents available literature on COVID-19 regarding monitoring techniques, and suggests an IoT based architecture, which can be used to minimize the spreading of COVID-19.	• Presents IoT architecture to avoid COVID-19, the use of IoT with smart sensors to measure and record the body temperature of individuals, which can help to identify infected individuals.	• The number of sensors to develop particular application are limited. • Only one application is used for per scenario, complete framework is missing. • The upcoming challenges to build these applications have not been discussed here.
Data science and the role of Artificial Intelligence in achieving the fast diagnosis of Covid-19 [6]	Due to less number of COVID-19 test kits, presents image classification approach on chest X-ray to predict COVID-19 test result.	• Elaborates a methodology that helps identify COVID-19 infected people among the individuals by utilizing CT scan and chest X-ray images using AI. • Experiment on a dataset of COVID-19 and normal chest X-ray images. • Calculates accuracy of an image using decision tree classifier.	• False positive rate can be high in allergy case. • The data is not categorized by age. • No discussion on security and privacy challenges to collect and store the patients' health data.
An IoT-based Framework for Early Identification and Monitoring of COVID-19 Cases [7]	Identification of potential cases of COVID-19.	• Presents a novel IoT framework, which consists of five major components. • Uses eight classification algorithms on a real COVID-19 symptom dataset using IoT framework to identify COVID-19 cases.	• The generated data can be bias, if number of COVID-19 cases are less than other type of diseases then the model can send false alarm.
Internet of Things and Blockchain-based framework for Coronavirus (Covid-19) Disease [14].	Aims to assist infected people online using the Internet of Things (IoT) and Blockchain technologies through smart devices.	• Presents four-layer architecture: hardware layer, shared ladger layer, communication layer, Application layer. • Develops IoT and Blockchain-based framework for healthcare.	• Raise security concerns with shared ladger layer to store health records of patient. • Challenges to build the framework have not been explained.
A drone-based networked system and methods for combating coronavirus disease (COVID-19) pandemic [8]	Investigates drone-based systems, which are used to handle pandemic situations in real-world scenarios.	• Presents an artificial intelligence-based system that collects data through drones. • Develops a multi-layered architecture that collects information from drones. • Implements a real-time drone-based system for sanitization, monitoring, and other applications.	• No user's data privacy solutions. • Limited scope on data security.
Applications of machine learning and artificial intelligence for Covid-19 (SARS-CoV-2) pandemic: A review [9]	Presents review of AI and ML as one significant method in the arena of screening, predicting, forecasting, contact tracing, and drug development for SARS-CoV-2 and its related epidemic.	• Discusses recent studies that apply ML and AI technologies towards augmenting current research works from multiple angles. • This study also addresses a few errors and challenges while using such algorithms in real-world problems.	• AI and ML based algorithms have not been discussed. • A complete framework is not shown, which can bring all small applications together.

Table 1 (*continued*)

Paper Title	Focus/Objective	Contribution	Limitations
Internet of things (IoT) applications to fight against COVID-19 pandemic [10]	Enables Internet of Things (IoT) based healthcare system, which helps to increase patient satisfaction and reduces re-admission rate in the hospital.	• IoT provides an extensive integrated network for healthcare providers to fight with COVID-19 pandemic. • Presents twelve major applications of IoT for COVID-19 pandemic.	• Any healthcare related IoT device has not been presented. • A novel implementation of any application has not been described. • Challenges to design these twelve applications are also missing in this paper.
Application of cognitive Internet of Medical Things for COVID-19 pandemic [11]	Cognitive Internet of Medical Things (CIoMT) is best suited to handle COVID-19.	• Presents the CIoMT platform, which enables real-time tracking, remote health monitoring and other applications to reduce the workload on the medical industry. • Identifies some challenges and future research directions.	• No implementation details of any application is discussed. • The details of other major challenges like interoperability, data biasing are missing.
Restructured society and environment: A review on potential technological strategies to control the COVID-19 pandemic [12]	Investigates various implemented technologies that assists the healthcare systems, government and public in diverse aspects for fighting against COVID-19.	• Presents prospective viable technologies that can be used in the current or future epidemic situation. • Discusses the technological changes that the environment and the society have undergone in tackling COVID-19.	• Limited technological solutions for COVID-19 risk. • Based on the survey, any novel idea is not presented.
Emerging Technologies for Use in the Study, Diagnosis, and Treatment of Patients with COVID-19 [13].	Focuses on analyzing possible opportunities and challenges of integrating emerging technologies into COVID-19 contact tracing.	• Designs the contact tracing application using emerging technologies to mitigate the coronavirus. • Observes various challenges like the security and privacy of people while using contact tracing application.	• It is not clear how effective the current contact tracing application would be using emerging technologies. • Lack of implementation details.
Role of biological Data Mining and Machine Learning Techniques in Detecting and Diagnosing the Novel Coronavirus (COVID-19): A Systematic Review [15]	Aims to address the limitations of utilizing data mining and ML algorithms to mitigate this virus, and provides health sector with the benefits of techniques.	• Reviews eight articles, which show data mining and ML based applications. • Analyzes several database, and performs various AI algorithms for detection, and classification of adaptive CoV.	• Analyzes only MERS, SARS disease datasets (2013-2016).

One of the easiest preventive measures is to wash your hands frequently and thoroughly with soap and water for at least 20 seconds or use hand sanitizer or an alcohol-based hand rub when soap and water are not available. People should keep social distancing (six feet distance) from others especially from people who are coughing or sneezing. It is suggested to wear mask and gloves in a public setting, and avoid touching the face and surfaces such as the button at a traffic light, a keypad to add a tip for the restaurant take-out order, elevator buttons, etc. Many surfaces are touched by hands accidentally and virus can be potentially picked up and then transmitted to other surfaces and locations. Once the hands are contaminated, the virus can be transferred through eyes, nose, or mouth, thus, it enters the human body. Respiratory Hygiene/Cough Etiquette is a term used to describe infection prevention measures to decrease the transmission of virus. There is a need to avoid cough or sneeze into the hands, and to cover mouth and nose with a tissue and throw away the tissue immediately. Groceries and packets can be contaminated from coronavirus, and it is recommended to wash grocery items carefully and wipe packets using a disinfectant spray. Local public health administrations regularly issue health guidelines, which people should follow.

The WHO, governments, and healthcare workers are all urging people to stay home if they can. On top of basic illness prevention, experts said that the best (and only real) defense against disease is a strong immune system. In addition to physical health, taking care of mental health is also necessary. High stress levels can take a toll on human's immune system, which is the opposite of what people want in this situation. In addition, mitigation strategies are a set of actions applied by the people and communities (hospitals, grocery stores, and cities) to help slow the spread of respiratory virus infections. These actions can be scaled up or down depending on the evolving local situation. At an individual level, if a person is infected with coronavirus, then he/she should self-isolate and follow the guidelines of quarantine provided by the hospital. The hospitals must support healthcare workforce, increase testing and intensive care capacity, and availability of Personal Protective Equipment (PPE). City governments can appoint task forces, open shelters for homeless people, and maintain availability of resources to implement preventive and mitigation strategies for this disease. While each community is unique, appropriate mitigation strategies vary based on the level of community transmission, characteristics of the community and their populations, and the local capacity to implement strategies. Nonetheless, it is crucial to understand the characteristics of this novel virus, spread awareness and up-to-date information across communities through appropriate technologies. Consequently, it is essential to address the challenges with significant research and implementation of strategies as shown in Table 2.

Table 2

COVID-19 Symptoms[21], Prevention[22], Mitigation and Challenges. (Items within the same row are unrelated)

Early Symptoms	Preventive Measures	Mitigation Strategies	Problems and Challenges
Common symptoms include fever, dry cough and myalgia or fatigue.	Clean hands often for at least 20 seconds with soap and water or use of alcohol-based hand sanitizer.	If sick stay in a single room for 14 days, avoid sharing personal household items.	Coping with anxiety disorder, depression issues, and mental health problems.
Shortness of breath or cannot breathe deeply enough to fill your lungs with air, chills.	Avoid face-to-face meetings, practice social distance from other people outside of the home.	Monitor symptoms regularly, wear a cloth covering or N-95 mask over nose and mouth.	Knowledge gaps to understand virus transmission, no specific antiviral treatment, and no vaccine available.
Loss of the sense of smell is most likely to occur by the third day of infection and some patients also have experience a loss of the sense of taste.	Cover mouth and nose with a cloth or wear mask when around others, wear gloves and discard them properly.	Manufacturers use of all cleaning and disinfection products, follow the workplace protocol[23] and provide PPE to their employee.	Lack of testing and essential resources such as ventilators, masks, beds, and health staffs, cancel elective surgery.
Diarrhea and nausea a few days prior to fever, sudden confusion or an inability to wake up and be alert may be a serious sign.	Cover your mouth and nose with a tissue when you cough or sneeze; Throw used tissues in the trash.	Hospital task force such as increase the number of testing, available the PPE for their staff members, and increase the incentive care.	Privacy issues: contact tracing, health data/medical records, virtual meeting, remote workforce.
A small number of patients can have headache or hemoptysis and even relatively asymptomatic.	Maintain proper hygiene, clean and disinfect frequently touched surfaces, and wash grocery items properly.	City/state government task force such as limited to 25% capacity at retail/restaurants, close the playground, and restrict or limit visitor access to nursing homes.	Reopening the country phases in highly contagious environment without data analytic, unified decision-making frameworks and some policies that span the country.
Pneumonia, kidney failure and dyspnea more frequent in most severe cases.	Follow travel restrictions (domestic flights only for essential services, No sail order)	Individuals limit community movement and adapt to disruptions in routine activities (school and/or work closures) according to guidance from local officials.	Due to novelty of the virus, projection of the model is unpredictable to identify number of positive cases and fatalities, and evolving symptoms such as COVID toes and rashes.
Normal or low white blood cell count or reduced lymphocyte in early onset.	Update periodically to follow WHO, and country guidelines.	Use existing technologies to mitigate the risk of virus.	No strict and defined guidelines from agencies due to ever changing dynamics of the virus.

4. Multi-layered Smart Communities Architecture

In this section, we explain an integrated multi-layer IoT architecture which can fundamentally change the infrastructure and underlying technologies for smart communities including hospital, grocery retail store, transportation, and city, etc. as shown in Fig. 2. Our proposed architecture extends and adapts existing IoT and CPS architectures [16–22], and focuses on the need for swift enforcement of policies, laws, and public guidelines, in order to curtail the widespread of such disease. The architecture integrates a hybrid cloud and edge computing nodes together with IoT and smart sensor devices, to enable real-time and data-driven services and applications needed in COVID-19 pandemic. Overall, the architecture consists of six layers: Object layer, Edge layer, Virtual Object layer, Cloud layer, Network Communication, and Application layer. The object layer is a rich set of IoT devices including sensors, actuators, embedded devices, roadside infrastructures, vehicles, etc. These physical objects are spread across and implemented in smart communities, such as hospitals, retail stores, homes, parking lots. The edge layer provides local real-time computation and analysis needed for smart resource-constrained physical objects. This layer incorporates edge gateways and cloudlets [23] which can enable local computation at this layer overcoming limited bandwidth and latency requirements, and also impacts the usability of the IoT applications.

This multi-layer architecture has integrated the concept of Virtual Objects (VOs) [24], which are the digital delineation of physical IoT devices. VOs show the current state of corresponding physical objects in the digital space when they are connected, and can also store a future state for these devices when they are offline. The cloud layer provides various services like remote storage, computation, big data analysis, and data-driven AI applications, etc. for a huge amount of information generated by billions of IoT devices connected to the cloud. We define a computation layer which comprises of edge layer, virtual object layer, and cloud layer. Computation, data analytic and processing services are performed in this layer. Network communication layer runs among different layers to establish the interaction. It is responsible for connecting physical sensors, smart devices, edge compute nodes or cloudlets, and cloud services with different technologies, and is also used for transmitting and processing sensor data. Application layer delivers specific services to end users through different IoT applications. Task scheduling algorithms [25] can be applied on this layer to manage the resources in order to deliver the
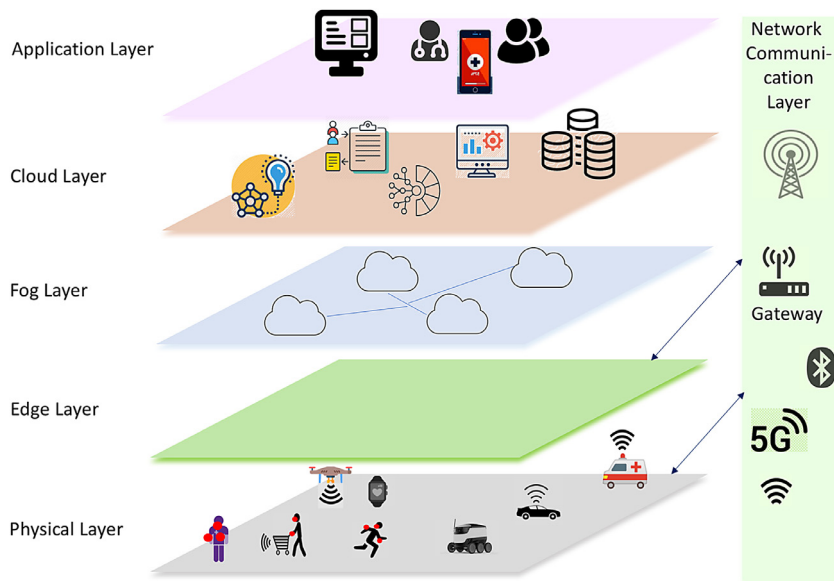
Fig. 2. Adaptable multi-layered smart communities architecture.

optimal Quality of Services (QoS). In the multi-layered smart communities' architecture, this application integrates mobile phones, edge computing, cloud computing, AI-based analytic, and data-driven services.

This architecture can incorporate the IoT application frameworks within different domains as discussed in Section 5, and different use case scenarios can be mapped and implemented using relevant technologies associated with each layer of the architecture.

5. Future Smart Connected Ecosystem and Technological Solutions

We propose IoT use case scenarios by deploying novel smart devices, data-driven applications and technologies to present a holistic view of IoT-enabled smart architectures for fighting COVID-19 outbreaks. We have divided our scenarios into five broader categories: E-Health, Smart Home, Smart Supply Chain, Smart Locality and Smart City, as described in the following subsections.

5.1. E-Health

It is expected that the global Internet of Medical Things (IoMT) market[24] will grow to 136.8 billion in year 2022. As of 2020, 3.7 million medical devices are in use today, which are used to monitoring patients' conditions and sending data to hospital practitioners in real-time. E-Health helps to mitigate fast-spreading COVID-19 that has taken over the entire healthcare ecosystem including hospitals, testing booths, vaccine developing labs, pharmaceutical companies, and health insurers. Data-driven applications such as ML for drug discovery, RPM, predictive analytic for hospital resource optimization, and interactive medicine deliver the right information at the right time in the healthcare system. Improving the efficiency of healthcare services and keeping healthcare costs under control have been important and critical challenges during the COVID-19 pandemic time. To overcome these limitations, we discuss three important application scenarios: smart hospital, RPM, and smart testing booth, which are shown in Fig. 3.

5.1.1. Smart Hospital

Today, smart hospitals are still facing several challenges including shortages of materials such as PPE and items that support a patient room, more specifically ventilator, thermometers, disinfectants, cleaning supplies, including hospital practitioners' shortage in responding to the COVID-19 pandemic. To overcome these problems, we propose a smart hospital use case scenario which employs IoT technology to extend existing infrastructure to enable coordinated actions for coronavirus patients. Various components of smart hospital concept have also been studied in the literature [26–29]. Within a smart hospital, RFID sensors can be an ideal way to keep track of PPE, cleaning supplies, medical supplies, smart beds, ventilators,
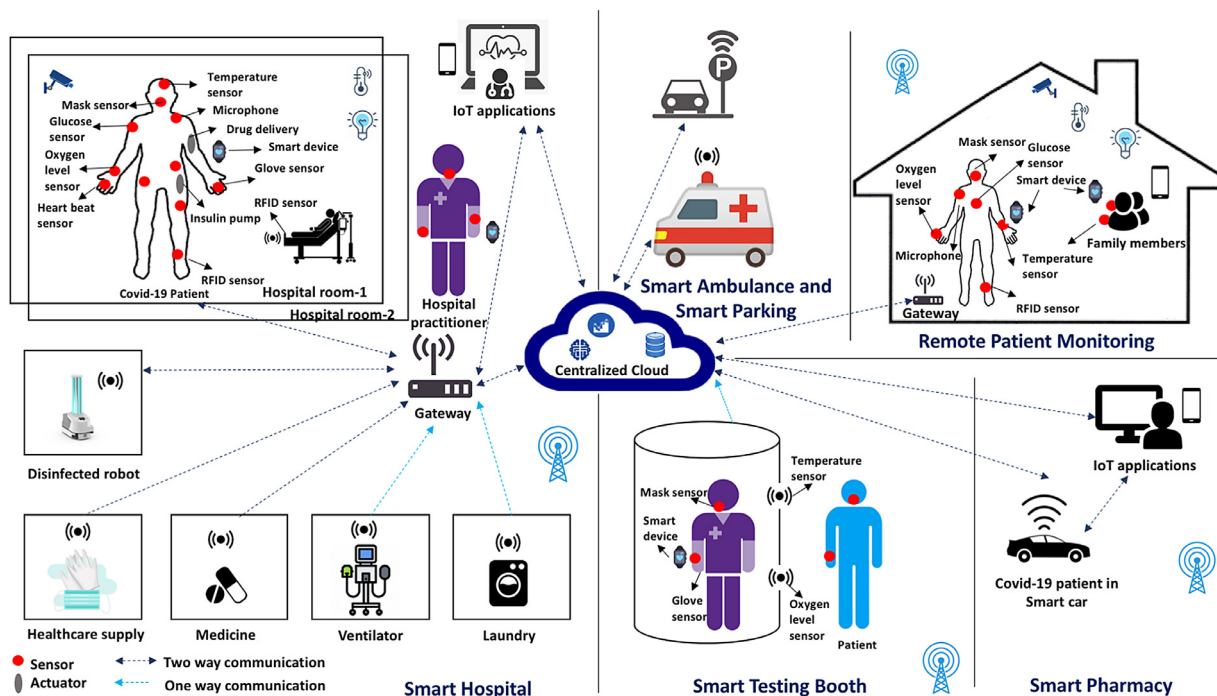

Fig. 3. Conceptual overview of connected smart e-health ecosystem.

and patients. While RFID sensor is used to track the location of materials and patients within the hospital, other IoT sensors along with technologies including AI, big data analytics, and Blockchain can provide multiple benefits to patients and facilities.

More specifically, hospital practitioners, staff members, and patients can wear smart bracelets (e.g., iHealth smartwatch) or smart rings (e.g., oura ring) to capture early symptoms of COVID-19 by collecting their data including body temperature, heart rate, and blood oxygen levels and store at edge data centers, which avoids latency and security issues. This data can be used for training purposes to build models using Deep Learning (DL) or federated learning as presented in Algorithm 1 (as discussed in Section 6). These models will increase the intelligence of data-assisted applications that can be used to predict early symptoms of coronavirus infection for hospital practitioners and staff members. Using IoT sensors and wearable devices, hospital practitioners can not only collect useful data with minimal in-person contact but can also reduce the risk of cross-infection from the patients. Typically, due to limited storage on the edge, data can be sent to a centralized cloud through secure data sharing tunnel. This tunnel is an encrypted link between edge device or gateway and centralized cloud. The searchable encryption scheme [30] can be replaced with simple adoption of an encryption scheme to enhance the privacy of IoMT data and also supports multi-clients.

The connected devices can communicate and operate autonomously. For example, smart ventilators can communicate through a patient's smart bracelets with embedded sensors and can respond according to the patient's body parameters. Health practitioners can also monitor patients and take decisions based on a combination of IoMT and Augmented-Reality (AR) technology. AR technology can provide additional benefits (e.g., breathing exercises) for patients. Autonomous robots can also help in healthcare systems as virtual clinic, smart guard, and provide food service. Similarly, smart cameras can be employed for continuous monitoring of patients including hospital inventory, hospital resources, peak hours, etc. An autonomous mobile UV-C (ultraviolet-C) or UVD disinfection robot can disinfect rooms and equipment with ultraviolet light and Hydrogen Peroxide Vapor (HPV) and will traverse in hospital using a random path planning algorithm to disinfect areas swiftly.

5.1.2. Remote Patient Monitoring (RPM)

RPM allows health practitioners to monitor COVID-19 patients remotely and provides care for recovering patients at home. Most popular companies, such as Gyant, Chronisense Medical, Ejenta, and iHealth, can enable RPM and provide a platform for physicians and hospitals to monitor patients outside of the hospital setting, where the technology can provide 24/7 data communication between patients and health practitioners. Patient-Generated Health Data (PGHD) including body temperature, SpO_2 percentage, BP level, pulse rate, coughing frequency, and ECG can be collected using wearable devices together with Internet-Enabled medical devices. This data will be sent to the web-server through Message Queuing Telemetry Transport (MQTT) protocol or Hypertext Transfer Protocol (HTTP) where it will be stored securely in patient's private cloud or a specific medical cloud. PGHD can be retrieved for analysis by hospital practitioners enabling early detection of COVID-

19 and identifying critical conditions of the patient using ML and DL algorithms. For example, if SpO_2 level of the patient is less than 85%, hospital practitioners will receive alerts through data-driven application and then send extra care services to the patient. Patients can also receive in-build corrective recommendations regarding medicines and extra precautions to be taken at home through IoT applications. He/she can also add his/her family members or friends to share his/her PGHD with different levels of access control due to security and privacy concerns. In general, due to privacy concerns, a patient might not agree to share his/her data, and in such cases, health devices will send data on a gateway device (e.g., patient's phone). The patient can also receive alerts based on threshold values through applications, especially when his/her health condition is critical. However, some alerts can be false positives, and to address such errors, dense sensor networks along with medical devices can help to reduce false positives. Furthermore, classification techniques such as Hidden Markov Model (HMM) [31] can be used to classify anomalies in PGHD. This model can be deployed on cloud or gateway to detect false alerts.

5.1.3. Smart Testing Booth

Boston hospital[25] developed an innovative coronavirus testing booth to keep healthcare workers safe while swabbing possibly infected patients and conserve PPEs. A smart testing booth can include multiple sensors like infrared large-scale body temperature sensor, no contact oxygen level sensors with Red, Green, and Blue (RGB) camera, RFID scanners and AI-assisted smart cameras. A single person at a time can enter one side of the glass-walled testing booth and will be identified through RFID tag based wearable device or optimized face recognition algorithm [32]. In-built sensors in the booth can record a person's body temperature and oxygen level including other PGHD which will be stored in medical cloud. An individual can receive the result of COVID-19 test through a phone application and also set an alert on his/her wearable device for test results.

Some other IoT applications and services in the context of E-Health are discussed here. Smart ambulance can provide virtual onboard assistants to help patients and find optimal paths [33], using ML services to the hospital, in case of emergency. The hospital smart parking system can scan license plate of driver to identify COVID-19 patient using the patient's data and can also assign a special spot to park his/her car. However, the patient's personal data can be stored on multiple storages to avoid centralization, which could lead to hacking, loss and mishandling of patient data due to centralization. Blockchain technology can be used to secure patient's personal data and can deliver decentralized attack detection model [34] to mitigate the single point of failure. In the above scenarios, data and information collected from smart devices are sent to edge gateways, services, or cloud. Due to high security and privacy concerns in the health domain, it is important to understand that these edge gateways and cloud-IoT platforms will be owned only by authorized entities, such as hospitals or other highly trusted entities through some private cloud. We elaborate on some of the challenges to enable these scenarios in Section 7.

5.2. Smart Home

Today, smart homes make our lives easier and provide convenience in our daily activities from automatically turning on thermostat from smartphone to opening the smart garage door remotely. However, we can also utilize smart devices to keep our homes healthy and sanitized. In real-world, it is nearly impossible to keep everything around you virus or germs free. However, individuals must employ precautionary measures to keep their homes clean and disinfected. In order to prevent the spread of COVID-19, the first step is to sanitize our homes. Currently, smart lights and temperature control with their compatible sensors have become ubiquitous in smart home environments enabled by Wireless Sensor Networks (WSN) [35]. According to global tech market advisory firm[26], voice control device based orders and shipments will grow globally by close to 30% over 2019. Using voice control allows people to avoid touching commonly touched surfaces around the home, such as smartphones, TV remotes, light switches, thermostats, door handles, and others. In this section, we elaborate on three different scenarios within the context of smart homes which can offer a more connected ecosystem to mitigate contagious disease spread, as shown in Fig. 4. Moreover, various aspects of smart home for health have been investigated in the literature [21,36–49].

5.2.1. Home Isolation

Some COVID-19 patients have high-risk enough to warrant quarantine but not serious enough to warrant smart hospital care. They should follow self-quarantine protocol and stay at their home; however, it will be a challenge to other family members to protect themselves in same home environment. In this scenario, it is expected that the patient should easily be monitored by hospital practitioners, family members, and local state authorities with different levels of authorization requirements. Patients' activities can be monitored through wearable and non-wearable devices at smart home. Non-wearable devices can be classified into three categories: vision-based devices (e.g., IR cameras, RGB cameras and depth cameras), medical devices (e.g., oximeter, scale, and thermometer), and dense sensing network-based devices (e.g., door sensor, light sensor, and motion sensor). The patient and family members can use wearable devices (e.g., smartwatch, smart mask, and microphone) to monitor their vitals regularly. Multiple sensors including mask sensor, temperature sensor, heart rate sensor, etc.

---

[25] https://whdh.com/news/boston-hospital-creates-coronavirus-testing-booth-designed-to-keep-healthcare-workers-safe-conserve-protective-equipment/
[26] https://www.techrepublic.com/article/COVID-19-pandemic-impact-pushing-smart-home-voice-control-devices-to-predicted-30-growth/
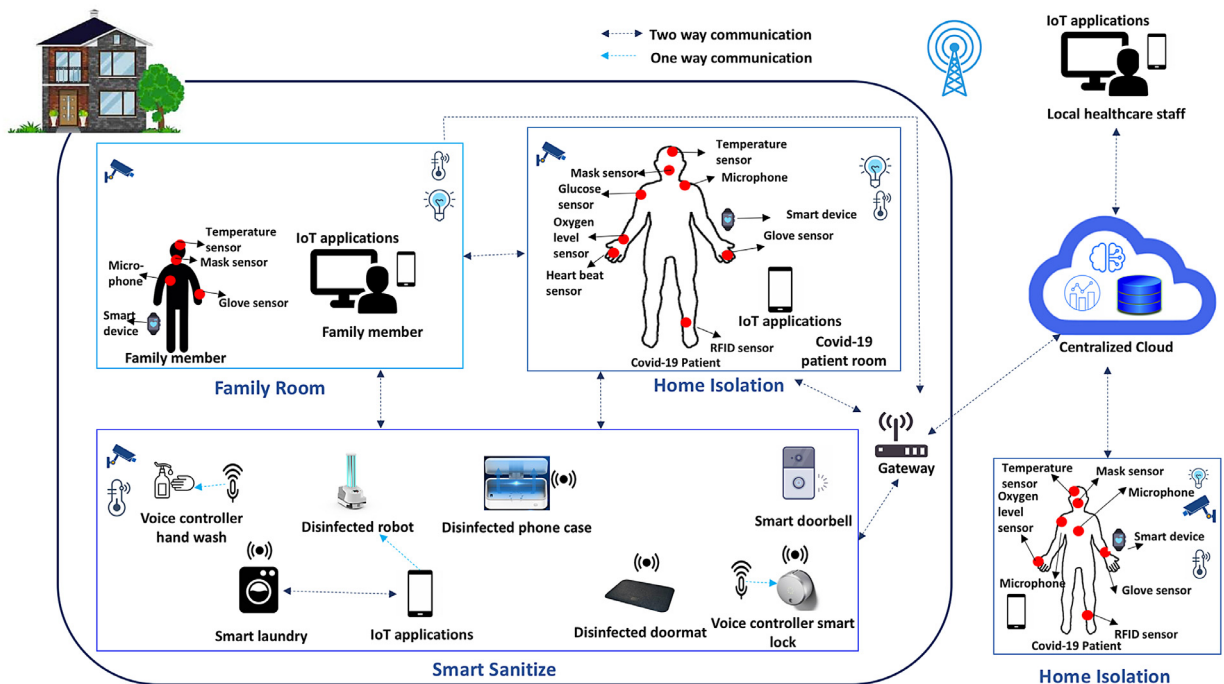
Fig. 4. Conceptual overview of connected smart home environment.

can be attached to patient's body, and other smart health devices and smart home IoT devices can also be installed in the patient room, as shown in Fig. 4. PGHD will be collected from these smart devices, which are Bluetooth Low Energy (BLE) or Wi-Fi based devices, and this data will also be shared with health practitioners for data analytics. PGHD will be monitored by health practitioners through their private cloud or manufacturer's cloud (e.g., iHealth's cloud, home automation cloud). To enable trust across multiple clouds, Blockchain technology can be used. Additionally, Secure Data Transmission Scheme (S-DTS) [50] can also support a distributed transmission among multiple clouds and can utilize four synchronization zones including IoT network zone, aggregation zone, mining zone, and management zone, and these zones can be operated by the Delegated Proof of Node (DPN) mechanism.

5.2.2. Smart Sanitize

Here, we present a smart sanitizing scenario which uses IoT technology. For instance, when a user will walk up to the home from the driveway and before he/she even reaches the front door, the door unlocks using optimize face recognition application [32] on the edge, then the user will walk inside the home. User's phone will connect with the home Wi-Fi network and will show the presence of the user at home. The smart home will set to the right temperature, and turn on smart home devices without touching any surface. The user can take off his shoes on smart UV-floor, and put his keys, phone in a smart UV lightbox that sanitizes these items. Hands-free automation including Gaggenau's handle-free refrigerators, faucets, doors, and closets can also be used at home to avoid spread of the virus. Voice-control devices such as Amazon echo, Honeywell Wi-Fi thermostat, hand sanitizer, and vocca light can be installed at home. Another futuristic technology that can be useful is air cleaning system that sanitizes clothing and footwear. This system can be installed in closets and laundry baskets. Similarly, smart vehicles can be sterilized with steam.

5.3. Smart Supply Chain Management

COVID-19 pandemic has created many gaps in the supply chain management, the emerging IoT technologies can be deployed to improvise this whole system. The use case scenarios including smart inventory and smart grocery store are discussed in this section and also shown in Fig. 5. These scenarios show how IoT devices and technologies can enable efficient supply-chain and also help in slowing the COVID-19 spread around us.

5.3.1. Smart Inventory

In past research, smart inventory systems have been investigated in the literature [51–57]. The studies show that mostly RFID tags have been used to identify the shortage of goods in smart inventory. Inventories are facing an unprecedented challenge in coping with the fallout from COVID-19. However, a smart inventory system can provide a safe and secure environment for the workers using technologies. Within the inventories, drones can be used to track all the employees to
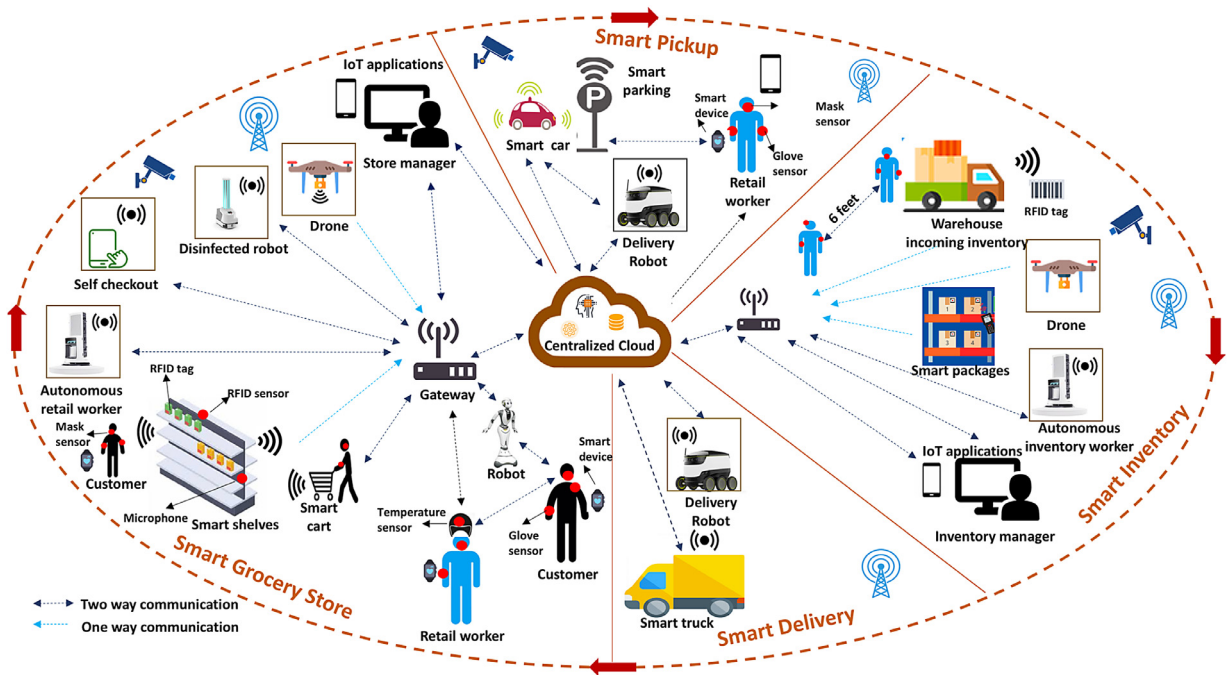
Fig. 5. Smart and connected supply chain management scenario.

check their temperature using thermal sensors, and also measure their social distancing using Algorithm 2 (as discussed in Section 6). Inventory manager can also provide UWB/LTE-based wearable devices that are less susceptible to interference than Bluetooth devices, and workers' health generated data will be stored on gateway server. If an employee is infected with coronavirus, then inventory manager can get notifications through data-driven IoT applications, given proper authorizations and privacy are enabled. In addition, disinfectant spray can be attached to the shelves that can start spraying when the associated sensor senses the sound of sneezing. An intelligent drone can monitor inventory in real-time and send alerts in case there is a shortage. Stereo Vision, Monocular Vision, Ultrasonic, Infrared, Time-of-Flight, and Lidar sensors are being used to detect and avoid obstacles. Sensor fusion can be used for obstacle detection, where data from different sensors are combined to compute useful information that could not be determined by just one sensor alone. Smart inventory will use RFID sensors and AI-assisted drone to track the items, and RFID antenna/AI camera will scan the number of units on the sales floor and will send an alert to a store manager in case of shortage. The generated data will allow to automate product orders and also identify the popularity of a certain item.

5.3.2. Smart Grocery Store

Smart grocery stores have been widely investigated in the literature [55,58–61]. IoT along with AI technologies can help slow the spread of infection by enforcing prevention and detection mechanisms through connected sensors in a smart grocery store. Chinese tech firm Kuang-Chi Technologies[27] has developed a smart helmet attached with thermal sensor, which is used to take body temperature at the retail store. Similarly, thermal cameras[28] and microphone sensors can also be installed at the store which can detect people who are coughing in store during shopping. The customer can wear an RFID tag or smart bracelet at the store, which can be provided by state government during COVID-19 testing. The customer can scan the tag/bracelet at the entrance of a grocery store, which will allow him/her to enter based on his/her health condition. From a customer's perspective, the user can enable alerts on his smartphone regarding his grocery list, can see the map of the store and crowded aisles, and plan accordingly to maintain social distance while shopping. The customer can visit desired aisles and will get items from the smart shelves that will put items in the smart cart without contact. Smart shelves will have three common elements - an RFID tag, an RFID reader, and an antenna. The customer-generated data will be collected by smart shelves and smart carts during the day and this data will be analyzed on the retail cloud. Social distancing can be measured and enforced by AI-assisted autonomous retail robots as well, who can alert the customers through a speaker. The UVD Robot can also use ultraviolet light to zap infection viruses and sanitize surfaces.
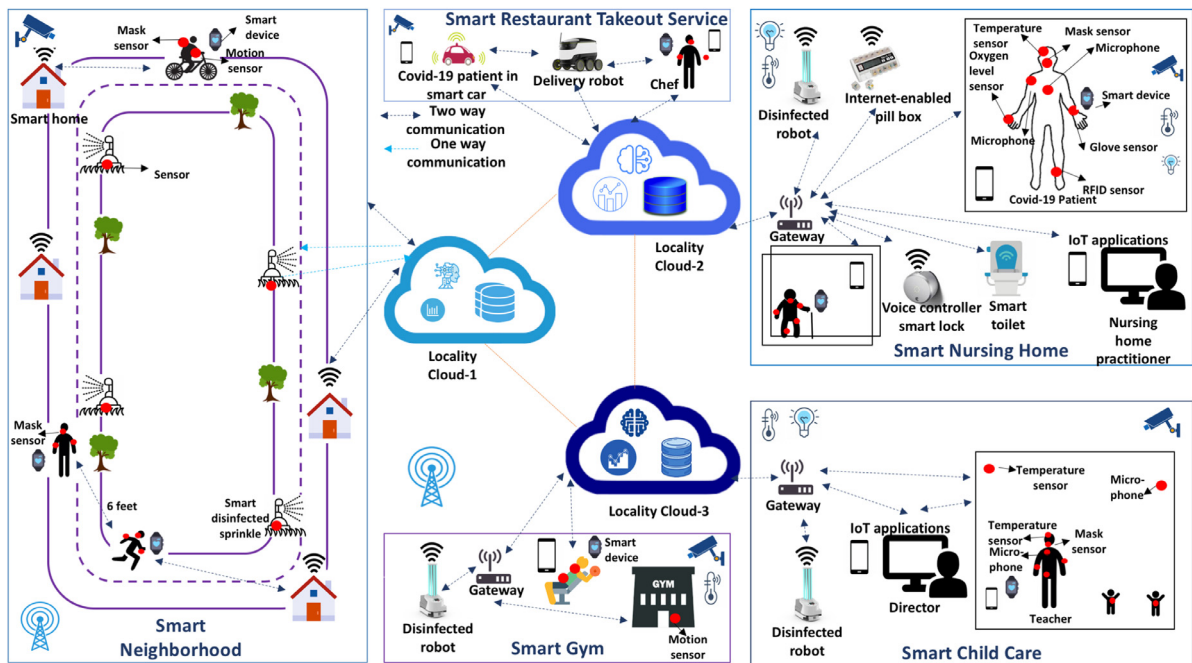

Fig. 6. Connected future smart locality.

Now-a-days, most grocery stores provide contact-less drive through pickup for all customers and delivery at their doors. However, some users, such as elderly people, may not be aware or familiar with such online options. For them, grocery stores can provide smart robot delivery or smart pickup outside the store and also provide a separate parking area to avoid long waiting lines. A restaurant takeout service can follow the same protocol for smart pickup. Intelligent Transportation System (ITS) [62–64] can support in delivering resources to users. Gupta et al. [65] have also elaborated how ITS and smart city infrastructures can be used to enable and enforce social distancing community measures in COVID-19 outbreak.

5.4. Smart Locality

Smart localities have been widely investigated in the literature [66–71]. Such localities consist of various interdependent human and physical systems, where IoT represents the sensing and actuating infrastructure to estimate the state of human and physical systems and also assist in adapting/changing these systems. Here, we discuss two scenarios, which can help humans to adapt to the new normal in COVID-19 situation. These two scenarios including other relevant scenarios are shown in Fig. 6.

5.4.1. Smart Neighborhood
Every individual, who lives in a smart neighborhood, will receive notifications regarding allotted time for outside activities, such as riding a bike, a walk on the trail, etc. in order to maintain the social distancing while being outside in common areas. In a smart neighborhood, motion sensors and cameras will sense the presence of people and will send the counting numbers to the locality cloud-1 as shown in Fig. 6. Cloud Smart Analytics[29] service can analyze the locality data and will send notifications to users. IoT applications can suggest different paths for each individual using motion sensors and traversing algorithms so that people can avoid meeting infected people without knowing his/her identity. There will be disinfected sprinkler installed that can spray on the pedestrian path and community park when sensors will sense the presence of an infected person in the area through notifications from the locality cloud-1.

5.4.2. Smart Child Care and Nursing Home
The U.S. CDC[30] have issued guidelines in order to safely open child care and schools in the locality. The child care can use RFID tags, motion sensors, door sensors, and smart devices for children's safety. The sensors can be attached to kid's clothes to monitor their sleep patterns, breathing patterns, body temperature, and body position and this data can only be stored on edge server for child security purpose, while staff/teacher-generated data can store on locality cloud-3. AI-assisted
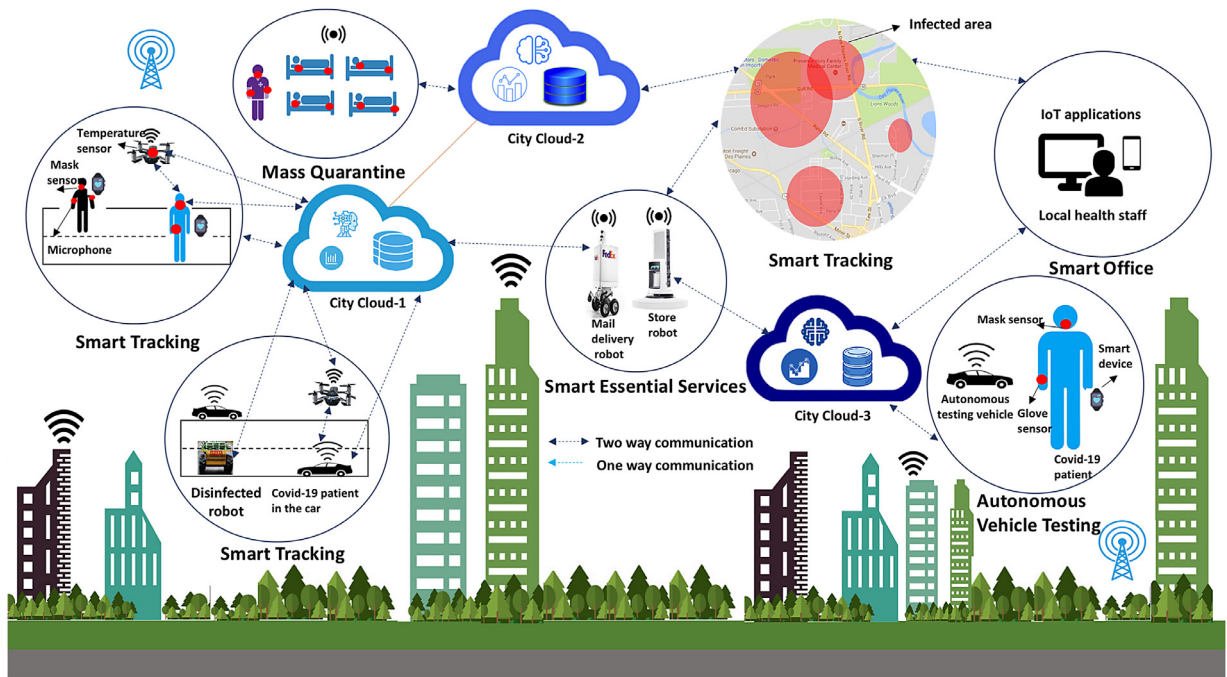
Fig. 7. Conceptual futuristic smart city overview.

camera can be installed in child care rooms to measure social distancing among children and teachers and it is shown in Algorithm 2. However, it is a challenging undertaking to maintain physical distancing in child care. In such a scenario, sensor based partitions of each room will allow a gap among the kids and will allow only one or two kids in each partitioned area to maintain the distance among them. The teacher and staffs will receive notifications to change their gloves and masks through attached sensors on gloves and masks. In a smart nursing home, if an elderly person shows symptoms of COVID-19, then he/she should be treated in an isolated room immediately. Autonomous robots can be utilized to help in disinfecting common areas, and by following Algorithm 3 (as discussed in Section 6). Elderly health generated data and their clinical reports can be accessed through applications and will store in locality cloud-2. The care coordinator should have access to locality cloud-2 to monitor each elder regularly.

Similarly, a smart gym would include motion sensors, door sensors, humidity sensor, temperature control sensors, and AI-assisted cameras. The generated data will be stored on locality cloud-3, and will be analyzed by cloud services. Gym manager/HOA can only access the analyzed information anonymously, so that he can assign a particular time to maintain the 25% occupancy and time interval to sanitize all gym equipment and surfaces. To enable multi-cloud secure data and information sharing and communications between locality clouds, there is a need to build a decentralized trust framework in place of using advanced technologies like Blockchain and trusted distributed computing.

5.5. Smart City

Daegu[31] has setup a novel system using a large amount of data gathered from various sensors and devices, such as surveillance camera footage and credit card transactions of confirmed coronavirus patients to recreate their movements. The Newcastle University Urban Observatory[32] developed a way of trackingpedestrian, car parks, traffic movement to understand how social distancing is being followed in Tyne and Wear. However, other major cities need to prepare themselves for coronavirus future outbreak waves. Smart cities can host a rich array of technological products that can assist in early detection of coronavirus outbreaks through IoT sensors, and mitigate infection through social distancing and mandatory masks policy. Connected sensors and data sharing through the cloud-IoT architectures can be utilized to enforce social distancing measures around a smart city. Here, we discuss various scenarios including smart tracking, and autonomous testing vehicles for the smart city, which are shown in Fig. 7. In the past, several research works [67,72–79] have been done on smart city infrastructures.

---

[31] https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109
[32] https://COVID.view.urbanobservatory.ac.uk/#intro

5.5.1. Smart Tracking

Most of the countries[33] used phone data to track citizens' movements during the pandemic. In addition, urban cities deployed connected drones and law enforcement, which can help to track and restrict movement of individuals in a smart city without evading citizens' privacy. A smart city can be characterized by smart infrastructures that will be optimized for performance to mitigate coronavirus outbreaks and saving lives of the citizens. The smart infrastructures need to follow the protocols defined by federal and state agencies. In Spain, Nice city[34] has been using drones controlled by police to enforce the lock down and circulate information announced messages like *"Please respect the safety distances."* attached with loudspeakers. These Unmanned Aerial Vehicles (UAVs) also sprayed disinfectant at Zhengwan village, amid an outbreak of the new coronavirus, in Handan, Hebei province, China. Savannah city[35] announced plans to use drones to enforce social distancing among residents.

In a smart city, AI-assisted drones are being used to measure six feet distance among people using distance measurement sensor mono/stereo. The distance measurement sensors are divided into multiple categories; however mono/stereo is less costly, accurate, fast, and high resolution. AI-assisted drones can also identify those people who do not follow the protocols, for example, user is not wearing a mask, may receive $500 fine. In smart cities, multiple drones monitor citizens, to avoid collision obstacle avoidance algorithm and Simultaneous Localization And Mapping (SLAM) can be employed. These drones train their models on edge using federated learning process before sharing its training data with an edge or city cloud-1, federated learning algorithm is discussed in Section 6. Thus, each drone can monitor its area based on individual experiences. However, aggregate value of parameters from nearby urban areas is collected at the edge computing side for collective decision making.

As shown in Fig. 7, COVID-19 test result of a patient can be stored on city cloud-1, which can be shared with local state staff and healthcare providers. Most dominant Cloud Service Providers (CSPs) use their own default data placement strategy to manage storage and computing of data, the CORE-Algorithm [80] can be used to re-organizes the distributed file system by redistributing the data blocks to give an optimal data placement. Furthermore, QR codes can help the citizens using geographic data to know about risk zones in the city.

5.5.2. Autonomous Testing Vehicle

In order to keep patients and healthcare providers safe, drive-thru coronavirus testing sites have been popping up in the city. An autonomous testing vehicle can be used for COVID-19 testing in urban city as well as rural areas. Multiple sensors including infrared body temperature sensor, oxygen level sensor, AI-assisted camera and microphone will be installed onto the vehicle which will also carry testing kits, PPE, etc. This autonomous vehicle can help reduce exposure of elderly and pre-existing condition people to COVID-19. A person will get notification of autonomous vehicle's arrival, then he/she can enter from one side of the glass-walled area in the car. In-built sensors can record a person's body temperature, oxygen level and can store this data on local edge device. The generated health data will be stored on local edge storage and these sensors will also publish the data on city cloud-3 to share with healthcare practitioners. It can also provide a test kit to individuals who can test themselves and return it through the car window. In rural areas, autonomous testing vehicles can bring awareness of COVID-19, improve accessibility to testing, and can even provide free testing to underprivileged communities.

To flatten the curve of confirmed cases, smart city can provide mass quarantine for coronavirus patients, who have mild symptoms but are higher risk individuals for spreading cross-infection to others. A smart hall or large stadium or facilities can be setup for quarantine with installed sensors, smart devices, and robots that are connected to cloud (as shown in Fig. 7). Disinfectant robot is an autonomous robot that can sterilize floors in these large areas as discussed in other scenarios. The large-scale disinfectant robot can also be used to clean the roads of the city. Autonomous and self-driving vehicles can be used for delivering the post, which will also help to reduce human contact and cutting down the number of COVID-19 cases. Smart city can also provide immunity-based RFID tags to those people, who recover from the disease and can allow the tag holders to return to work with extra-precautions. In the future, once COVID-19 vaccines are available, the individual with vaccination can get similar immunity-based RFID tags to prove their immunity. In another context, autonomous vehicles have been extensively investigated in the literature [81–89].

6. Implementation and Enforcement

In this section, we present a general implementation and enforcement framework for smart community use case scenarios discussed in Section 5 utilizing AWS cloud and IoT platform. We also discuss a family of algorithms that can be used in the context of different use case scenarios. To further demonstrate the applicability and benefits of smart connected communities, we also implement an RPM use case along with proof of concept deployment setup, configurations for physical devices, and cloud services used for enforcing this scenario. This prototype implementation can be considered as a baseline which can be extended and customized to wide geographic and large scale connected communities. It must be noted
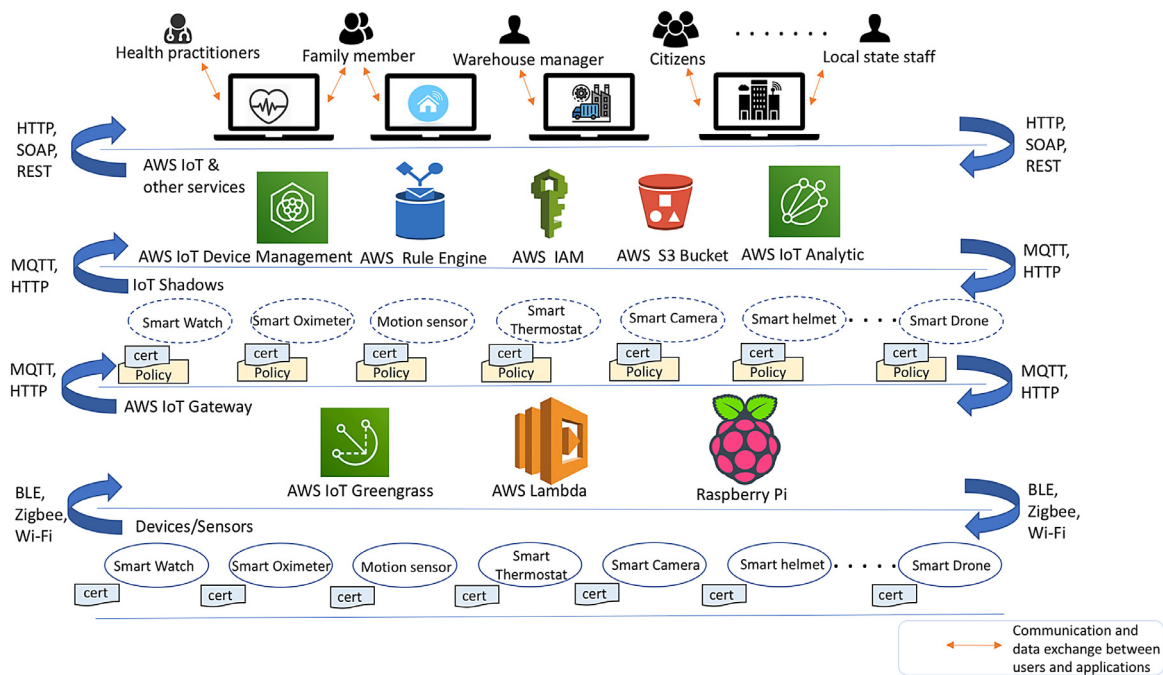

Fig. 8. General implementation framework for smart communities utilizing AWS IoT and cloud services.

that AWS is one of the cloud providers that can support this general framework. Similarly, other architectures can also be supported using different cloud and IoT providers, such as Google IoT[36], Microsoft Azure[37], Openstack[38], etc.

6.1. Generalized Implementation Framework in AWS

The smart connected ecosystem with specific use case scenarios can be implemented using real-world cloud-enabled IoT architecture, such as supported by AWS cloud and IoT platform. Fig. 8 illustrates our proposed implementation architecture, which can be used as a general framework for the use case scenarios discussed in Section 5. This framework consists of smart devices per use case requirements, virtual things/objects, AWS cloud and its IoT and other services. Fig. 8 shows a set of devices at object layer and their corresponding virtual objects at VO layer (as discussed in multi-layered architecture in Section 4). However, other types of devices and their VOs can be created based on use case scenarios. More specifically, this proposed implementation includes AWS IoT core[39] in cloud, AWS Greengrass[40] running on edge gateways (e.g., Raspberry Pi enabled gateway), and IoT devices/things. The edge gateway can be enabled using Raspberry Pi[41] that host the AWS Greengrass deployment, and customized lambda[42] functions that can run on the gateway for edge communication and computation, sending notifications, or enforcing access control and privacy policies. After setting up AWS Greengrass gateway, data collection from smart devices can be processed locally to enhance the real-time intelligence of IoT applications and devices, critical in health related scenarios, such as RPM. For instance, a COVID-19 patient's body temperature and oximeter data need to be monitored regularly, and if there are any complexities (e.g., high temperature, breathing issue), then a notification would be sent to a connected ambulance. The patient can also define more restrictive policies for data security and privacy, for example, only hospital doctor can access his/her health data.

AWS Greengrass can enable edge communication between devices and gateways. As shown in Fig. 8, AWS Greengrass allows users to securely connect their devices to gather data and communicate with gateway (where Greengrass is deployed) which allows to take intelligent actions locally even when the internet connectivity is down. When connectivity is re-established, the data will synchronize with other cloud based IoT services including AWS IoT core, AWS IoT device management, AWS S3[43] bucket, etc. Data collected by smart devices can also be forwarded to AWS IoT cloud using MQTT/HTTP

---

[36] https://cloud.google.com/iot-core
[37] https://azure.microsoft.com/en-us/
[38] https://www.openstack.org/
[39] https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html
[40] https://aws.amazon.com/greengrass/
[41] https://www.raspberrypi.org/
[42] https://aws.amazon.com/lambda/
[43] https://aws.amazon.com/s3/

Algorithm 1 Federated Learning on Smart Edge Gateway Device i for Monitoring.

1: Define initial parameters w^i, learning rate α and number of local epochs H.
2: Repeat all the steps until minimum error is obtained:
3: Download parameters w^{global} from Parameter Server to learn the symptoms of COVID-19.
4: Collect user health data from wearable devices including smart bracelets, smart rings and non-wearable devices including thermal scanner, oximeter and send the data to edge devices including mobile phone, Raspberry Pi.
5: LocalTraining (i,w^i): Train user health data on each device to build own ML model for monitoring.
6: Split local dataset D_i to minibatches of size K which are included into the set K_i.
7: **for** each local epoch j from 1 to H **do**
8:     **for** each k $\in K_i$ **do**
9:

$$\Delta w^i = \Delta w^i - \alpha \frac{\partial E_i}{\partial w^i} \qquad (1)$$

10:     **end for**
11: **end for**
12: Each edge device uploads local gradients Δw^i to Parameter Server.
13: Parameter Server also aggregates these local gradients Δw^i asynchronously.

$$w^{global} = w^{global} + \Delta w^i \qquad (2)$$

14: Each edge device downloads updated parameters w^{global}.

Algorithm 2 Social Distancing through Smart Assistant Camera i.

1: **for** each smart assistant camera i **do**
2:     Measure δ using mono/stereo distance sensors attached in smart assistant camera
3:     **if** $\delta <$ predefined threshold **then**
4:         Send alert to maintain distance
5:     **end if**
6: **end for**

---

protocols. For enabling a secure architecture, AWS IoT Core provides mutual authentication and encryption for secure data transfer and at rest. The mutual authentication mechanism is based on X.509 certificate to ensure proper secure device provision and authorization for data exchange between devices and AWS IoT core. AWS IoT will generate certificates signed by certificate authority, which can be assigned authorization policies to secure user devices and data, and also to enable different access levels (full control/view only) to individuals (e.g., family members, friends, and health practitioners). In AWS IoT, device management service allows users to quickly onboard their large and diverse fleets of devices and store the data while keeping their fleets secure. Some other services on top of them like AWS IoT analytic can also be used to analyze a large amount of data collected from these devices. For instance, health practitioners can analyze patient's health data using AWS IoT analytic service. It can also integrate seamlessly with other AWS services, such as amazon quick site for visualization of IoT data and AWS sage maker hosted by ML service which is used for predictive analytics. In this proposed framework, the smart devices (e.g., smartwatch, oximeter, etc.) must be compatible with AWS cloud to use its services.

We have proposed three algorithms which can be adapted and aligned based on the needs of different smart community use-cases. Algorithm 1 outlines a wearable and non-wearable device's federated learning process on the edge including mobile phone and Raspberry Pi before sharing its training data with cloud. We assume local vector of neural-network parameters w^i to learn a model to predict the symptoms of COVID-19. Parameter Server (PS) maintains a separate parameter vector w^{global}. The model on edge device will initialize parameters (weights) w^i, where $i=1,2,3,..N$, randomly or by downloading their latest values from PS. Each edge device or Raspberry pi trains a local model and optimize the loss value using Stochastic Gradient Descent (SGD). This process continues until SGD converges to a local optimum. Let E be the error or loss value, i.e., the difference between the true value of the objective function and the computed output of the network, and it can be based on L^2 norm or cross entropy. The back-propagation algorithm computes the partial derivative of E with respect to each parameter in w^k and updates the parameter so as to reduce its gradient. We refer to one full iteration over all available input data as an epoch. Thus, the mobile device and Raspberry Pi train user's data on edge. Algorithm 2 outlines that smart assistant camera, attached with distance measure sensors including mono/stereo, measure the distance δ between two users at any smart community to enforce social distancing. The user will receive alert, if his distance from other user is less than a certain threshold value (e.g., 6 feet).

Similarly, Algorithm 3 presents a general traversing strategy that can be followed by any smart sanitizing device within any smart infrastructure including smart hospital, smart nursing home, and smart home, etc. We assume that smart infrastructure can be divided into three different zones: Isolation Zone (IZ), Living Zone (LZ), and Staff Zone (SZ), where COVID-19

Algorithm 3 Traversing Strategy for Smart Sanitizing Device i.

1: Divide any infrastructure into three different zones: Isolation Zone (IZ), Living Zone (LZ), and Staff Zone (SZ)
2: Call count_person()
3: **for** each smart sanitizing device i **do**
4:     **if** number_IZ $\geq$ max-threshold-1 **then**
5:        sanitize IZ
6:     **end if**
7:     α = max(number_LZ, number_SZ)
8:     **if** $\alpha \geq$ max-threshold-2 **then**
9:        sanitize that zone
10:     **end if**
11: **end for**
1: **count_person()**
2: set number_IZ= 0, number_LZ = 0, number_SZ = 0
3: **for** each motion sensor j **do**
4:     **if** mono/stereo, ultrasound and motion sensors detect presence of person in IZ at any infrastructure **then**
5:        number_IZ = number_IZ + 1
6:     **else**
7:        **if** mono/stereo, ultrasound and motion sensors calculate number of person at LZ at any infrastructure **then**
8:           number_LZ = number_LZ + 1
9:        **end if**
10:     **else**
11:        **if** mono/stereo, ultrasound and motion sensors detect the persons in SZ at any infrastructure **then**
12:           number_SZ = number_SZ + 1
13:        **end if**
14:     **end if**
15: **end for**

---

patients live in IZ, the presence of visitors and working staffs represent by LZ and SZ, respectively. The threshold value of IZ will be different from LZ and SZ. The motion sensors will count the number of people in a particular zone. The max-threshold-1 is assigned for IZ, while max-threshold-2 is assigned for LZ and SZ. Smart sanitizing devices including autonomous robots will communicate with motion sensors and will traverse accordingly as per the algorithm. Here, we present generic algorithms that can be adopted in different scenarios as well as can be customized as per the needs of spe-
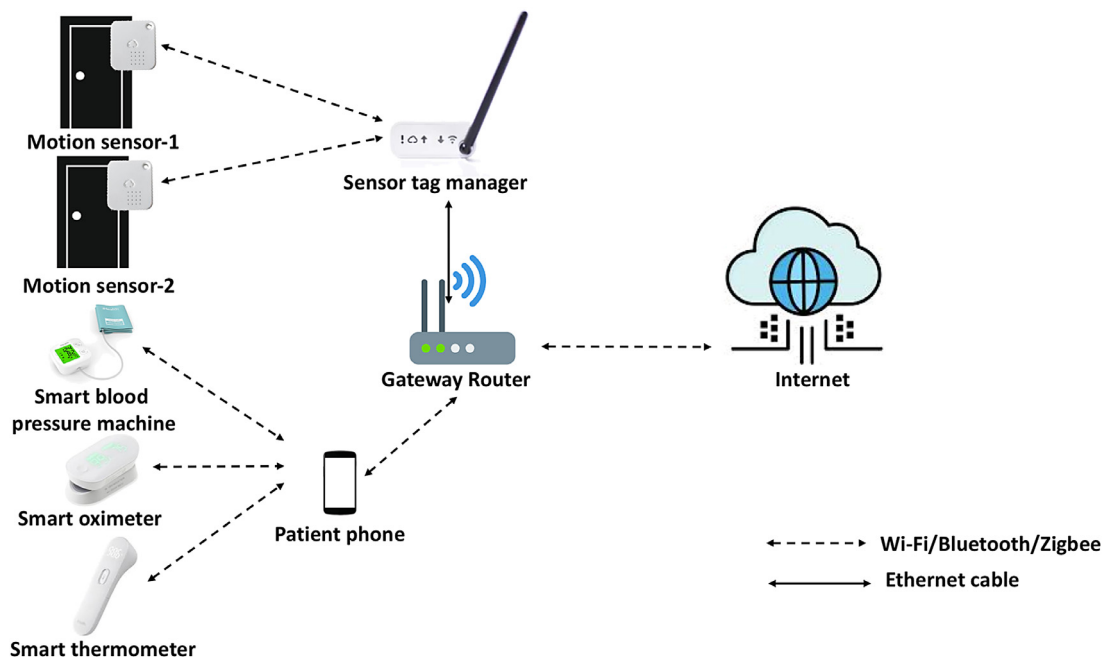

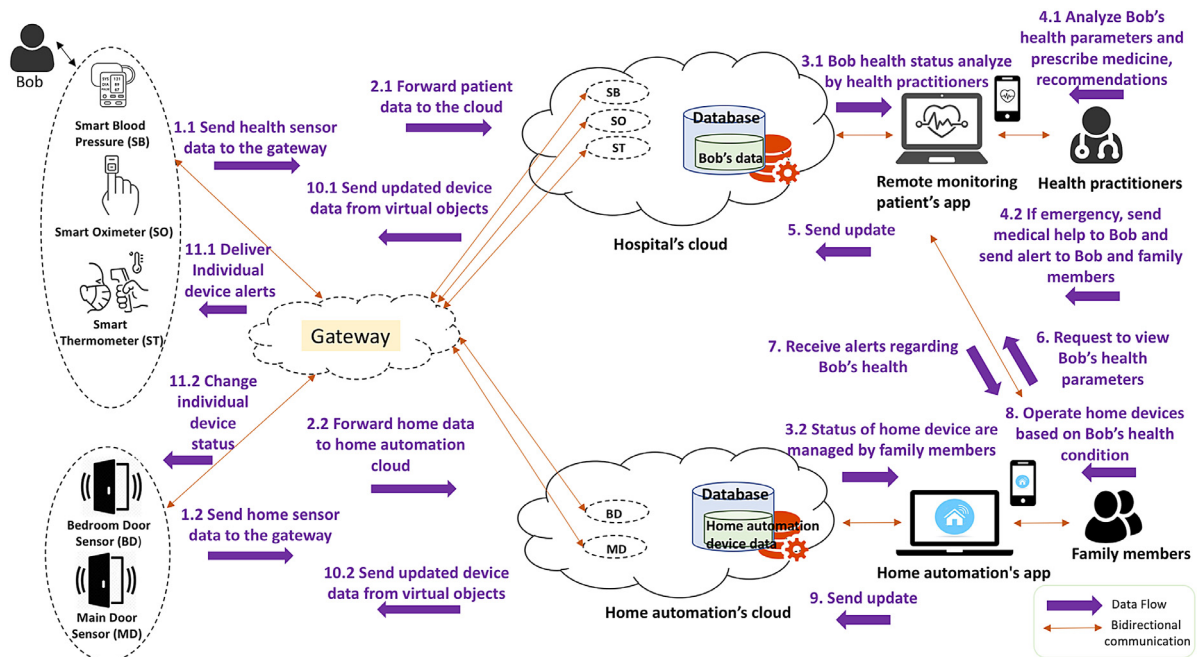**Fig. 9.** Set up of remote patient monitoring in a smart home.

Fig. 10. Sequential view of remote patient monitoring in a smart home.

cific application scenarios. Discussed use case scenarios can implement any of the defined algorithms on AWS cloud based implementation and enforcement architecture with other technologies.

6.2. Proof of Concept Implementation of Remote Patient Monitoring Use Case

E-Health use case consists of various scenarios including smart hospital, RPM, and smart testing. This section presents implementation of an RPM scenario in real-world. We consider Bob, who is 34 years old and lives alone at his home, has been diagnosed with coronavirus. He is monitored by his health practitioners continuously through the RPM system. His family members, who live in a different state, also monitor him through RPM system. We set up and configure the RPM system with smart health and smart home devices at his home setting as shown in Fig. 9. For implementation of RPM, we set up a wireless network at Bob's home using ARRIS SB6121 modem, TP-Link AC1200 wireless router, and smart devices including Ethernet Tag Manager, wireless sensor tags, and various BLE based health devices (e.g., iHealth smart oximeter, iHealth smart blood pressure monitor, and iHealth smart thermometer). These health devices are suggested by Bob's health practitioners. Ethernet tag manager is connected to a router through CAT 5 Ethernet cable, it is linked with two wireless sensor tags installed at bedroom door and main door. This entire testbed setup is deployed around 8 - 10 days.

Fig. 10 shows a sequential view of RPM for COVID-19 patient Bob at his smart home and his health conditions are continuously being monitored by health practitioners and his family members. The data generated from these devices is stored at their corresponding manufacturer's clouds (e.g., iHealth cloud, Wireless sensor cloud) and analyzed by their cloud services. At his smart home, motion sensors are attached at doors with 30° angle. If the angle of door is more than 30° the sensor sends the notification "open-door" to gateway device (e.g., Bob's smart phone). The generated data is pushed onto home automation's cloud, and his family members will also receive notification through IoT applications. Both motion sensors communicate through Ethernet tag manager, which has a connected light. When light turns ON it means that it is connected to the cloud based web service, when update light flashes it means that it is forwarding door sensor state (Open/Close) to the web service. Bob checks his body temperature, oxygen level, and blood pressure in every 3 hours, and connected health devices at object layer communicate to a gateway device (i.e., Bob's smart phone) which allows interaction with the upper layers of the architecture. During 15 days of monitoring, The range of Bob's body parameters are - SpO_2 (88% - 98%), blood pressure readings (110/65 mm Hg - 130/70 mm/Hg), and body temperature (98° - 103°). When Bob's body temperature reached at 103°, the health practitioners prescribed medicine and also informed his family members to watch him continuously. Bob was not able to sleep at night coughing, then his family members received notification from bedroom door sensor through home automation cloud service. They then communicated with him and asked him to check his oxygen level, which should not be less than 80%. Fig. 10 shows an overall sequential view of RPM at home along with data flow and interactions among entities and components of the system.

This setup is an implementation of one of the smart communities' scenarios, i.e., RPM. Similarly, other use case scenarios can be implemented using the same technologies and solutions along with various IoT devices and utilizing our proposed
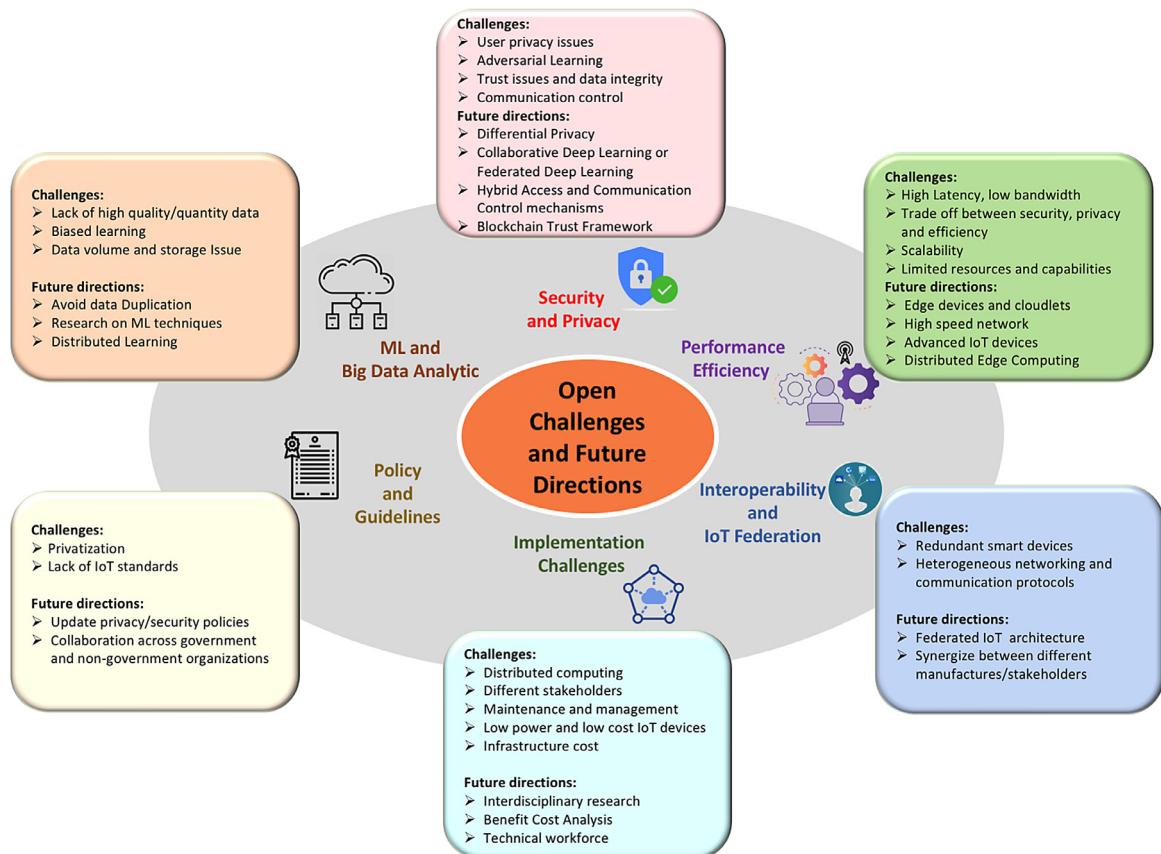
Fig. 11. Open challenges and future directions in smart communities deployment.

implementation architecture. While we discuss an existing cloud-enabled IoT implementation architecture and relevant technologies, there are several challenges to scale it for enabling future smart communities with various such smart application scenarios. Therefore, enabling such highly distributed, autonomous, and interdisciplinary architecture in a real-world environment demands future research to overcome current challenges and make smart communities a reality in the future.

7. Open Challenges and Future Directions

The development of the proposed smart connected ecosystem requires addressing several challenges and needs interdisciplinary research from an integrated perspective involving different domains and stakeholders that we learned from proposed implementation of smart communities and implemented RPM system. In this section, we will discuss these challenges and required future research in detail with examples from each of the proposed scenarios, as illustrated in Fig. 11.

7.1. Security and Privacy

One of the major challenges in the deployment of the smart infrastructures is the security and privacy concerns pertaining to IoT and CPS [90] users, smart devices, data, and applications in different application domains like healthcare, smart home, supply chain management, transportation, and smart city. In the health care industry, it is still a challenge to secure connected medical devices and ensure user privacy.

In E-health scenario, for instance, a user visits smart testing booth for COVID-19 testing, and his/her data will transmit and store on smart hospital private cloud. Hospitals then share this data with state healthcare staff or city government for tracking and monitoring the user activities. To secure the identity of a user and ensure privacy, differential privacy [91] and data masking techniques [92] (pseudonymize [93], anonymize [94]) can be used. However, there are limitations intrinsic to these solutions. In pseudonymize technique, data can be traced back into its original state with high risk of compromising user privacy, whereas it becomes impossible to return data into its original state in anonymize. It is critical to ensure user privacy while deploying IoT and data-driven applications for their wide-adoption in preventing, monitoring, and mitigating COVID-19.

Secure authentication mechanisms including access control and communication control models are necessary for cloud-enabled IoT platforms to defend against unauthorized access and securing data, both at rest [95–99] and in motion. Several IoT access control models have been developed in the literature [100], with cloud-assisted IoT access control models for AWS [48], Google [42], and Azure [101]. Traditional access control models are not adequate in addressing dynamic and evolving access control requirements in IoT. Attribute-Based Access Control (ABAC) [102–105], offers a flexible and dynamic access control model, which fits more into distributed IoT environments, such as smart home [49], connected vehicles [88,106], and wearable IoT devices [21,107].

In addition to access control, communications in terms of data flow between various components in cloud-enabled IoT platforms need to be secured from unauthorized data access and modifications. Thus, Attribute-Based Communication Control (ABCC) [108] has been introduced. A novel lightweight authentication protocol [109] has been proposed to protect password, which is based on smart card and biometric identification. Moreover, for multi-cloud interaction and collaboration across several connected communities, there needs distributed computing enabled by dynamic trust frameworks. Further research on Blockchain technology [110] to enable a trusted framework among different cloud based platforms is necessary. Advanced access control techniques with a hybrid approach (including benefits of several access control models) need to be designed to give access to users at different levels. For example, in a smart connected community, users will have different levels of access on smart devices, data, and applications. With the recent surge in contact tracing applications, user data privacy concerns are surfacing and will continue to arise in the future. Recent article[44] have suggested the need to ensure privacy and develop privacy-aware contact tracing solutions to balance public health and personal privacy of the users. A pertaining risk to these and other AI-assisted system and applications is adversarial machine learning [111], using which adversaries compromise user data and privacy. In order to protect the data sets, differential privacy [91,112] can be applied to add noise. Cloud based medical data storage and the upfront challenges have been extensively addressed in the literature [113,114]. A study [115] conducted semi-structured interviews with fifteen people living in smart homes to learn about how they use their smart homes, and to understand their security and privacy concerns, expectations, and actions.

Various supervised ML algorithms are used for security such as classification of IoT data as "attack" or "normal"; however, these algorithms have not succeed to produce significant results due to distinct requirements of IoT devices including scalability, distribution, resource limitations, and low latency. This study [116] introduced a fog-based attack detection framework and a ELM-based Semi-supervised Fuzzy C-Means (ESFCM) method, which are the extension of cloud computing, fog computing based framework enables attack detection at the network edge and ESFCM method uses a semi-supervised fuzzy c-means algorithm to handle the labeled data issue.

In future research, there are requirements to conduct interviews of health practitioners to understand the security and privacy concerns while developing the smart hospital and need to apply similar approach involving community residents, infrastructure developers and stakeholders to develop other components of the smart connected ecosystem. Privacy preserving deep learning [117,118] approaches such as collaborative deep learning or federated learning also need to be explored to train and deploy local models at the edge devices. A Blockchain-based secure DL [119] that combines DL and Blockchain to support secure collaborative DL in IoT. Collaborative DL approach is performed at the edge device level to avoid the third party, whereas Blockchain is engaged to verify the confidentiality and integrity of collaborative DL in IoT.

7.2. Performance Efficiency

Within a connected ecosystem, users are constantly interacting with numerous smart devices and applications. One of the main challenges in such an environment with billions of smart devices is performance efficiency and QoS. High latency, response time, packet loss, and low bandwidth are various parameters in a network system that affect the usability and feasibility of IoT systems. These devices generate large volumes of data which results in a surge in data traffic that causes network congestion and latency.

Due to high latency, it is not recommended to perform any computation on a centralized cloud for critical healthcare services in an emergency situation. End-users and front-line workers prefer computation on edge devices and cloudlets to lower the wait and offer real-time analytics. This study [33] shows various approaches to improve accuracy and efficiency of applications. Research and advancements in distributed edge computing technologies, low latency networking and communication protocols are essential to enable continued success of IoT-enabled smart environments. Data can be stored on multiple edge devices to improve processing efficiency and response time. Typically, high energy consumption required by mobile communications is a serious hurdle to large scale IoT deployments of use case scenarios. In near future, we expect to witness IoT applications expand in a world of 5G, with the proliferation of high speed networks with low latency applications, such as RPM, real-time Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication.

7.3. Interoperability and IoT Federation

Recently, there have been many smart devices introduced by various manufactures in the market. For example, there are several smart home assistants (e.g., Google Home, Alexa) that users can choose, however, these devices use different

---

[44] https://spectrum.ieee.org/telecom/security/tracking-covid19-with-the-iot-may-put-your-privacy-at-risk

communication protocols and also have connections with their corresponding cloud services. Interoperability among IoT devices has been an issue since the beginning of smart ecosystem deployments. The heterogeneity among billions of IoT devices adds to the challenge of developing smart connected communities. While in computer systems, TCP/IP is a standard suite of protocols that enable any system to communicate with other systems, such standards are still lacking in IoT domain.

Another critical issue is how to reduce redundant smart devices. An effective solution to this problem would be to develop federated IoT and cloud architectures that can communicate with any type of sensors and devices. For instance, in different smart domains, a user received multiple wearable smart bracelets in smart communities. It will be challenging to keep track of all alerts through their corresponding IoT applications. Therefore, there is a need to develop federated IoT architectures to enable federation across multiple smart devices and applications which can allow access and data communication across multiple IoT platforms. The research [120] suggested that IoT cloud provider allowed all devices belonging to the same private/public owner to participate in the federation process. However, many devices do not support other manufacturer's application platforms. For instance, in a smart home, all sensors and devices are connected through a home assistant, and AI-assisted application sends notification to the home assistant. Due to interoperability or compatibility issue, home assistant could not receive the notifications from all devices. For future research, IoT software engineers, manufacturers, and stakeholders should create synergies together to build smart devices and federated IoT architectures.

7.4. Policy and Guidelines

IoT is an emerging technology that is being adopted by several nations across the world. Countries[45] have different guidelines and policies for preserving privacy of users and their personal data [121–123], which are still evolving. Australian Privacy Principles (APP) [124] designed their own guidelines, procedures and standards to protect individual privacy associated with data collection through IoT. The U.S. Department of Transportation (USDOT) has similarly issued smart city challenge[46] and policy initiative in this direction. The U.S. government has committed approximately $160 million[47] over the next five years to support smart city initiatives smart connected communities with hospitals, homes, cities, or transportation demand new constitutions and policies for preserving user data privacy and misuse of data and information. Such policies should maintain the privacy of users and address other issues including accuracy, property and accessibility, together with infrastructure design to facilitate swift implementation of guidelines and public orders in COVID-19 and other similar situations.

One reason for the lack of constitutions and policies may be because the IoT differs from other network technologies and there is a lack of specific IoT standards. The research on constitution and policy, including engagement on public policy development debates, and IoT standards is necessary to successfully integrate privacy, accuracy, property and accessibility solutions in the smart communities. To develop effective constitutional policies and standards, collaboration across governmental, non-governmental organizations, and industry partners as cloud providers, IoT manufacturers, would be beneficial.

7.5. Implementation Challenges

Enabling a smart community requires thousands of low-power and low-cost embedded devices, which work together with large scale data analytics and applications. There are several implementation challenges involved in developing such a large scale smart infrastructure. Fault tolerance and resilience are the challenges for reliable delivery of sensor data from smart devices to distributed cloud services. IoT applications need fault tolerance since there can be various issues in applications or systems including face recognition, community infrastructure management, and emergency response in smart infrastructure. GEOgraphically Correlated Resilient Overlay Networks (GeoCRON) [125] is developed to capture the localized nature of community IoT deployments in the context of small failures. Research [126] proposed a new fault-tolerant routing technique for hierarchical sensor networks. Cloud service providers can be maximized their revenue using an optimal pricing scheme [127]. Another challenge for constant running and managing these IoT devices is costs related to energy, communication, computation, infrastructure, and operation. There is generally a trade-off between benefit and cost for IoT applications [128], however in the scenario of COVID-19 pandemic, expected benefits (saving lives, economic growth) should outweigh the operational and deployment costs. For instance, to build RPM platform with various vendors - Intel technologies, iHealth labs, etc., which provide pre-validated platforms for faster and lower cost development. Combined implementation cost includes smart devices cost, servicing and monitoring cost for RPM platform, which can be range from $275 - $2300 per patient per year. As we setup test bed of RPM use case at home, the total cost of this test bed is $310 and spent 8 - 10 days to setup this use case.

Another challenge is to build a prediction model by paying minimum cost, which may affect the accuracy of the model. This study [129] proposed a game theoretical analysis to allocate more storage capacity in a cost-effective manner, which achieves to maximize the benefits. For future directions, game theoretical approach can be used to analyze the smart infrastructures in terms of cost-benefit analysis. Furthermore, interdisciplinary research collaboration is inevitable to implement a smart connected ecosystem. There are several areas of research and engineering aspects, as machine-to-machine technology,

---

artificial intelligence [130,131], ML, predictive analysis, security and privacy, and others need to be merged and collaborative research approach is necessary for implementing, deploying, and managing a smart connected ecosystem.

7.6. Machine Learning and Big Data Analytic

IoT generates a tremendous amount of data, and this raw data is converted into valuable knowledge using AI and ML technologies. The "6V" (Value, Velocity, Volume, Variety, Variability, and Veracity) big data challenges for IoT applications are discussed in [132,133]. The volume of data from IoT devices overwhelms storage capacities. There is not only a storage issue, but data needs to be organized properly so that it can be retrieved and processed. Data duplication is an issue when an organization has multiple copies of the same data source. For example, a user has multiple wearable smart bracelets (smart hospital bracelet, smart grocery bracelet, and RFID antibody tag bracelet), these wearable devices will collect similar kind of data, which can create an issue of data duplication.

ML based applications require a large amount of valuable data for correct prediction, however, complicated and insufficient data can be an issue to the accuracy of the learning and predictive models. In addition, ML approaches need further research and development to deal with such heterogeneous and constantly evolving sensory data inputs. For instance, a locality-based COVID-19 patient detection model can predict early symptoms, which will be based on the collaboration of smart nursing home data sets and smart child care data sets. The prediction model can be biased towards elderly people if the number of patients in smart nursing home is more than smart child care. To overcome this problem, both models can learn at their edge networks using collaborative deep learning [134]. Research on these open challenges will help early development and deployment of future smart communities.

8. Conclusion

In this paper, we propose future smart connected community scenarios, which are blueprints to develop smart and intelligent infrastructures against COVID-19 to stop pandemic outbreaks in the future. The autonomous operations with low human intervention in smart communities enable a safe environment and enforce preventive measures for controlling the spread of infection in community. Data-driven and AI-assisted applications facilitate increased testing, monitoring and tracking of COVID-19 patients, and help to enforce social distancing measures, predict possible infections based on symptoms and human activities, optimize the delivery of essential services and resources in a swift and efficient manner. This paper discussed different scenarios to reflect smart applications and connected ecosystems. Further, it proposed IoT enabled big data collection and analysis in different sectors including healthcare, home, supply chain management, transportation, environment, and city. A general implementation framework of smart communities is discussed on AWS cloud service. In addition, a proof of concept implementation of a RPM use case is presented. Furthermore, wider implementation of proposed smart connected communities faces many challenges, such as legislation and policy, deployment cost, time, security and privacy, which have also been discussed in the paper. We believe that our vision of future smart communities will ignite interdisciplinary research and development of connected ecosystem to prepare our world against future pandemic outbreaks.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

References

[1] M.H. Kabir, K. Thapa, J.-Y. Yang, S.-H. Yang, State-space based linear modeling for human activity recognition in smart space, Intell. Automat. Soft Comput. 25 (4) (2019) 673–681.
[2] L. Bai, et al., Chinese experts' consensus on the internet of things-aided diagnosis and treatment of coronavirus disease 2019 (COVID-19), Clinical eHealth 3 (2020) 7–15.
[3] R. Vaishya, M. Javaid, I.H. Khan, A. Haleem, Artificial intelligence (ai) applications for COVID-19 pandemic, Diab. Metabol. Syndrome Clinical Res. Rev. (2020).
[4] M. Javaid, A. Haleem, R. Vaishya, S. Bahl, R. Suman, A. Vaish, Industry 4.0 technologies and their applications in fighting COVID-19 pandemic, Diabet. Metabol. Syndrome Clinical Res. Rev. (2020).
[5] K. Kumar, N. Kumar, R. Shah, Role of IoT to avoid spreading of COVID-19, Int. J. Intell. Netw. 1 (2020) 32–35.
[6] D.N. Vinod, S. Prabaharan, Data science and the role of artificial intelligence in achieving the fast diagnosis of COVID-19, Chaos Solitons Fract. (2020) 110182.
[7] M. Otoom, N. Otoum, M.A. Alzubaidi, Y. Etoom, R. Banihani, An IoT-based framework for early identification and monitoring of covid-19 cases, Biomed. Signal Process Control (2020) 102149.
[8] A. Kumar, K. Sharma, H. Singh, S.G. Naugriya, S.S. Gill, R. Buyya, A drone-based networked system and methods for combating coronavirus disease (covid-19) pandemic, Future Generat. Comput. Syst. (2020).

[9] S. Lalmuanawma, J. Hussain, L. Chhakchhuak, Applications of machine learning and artificial intelligence for COVID-19 (sars-cov-2) pandemic: a review, Chaos Solit Fract (2020) 110059.

[10] R.P. Singh, M. Javaid, A. Haleem, R. Suman, Internet of things (iot) applications to fight against COVID-19 pandemic, Diabet Metabol Syndr Clin Res Rev (2020).

[11] S. Swayamsiddha, C. Mohanty, Application of cognitive internet of medical things for COVID-19 pandemic, Diabet. Metabol. Syndr. Clin. Res. Rev. (2020).

[12] R.M. Elavarasan, R. Pugazhendhi, Restructured society and environment: a review on potential technological strategies to control the COVID-19 pandemic, Sci. Total Environ. (2020) 138858.

[13] M.T. Vafea, et al., Emerging technologies for use in the study, diagnosis, and treatment of patients with covid-19, Cell. Mol. Bioeng. (2020) 1–9.

[14] T. Alam, Internet of things and blockchain-based framework for coronavirus (COVID-19) disease, 2020, Available at SSRN 3660503.

[15] A. Albahri, R.A. Hamid, et al., Role of biological data mining and machine learning techniques in detecting and diagnosing the novel coronavirus (COVID-19): a systematic review, J. Med. Syst. 44 (7) (2020).

[16] V. Stantchev, A. Barnawi, S. Ghulam, J. Schubert, G. Tamm, Smart items, fog and cloud computing as enablers of servitization in healthcare, Sensors Transd. 185 (2) (2015) 121.

[17] Y. Li, L. Guo, Y. Guo, Enabling health monitoring as a service in the cloud, in: Proceedings of the IEEE/ACM 7th International Conference on Utility and Cloud Computing, IEEE, 2014, pp. 127–136.

[18] F. Fernandez, G.C. Pallis, Opportunities and challenges of the internet of things for healthcare: Systems engineering perspective, in: Proceedings of the IEEE International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), 2014, pp. 263–266.

[19] M. Gupta, M. Abdelsalam, S. Khorsandroo, S. Mittal, Security and privacy in smart farming: challenges and opportunities, IEEE Access 8 (2020) 34564–34584.

[20] M.S. Hossain, G. Muhammad, Cloud-assisted industrial internet of things (IoT)–enabled framework for health monitoring, Comput. Netw. 101 (2016) 192–202.

[21] S. Bhatt, F. Patwa, R. Sandhu, An access control framework for cloud-enabled wearable internet of things, in: Proceedings of the IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), IEEE, 2017, pp. 328–338.

[22] A.K. Yadav, M. Garg, et al., Docker containers versus virtual machine-based virtualization, in: Proceedings of the Emerging Technologies in Data Mining and Information Security, Springer, 2019, pp. 141–150.

[23] M. Satyanarayanan, P. Bahl, R. Caceres, N. Davies, The case for vm-based cloudlets in mobile computing, IEEE Pervas. Comput. 8 (4) (2009) 14–23.

[24] M. Nitti, V. Pilloni, G. Colistra, L. Atzori, The virtual object as a major element of the internet of things: a survey, IEEE Commun. Surv. Tutor. 18 (2) (2015) 1228–1240.

[25] V. Pandey, P. Saini, Application layer scheduling in cloud: fundamentals, review and research directions, Comput. Syst. Sci. Eng. 34 (6) (2019) 357–376.

[26] L. Catarinucci, et al., An IoT-aware architecture for smart healthcare systems, IEEE Int. Things J. 2 (6) (2015) 515–526.

[27] S. Park, S. Jayaraman, Enhancing the quality of life through wearable technology, IEEE Eng. Med. Biol. Mag. 22 (3) (2003) 41–48.

[28] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M.L. Stefanizzi, L. Tarricone, An IoT-Aware architecture for smart healthcare systems, IEEE Int. Things J. (2015).

[29] F. Axisa, P.M. Schmitt, C. Gehin, G. Delhomme, E. McAdams, A. Dittmar, Flexible technologies and smart clothing for citizen medicine, home healthcare, and disease prevention, IEEE Trans. Inf. Technol. Biomed. 9 (3) (2005) 325–336.

[30] L. Xu, C. Xu, Z. Liu, Y. Wang, J. Wang, Enabling comparable search over encrypted data for IoT with privacy-preserving, CMC-Comput. Mater. Cont. 60 (2) (2019) 675–690.

[31] S. Deep, X. Zheng, C. Karmakar, D. Yu, L.G. Hamey, J. Jin, A survey on anomalous behavior detection for elderly care using dense-sensing networks, IEEE Commun. Surv. Tutor. 22 (1) (2019) 352–370.

[32] S. Li, F. Liu, J. Liang, Z. Cai, Z. Liang, Optimization of face recognition system based on azure IoT edge, CMC-Comput. Mater. Continua 61 (3) (2019) 1377–1389.

[33] Y. Li, H. Gao, Y. Xu, Special section on big data and service computing, 2019b.

[34] S. Rathore, et al., Blockseciotnet: blockchain-based decentralized security architecture for IoT network, J. Netw. Comput. Appl. 143 (2019) 167–177.

[35] P. Bellavista, G. Cardone, A. Corradi, L. Foschini, Convergence of MANET and WSN in IoT urban scenarios, IEEE Sens. J. 13 (10) (2013) 3558–3567.

[36] D.J. Freitas, T.B. Marcondes, L.H.V. Nakamura, R.I. Meneguette, A health smart home system to report incidents for disabled people, in: Proceedings of the International Conference on Distributed Computing in Sensor Systems, 2015, pp. 210–211.

[37] N. Hamlil, M. Benabdellah, Study and implementation of a network point health smart home electrocardiographic, in: Proceedings of the International Conference on Advances in Biomedical Engineering, 2013, pp. 109–112.

[38] G. Sprint, D. Cook, R. Fritz, M. Schmitter-Edgecombe, Detecting Health and Behavior Change by Analyzing Smart Home Sensor Data, in: Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP), 2016, pp. 1–3.

[39] M.S. Hossain, Patient status monitoring for smart home healthcare, in: Proceedings of the IEEE International Conference on Multimedia Expo Workshops (ICMEW), 2016, pp. 1–6.

[40] P.N. Dawadi, D.J. Cook, M. Schmitter-Edgecombe, Automated cognitive health assessment from smart home-Based behavior data, IEEE J. Biomed. Health Inf. (2016).

[41] O. Kayode, D. Gupta, A.S. Tosun, Towards a distributed estimator in smart home environment, IEEE 6th World Forum Int. Things (WF-IoT) (2020).

[42] D. Gupta, S. Bhatt, M. Gupta, O. Kayode, A.S. Tosun, Access control model for Google cloud iot, in: Proceedings of the IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), IEEE, 2020, pp. 198–208.

[43] A. Tekeoglu, A.Ş. Tosun, A closer look into privacy and security of chromecast multimedia cloud communications, in: Proceedings of the Multimedia Cloud Communication Workshop, Held in conjunction with INFOCOM 2015, 2015. Hong Kong, China.

[44] A. Tekeoglu, A.Ş. Tosun, Investigating security and privacy of a cloud-based wireless IP Camera: NetCam, in: Proceedings of the Workshop on Privacy, Security and Trust in Mobile and Wireless Systems (MobiPST 2015), Held in conjunction with ICCCN 2015, 2015. Las Vegas, USA.

[45] A. Tekeoglu, A.S. Tosun, A testbed for privacy and security of IoT Devices, in: Proceedings of the IEEE International Workshop on Data Science for Internet of Things, MASS 2016, 2016, pp. 1–6.

[46] A. Tekeoglu, A.Ş. Tosun, An experimental framework for investigating security and privacy of IoT Devices, in: Proceedings of the International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, 2017. Vancouver, CA.

[47] O. Kayode, A.S. Tosun, Analysis of IoT Traffic using HTTP Proxy, in: Proceedings of the ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–7, doi:10.1109/ICC.2019.8761601.

[48] S. Bhatt, F. Patwa, R. Sandhu, Access control model for aws internet of things, in: Proceedings of the International Conference on Network and System Security, Springer, 2017, pp. 721–736.

[49] S. Bhatt, A.T. Lo'ai, P. Chhetri, P. Bhatt, Authorizations in cloud-based Internet of Things: current trends and use cases, in: Proceedings of the Fourth International Conference on Fog and Mobile Edge Computing (FMEC), IEEE, 2019, pp. 241–246.

[50] D.-Y. Kim, S.D. Min, S. Kim, A dpn (delegated proof of node) mechanism for secure data transmission in iot services, CMC Comput. Mater. Cont 60 (2019) 1–14.

[51] Y. Liang, et al., A method to make accurate inventory of smart meters in multi-tags group-reading environment, in: Proceedings of the International Conference on RFID Technology and Applications (RFID-TA), 2016, pp. 123–128.

[52] J. Lin, M. Zheng, J. Chen, K. He, E. Pan, Smart Spare Part Inventory Management System with Sensor Data Updating, in: Proceedings of the IEEE International Conference on Industrial Cyber Physical Systems (ICPS), 2019, pp. 597–602.

[53] L. Zhang, N. Alharbe, A.S. Atkins, An IoT Application for Inventory Management with a Self-Adaptive Decision Model, in: Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, pp. 317–322.

[54] W. Raad, M. Bueno-Delgado, M. Deriche, W. Suliman, An IoT based inventory system for high value laboratory equipment, in: Proceedings of the Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2019, pp. 314–319.

[55] R. Li, T. Song, N. Capurso, J. Yu, J. Couture, X. Cheng, IoT applications on secure smart shopping system, IEEE Int. Things J. 4 (6) (2017) 1945–1954.

[56] A. Oplas, M.H. Rabago, C.L. Tormes, C.L.S. Romana, R. Laviste, Aeon: a smart medicine delivery and inventory system for cebu city government's long life medical assistance program, in: Proceedings of the IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM), 2018, pp. 1–6.

[57] W. Ding, Study of smart warehouse management system based on the IoT, in: Proceedings of the Intelligence computation and evolutionary computation, Springer, 2013, pp. 203–207.

[58] S.V. Hove, A. All, L.D. Marez, Short on time? context-aware shopping lists to the rescue: an experimental evaluation of a smart shopping cart, in: Proceedings of the Eleventh International Conference on Quality of Multimedia Experience (QoMEX), 2019, pp. 1–6.

[59] S. Mekruksavanich, The Smart Shopping Basket Based on IoT Applications, in: Proceedings of the IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), 2019, pp. 714–717.

[60] O. Raad, M. Makdessi, Y. Mohamad, I. Damaj, Sysmart indoor services: A system of smart and connected supermarkets, in: Proceedings of the IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), IEEE, 2018, pp. 1–6.

[61] G. Roussos, Enabling rfid in retail, Comput. (Long Beach Calif) 39 (3) (2006) 25–30.

[62] M. Gupta, J. Benson, F. Patwa, R. Sandhu, Secure V2V and V2I communication in intelligent transportation using cloudlets, IEEE Trans. Serv. Comput. (2020).

[63] M. Gupta, F.M. Awaysheh, J. Benson, M. Al Azab, F. Patwa, R. Sandhu, An attribute-based access control for cloud-enabled industrial smart vehicles, IEEE Trans. Ind. Inf. (2020). pages 1–1.

[64] M. Gupta, J. Benson, F. Patwa, R. Sandhu, Secure cloud assisted smart cars using dynamic groups and attribute based access control, arXiv preprint arXiv:1908.08112 (2019).

[65] M. Gupta, et al., Enabling and enforcing social distancing measures using smart city and ITS infrastructures: a COVID-19 use case, arXiv preprint arXiv:2004.09246 (2020).

[66] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, X. Lin, Smart community: an internet of things application, IEEE Commun. Mag. 49 (11) (2011) 68–75.

[67] Y. Sun, H. Song, A.J. Jara, R. Bie, Internet of things and big data analytics for smart and connected communities, IEEE Access 4 (2016) 766–773.

[68] P.A. Catherwood, D. Steele, M. Little, S. Mccomb, J. Mclaughlin, A community-Based IoT personalized wireless healthcare solution trial, IEEE J. Transl. Eng. Health Med. 6 (2018) 1–13.

[69] Y. Lee, W. Hsiao, C. Huang, S.T. Chou, An integrated cloud-based smart home management system with community hierarchy, IEEE Trans. Consum. Electron. 62 (1) (2016) 1–9.

[70] K. Axel, I.S. Khayal, Modeling 'thriving communities' using a systems architecture to improve smart cities technology approaches, in: Proceedings of the IEEE International Smart Cities Conference (ISC2), 2018, pp. 1–2.

[71] H. Yan, D. Long, Research on Key Technology for Data Storage in Smart Community Based on Big Data, in: International Conference on Intelligent Transportation, Big Data and Smart City, 2015.

[72] O.B. Mora, et al., A use case in cybersecurity based in blockchain to deal with the security and privacy of citizens and smart cities cyberinfrastructures, in: Proceedings of the IEEE International Smart Cities Conference (ISC2), IEEE, 2018, pp. 1–4.

[73] A. Zanella, et al., Internet of things for smart cities, IEEE Int. Things J. (2014).

[74] J. Jin, J. Gubbi, S. Marusic, M. Palaniswami, An information framework for creating a smart city through internet of things, IEEE Int. Things J. 1 (2) (2014) 112–121.

[75] M. Centenaro, L. Vangelista, A. Zanella, M. Zorzi, Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios, IEEE Wirel. Commun. 23 (5) (2016) 60–67.

[76] A. Solanas, C. Patsakis, M. Conti, I.S. Vlachos, V. Ramos, et al., Smart health: a context-aware health paradigm within smart cities, IEEE Commun. Mag. 52 (8) (2014) 74–81.

[77] H. Menouar, I. Guvenc, K. Akkaya, A.S. Uluagac, A. Kadri, A. Tuncer, UAV-enabled intelligent transportation systems for the smart city: applications and challenges, IEEE Commun. Mag. 55 (3) (2017) 22–28.

[78] X. Zheng, L. Tian, G. Luo, Z. Cai, A collaborative mechanism for private data publication in smart cities, IEEE Internet Things J. (2020). pages 1-1

[79] A. Meslin, N. Rodriguez, M. Endler, Scalable mobile sensing for smart cities: the MUSANet experience, IEEE Internet Things J. (2020). pages 1-1

[80] Vengadeswaran, Balasundaram, Core-an optimal data placement strategy in hadoop for data intensive applications based on cohesion relation, Comput. Syst. Sci. Eng. 34 (1) (2019) 47–60.

[81] J. Llinas, D.L. Hall, An introduction to multi-sensor data fusion, in: Proceedings of IEEE International Symposium on Circuits and Systems, 6, 1998, pp. 537–540.

[82] P. Varaiya, Smart cars on smart roads: problems of control, IEEE Trans. Autom. Control 38 (2) (1993) 195–207.

[83] J.P. Hubaux, S. Capkun, J. Luo, The security and privacy of smart vehicles, IEEE Secur. Priv. 2 (3) (2004) 49–55.

[84] D.M. Gavrila, V. Philomin, Real-time object detection for "smart" vehicles, in: Proceedings of the Seventh IEEE International Conference on Computer Vision, 1, 1999, pp. 87–93. vol.1

[85] P. Falcone, F. Borrelli, J. Asgari, H.E. Tseng, D. Hrovat, Predictive active steering control for autonomous vehicle systems, IEEE Trans. Control Syst. Technol. 15 (3) (2007) 566–580.

[86] J. Funke, M. Brown, S.M. Erlien, J.C. Gerdes, Collision avoidance and stabilization for autonomous vehicles in emergency scenarios, IEEE Trans. Control Syst. Technol. (2017).

[87] M. Kuderer, S. Gulati, W. Burgard, Learning driving styles for autonomous vehicles from demonstration, in: Proceedings of the IEEE International Conference on Robotics and Automation (ICRA), 2015, pp. 2641–2646.

[88] M. Gupta, J. Benson, F. Patwa, R. Sandhu, Dynamic groups and attribute-based access control for next-generation smart cars, in: Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, 2019, pp. 61–72.

[89] M. Gupta, J. Benson, F. Patwa, R. Sandhu, Dynamic groups and attribute-based access control for next-generation smart cars, 2020, US Patent App. 16/811,165.

[90] S. Sontowski, M. Gupta, S.S.L. Chukkapalli, M. Abdelsalam, S. Mittal, A. Joshi, R. Sandhu, Cyber attacks on smart farming infrastructure, UMBC Student Collection (2020).

[91] C. Dwork, A. Roth, et al., The algorithmic foundations of differential privacy, Found. Trends Theoret. Comput. Sci. 9 (3–4) (2014) 211–407.

[92] E. Vasilomanolakis, et al., On the security and privacy of Internet of Things architectures and systems, in: Proceedings of the International Workshop on Secure Internet of Things (SIoT), IEEE, 2015, pp. 49–57.

[93] A. Kobsa, J. Schreck, Privacy through pseudonymity in user-adaptive systems, ACM Trans. Int. Technol. (TOIT) 3 (2) (2003) 149–183.

[94] T.M. Truta, B. Vinay, Privacy protection: p-sensitive k-anonymity property, in: Proceedings of the 22nd International Conference on Data Engineering Workshops (ICDEW'06), IEEE, 2006. pp. 94–94

[95] M. Gupta, F. Patwa, R. Sandhu, An attribute-based access control model for secure big data processing in hadoop ecosystem, in: Proceedings of the Third ACM Workshop on Attribute-Based Access Control, 2018, pp. 13–24.

[96] M. Gupta, et al., Multi-layer authorization framework for a representative hadoop ecosystem deployment, in: Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, 2017, pp. 183–190.

[97] M. Gupta, F. Patwa, R. Sandhu, Object-tagged RBAC model for the hadoop ecosystem, in: Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, Springer, 2017, pp. 63–81.

[98] M. Gupta, F. Patwa, R. Sandhu, Poster: Access control model for the hadoop ecosystem, in: Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, 2017, pp. 125–127.

[99] F.M. Awaysheh, M. Alazab, M. Gupta, T.F. Pena, J.C. Cabaleiro, Next-generation big data federation access control: a reference model, Future Generat. Comput. Syst. (2020).

[100] A. Ouaddah, H. Mousannif, A.A. Elkalam, A.A. Ouahman, Access control in the internet of things: big challenges and new opportunities, Comput. Networks 112 (2017) 237–262.

[101] A. Thakare, E. Lee, A. Kumar, V.B. Nikam, Y.-G. Kim, PARBAC: Priority-Attribute-Based RBAC model for azure IoT cloud, IEEE Internet Things J. 7 (4) (2020) 2890–2900.

[102] V.C. Hu, et al., Guide to attribute based access control (abac) definition and considerations (draft), NIST special publication 800 (162) (2013).

[103] X. Jin, R. Krishnan, R. Sandhu, A unified attribute-based access control model covering DAC, MAC and RBAC, in: IFIP Annual Conference on Data and Applications Security and Privacy, Springer, 2012, pp. 41–55.

[104] M. Gupta, R. Sandhu, The GURA$_G$ administrative model for user and group attribute assignment, in: International Conference on Network and System Security, Springer, 2016, pp. 318–332.

[105] M. Gupta, Secure Cloud Assisted Smart Cars and Big Data: Access Control Models and Implementation, The University of Texas at San Antonio, 2018 Ph.D. thesis.

[106] M. Gupta, R. Sandhu, Authorization framework for secure cloud assisted connected cars and vehicular internet of things, in: Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, 2018, pp. 193–204.

[107] P. Bhatt, S. Bhatt, M. Ko, Poster: IoT SENTINEL-An ABAC Approach Against Cyber-Warfare In Organizations, in: Proceedings of the 25th ACM Symposium on Access Control Models and Technologies, 2020, pp. 223–225.

[108] S. Bhatt, R. Sandhu, ABAC-CC: Attribute-Based Access Control and Communication Control for Internet of Things, in: Proceedings of the 25th ACM Symposium on Access Control Models and Technologies, 2020, pp. 203–212.

[109] L. Kou, Y. Shi, L. Zhang, D. Liu, Q. Yang, A lightweight three-factor user authentication protocol for the information perception of iot, Computers Materials & Continua 58 (2) (2019) 545–565.

[110] B. Tang, H. Kang, J. Fan, Q. Li, R. Sandhu, Iot passport: a blockchain-based trust framework for collaborative internet-of-things, in: Proceedings of the 24th ACM Symposium on Access Control Models and Technologies, 2019, pp. 83–92.

[111] S.G. Finlayson, J.D. Bowers, J. Ito, J.L. Zittrain, A.L. Beam, I.S. Kohane, Adversarial attacks on medical machine learning, Science 363 (6433) (2019) 1287–1289.

[112] A.K. Gautam, V. Sharma, S. Prakash, M. Gupta, Improved hybrid intrusion detection system (hids): mitigating false alarm in cloud computing, BL Joshi (2012) 101.

[113] A.F.M. Hani, et al., Development of private cloud storage for medical image research data, in: Proceedings of the IEEE International Conference on Computer and Information Sciences, 2014, pp. 1–6.

[114] G. Nalinipriya, R.A. Kumar, Extensive medical data storage with prominent symmetric algorithms on cloud-a protected framework, in: Proceedings of the International Conference On Smart Structures And Systems-ICSSS'13, IEEE, 2013, pp. 171–177.

[115] E. Zeng, S. Mare, F. Roesner, End user security and privacy concerns with smart homes, in: Proceedings of the Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017), 2017, pp. 65–80.

[116] S. Rathore, J.H. Park, Semi-supervised learning based distributed attack detection framework for iot, Appl. Soft. Comput. 72 (2018) 79–89.

[117] A. McDole, M. Abdelsalam, M. Gupta, S. Mittal, Analyzing CNN based behavioural malware detection techniques on Cloud IaaS, arXiv preprint arXiv:2002.06383 (2020).

[118] A. Piplai, S. Mittal, M. Abdelsalam, M. Gupta, A. Joshi, T. Finin, et al., Knowledge enrichment by fusing representations for Malware threat intelligence and behavior, 2020.

[119] S. Rathore, et al., Blockdeepnet: a blockchain-based secure deep learning for IoT network, Sustainability 11 (14) (2019) 3974.

[120] I. Farris, L. Militano, M. Nitti, L. Atzori, A. Iera, MIFaaS: a mobile-IoT-federation-as-a-service model for dynamic cooperation of IoT cloud providers, Future Generat. Comput. Syst. 70 (2017) 126–137.

[121] R.H. Weber, Internet of things-New security and privacy challenges, Comput. Law Secur. Rev. 26 (1) (2010) 23–30.

[122] A.T. Chatfield, C.G. Reddick, A framework for internet of things-enabled smart government: a case of IoT cybersecurity policies and use cases in US federal government, Gov. Inf. Q. 36 (2) (2019) 346–357.

[123] L.M. Tanczer, I. Brass, M. Elsden, M. Carr, J.J. Blackstock, The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape, in: R. Ellis, V. Mohan (Eds.), Rewired: Cybersecurity Governance, 2019, pp. 37–56.

[124] X. Caron, et al., The internet of things (IoT) and its impact on individual privacy: n Australian perspective, Comput. Law Secur. Rev. 32 (1) (2016) 4–15.

[125] K.E. Benson, Q. Han, K. Kim, P. Nguyen, N. Venkatasubramanian, Resilient overlays for IoT-based community infrastructure communications, in: Proceedings of the IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI), 2016.

[126] T. Muhammed, R. Mehmood, A. Albeshri, Enabling reliable and resilient IoT based smart city applications, in: Proceedings of the International Conference on Smart Cities, Infrastructure, Technologies and Applications, Springer, 2017, pp. 169–184.

[127] H. Zhang, G. Chen, X. Li, Resource management in cloud computing with optimal pricing policies, Comput. Syst. Sci. Eng. 34 (4) (2019) 249–254.

[128] M.J. Van Der Donckt, D. Weyns, M.U. Iftikhar, R.K. Singh, Cost-benefit analysis at runtime for self-adaptive systems applied to an internet of things application., in: Proceedings of the ENASE, 2018, pp. 478–490.

[129] G. Skourletopoulos, et al., Cost-benefit analysis game for efficient storage allocation in cloud-centric internet of things systems: a game theoretic perspective, in: Proceedings of the IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 1149–1154.

[130] S.S.L. Chukkapalli, S. Mittal, M. Gupta, M. Abdelsalam, A. Joshi, R. Sandhu, K.P. Joshi, et al., Ontologies and artificial intelligence systems for the cooperative smart farming ecosystem, IEEE Access 8 (2020) 164045–164064.

[131] S.S.L. Chukkapalli, A. Piplai, S. Mittal, M. Gupta, A. Joshi, et al., A smart-farming ontology for attribute based access control, in: Proceedings of the 6th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2020), 2020.

[132] L. Farhan, R. Kharel, Internet of things: Vision, future directions and opportunities, in: Modern Sensing Technologies, Springer, 2019, pp. 331–347.

[133] M. Mohammadi, A. Al-Fuqaha, S. Sorour, M. Guizani, Deep learning for IoT big data and streaming analytics: a survey, IEEE Commun. Surv. Tutor. (2018).

[134] D. Gupta, O. Kayode, S. Bhatt, M. Gupta, A.S. Tosun, Learner's Dilemma: IoT devices training strategies in collaborative deep learning, IEEE 6th World Forum Internet Things (WF-IoT) (2020).